Nuova edizione
ottobre 2024

Rapporto

Clusit

2024

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Indice

ASTREA Via Copernico, 38 - 20125 Milano

Prefazione

Quella che mi appresto a scrivere è l'ultima prefazione del Rapporto Clusit che porterà la mia firma posto che, come avevo annunciato all'Assemblea del dicembre 2022 quando venni rieletto per la quinta volta, non mi ricandiderò alle elezioni che si terranno fra poco più di un mese.
Dopo cinque mandati, infatti, è ora di lasciare spazio a nuove idee e a una nuova linea d'azione.
In questi dieci anni, grazie al lavoro di tutti i membri del Consiglio Direttivo, del Comitato Scientifico e dei volontari, il Clusit è cresciuto, come numero di associati e come rappresentatività dei soci.
Sono aumentate le attività associative, gli eventi organizzati, le ore di formazione e aggiornamento che mettiamo a disposizione dei soci e in generale le iniziative che il Clusit organizza e a cui partecipa quasi quotidianamente.
Sicuramente, ma direi purtroppo, ha aiutato anche l'evoluzione del fenomeno cyber che continua a aumentare come numerosità dei casi (e come impatto medio di ogni attacco) che i nostri ricercatori mappano e analizzano.
Ha certamente contribuito anche il legislatore europeo e nazionale che in questi dieci anni ha dato vita a una vera e propria infrastruttura istituzionale che in questi giorni sta conoscendo un nuovo passo fondamentale grazie alla NIS2.

Tutto questo ha voluto dire altre Associazioni che si sono affiancate al Clusit, nuove iniziative convegnistiche, una infinità di eventi, master, corsi, pubblicazioni, pagine linkedin e soprattutto migliaia e migliaia di professionisti della cyber che da tutti i punti di vista stanno contribuendo ad affrontare la, oserei dire drammatica, situazione in cui si trova l'Italia.

Il mio invito alla famiglia professionale degli esperti di cybersicurezza è di saper essere uniti.
Le occasioni ci sono per tutti e sarebbe importante finalmente superare alcune modalità divisive che, purtroppo, ogni tanto si sentono e si leggono soprattutto nelle chat e sui social dove, talvolta, toni sprezzanti, autoreferenziali e un pochino supponenti dovrebbero lasciare spazio a idee e prospettive.
Una famiglia professionale coesa, capace di accettare la presenza di professionisti di vari livelli di preparazione e di età (che hanno tutti diritto di parola e di lavoro perché, come in tutte le professioni, non sempre c'è bisogno dei top gun), che sia in grado di fare fronte comune nell'interesse di tutti, sarà fondamentale nei prossimi anni.

E questo appare ancora più vero in un momento particolarmente critico.
È stata appena scoperta la rete di criminali che ha dato vita a un vero e proprio mer-

cato nero dei dossier (e al momento si sa ancora pochissimo ma in tutta evidenza si tratta di un fatto gravissimo che non potrà non avere ripercussioni politiche e legislative), abbiamo assistito al grande fallimento del piracy shield tramite il quale è stato bloccato google drive e possiamo ora leggere i numeri del primo semestre 24 che ci dicono che l'Italia, seppur con un rallentamento, vede ancora molto alto il numero di attacchi riusciti e gravi da noi censiti.

Questa ultima notizia è la più importante di tutte.
Stiamo forse assistendo, per la prima volta, a un'inversione di tendenza? Forse finalmente tutte le azioni che tanti operatori del settore, fra cui il Clusit, hanno posto in essere in questi anni stanno dando i primi frutti?
Vedremo. È presto per trarre conclusioni.
Ma come tante altre volte abbiamo dovuto scrivere e dichiarare che eravamo davanti all'anno peggiore di sempre, possiamo oggi dire che questo primo semestre non è stato il peggiore di sempre.
Ed è già qualcosa.

E allora in bocca al lupo a chi mi seguirà come Presidente del Clusit e al nuovo Consiglio Direttivo a cui auguro di avere meno da fare rispetto a quanto abbiamo dovuto fare in questi dieci anni perché devo per forza augurarmi che il fenomeno cyber, veramente, inizi a rallentare.

Chiudo ribadendo l'auspicio che purtroppo ormai faccio da diversi Rapporti: che i conflitti armati che interessano due zone del mondo in particolare, cessino nel più breve tempo possibile. Sono tragedie immani. Basta. Basta. Basta.

*** *** ***

E allora buona lettura del Rapporto che avete fra le mani.
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.

Ringrazio, a nome di tutti gli Associati e di tutti coloro che lo leggeranno, i Colleghi che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit per il primo semestre 2024. **Oltre 80.000 copie scaricate** e più di 800 articoli pubblicati e servizi su web, cartaceo, Radio e TV negli ultimi 12 mesi, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi 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

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Nei primi sei mesi del 2024 **gli attacchi cyber** censiti dagli esperti del Clusit **sono cresciuti del 23%** rispetto al semestre precedente. In media, si sono verificati nel mondo 9 attacchi importanti al giorno; **in Italia il 7,6% degli incidenti.**

La sanità è il settore più colpito a livello globale. **In Italia** bersagliato **il manifatturiero**, ma **gli attacchi alla sanità crescono dell'83%** rispetto al primo semestre 2023.

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel primo semestre del 2024**, confrontandoli con i dati raccolti negli anni precedenti.

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

Segue un **approfondimento sulla** evoluzione della **Cybersecurity in ambito manifatturiero/industriale**, con i dati di settore tratti dalle ultime rilevazioni Clusit al 30 giugno 2024. Completa lo speciale Manufacturing un articolo sul **Regolamento Macchine e la Cybersecurity nel settore manifatturiero**, a cura di CAST.

Riportiamo in seguito i risultati di **una survey sulla Cybersecurity nelle piccole e medie imprese.** Più di **500 aziende hanno risposto alla survey che è stata realizzata** tra maggio e luglio 2024 **dalla Camera di Commercio di Modena e dall'Università di Modena e Reggio Emilia**, in collaborazione col Clusit.

Questi sono infine i temi trattati nella sezione FOCUS ON:

- **Cybersecurity e cyber resilience nell'era del quantum**, a cura di Federica Maria Rita Livelli.
- **Dall'assessment cyber al trasferimento del rischio residuo nel complesso scenario di minacce e responsabilità: una collaborazione virtuosa**, a cura del Centro di Competenza START 4.0 e di UnipolSai.
- **Il divario di realtà - Focus sulla crescente disparità tra rischio e prevenzione negli attacchi via e-mail**, a cura di Libraesva.
- **Come utilizzare l'AI per accelerare detection, investigation e response**, a cura di CrowdStrike.

Analisi dei principali cyber attacchi noti del primo semestre del 2024 a livello globale

Italia (ancora) sotto assedio?

In questa prima sezione dell'aggiornamento semestrale del Rapporto CLUSIT 2024, giunto ormai al suo tredicesimo anno di pubblicazione, analizziamo i più gravi incidenti cyber noti avvenuti a livello globale (Italia inclusa) nei 5 anni precedenti e li confrontiamo con l'analisi degli incidenti noti del 2023 e del primo semestre 2024.

Analizzando i dati dell'ultimo quinquennio, dal punto di vista quantitativo, la situazione è nettamente peggiorata, mostrando una tendenza pressoché costante, tanto che la media mensile di incidenti gravi a livello globale è passata dai 139 del 2019 ai 232 del 2023, fino ai 273 del primo semestre 2024: in pratica, in 5 anni a livello globale siamo passati dal rilevare 4,5 eventi al giorno a classificarne mediamente 9.

Nel 2023 gli incidenti sono aumentati del 11% a livello globale rispetto al 2022 (ma quelli verso l'Italia sono aumentati ben del 65%). La tendenza globale del primo semestre 2024 mostra una ulteriore crescita, molto significativa, pari al 23% rispetto al semestre precedente.

Oltre a osservare una crescita costante della frequenza degli incidenti, anche dal punto di vista qualitativo negli anni la situazione è peggiorata in modo drammatico. La nostra valutazione della *Severity* media (indice di gravità) degli attacchi rilevati è peggiorata anno dopo anno, il che rappresenta un ulteriore moltiplicatore dei danni. Nel 2023, gli eventi classificati come "critici" o "gravi" rappresentano ormai oltre l'81% del totale (erano il 47% nel 2019), dato che si conferma anche nel primo semestre 2024.

Considerato che questa analisi riguarda solo attacchi andati a buon fine ("incidenti", cioè attacchi effettivamente avvenuti e confermati) divenuti di dominio pubblico, l'osservazione di queste dinamiche conferma la nostra convinzione che, rispetto al periodo 2011-2018, negli ultimi anni sia avvenuto un cambiamento drastico nello scenario globale della cyber-insicurezza, al quale, visti gli esiti, non è evidentemente corrisposto un incremento sufficiente delle contromisure adottate dai difensori.

Come abbiamo scritto commentando i dati dell'ormai remoto 2021, "siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'ICT e della stessa Cyber Security, ed hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell'economia e della geopolitica".

Per quanto numericamente il cybercrime sia responsabile della maggior parte degli incidenti rilevati, dal 2022 a queste dinamiche, si sono aggiunti ii conflitti Russo-Ucraino e quello Israelo-Palestinese, che hanno accelerato il dispiegamento su larga scala di capacità cibernetiche offensive di livello statuale, impiegate dai contendenti, dai loro alleati e in generale da tutti i principali attori globali, a supporto di attività di cyber-intelligence, di cyber-warfare e di operazioni ibride, realizzate sia "tramite" che "contro" il cyberspazio, nonché di attività di supporto ideologico sotto forma di attacchi dimostrativi (principalmente di tipo DDoS) contro obiettivi "ampi" riferibili ai Paesi avversari. Questo fenomeno, oltre a complicare la vita degli analisti, introduce un "cambiamento di fase" importante, con implicazioni molto serie nel medio-lungo termine.

In particolare, Mosca utilizza da tempo cyber operations per realizzare campagne di disinformazione di massa e plasmare la percezione pubblica. Nell'ambito del conflitto in Ucraina i principali obiettivi di queste attività sono minare il governo ucraino e il morale della popolazione, indebolire l'Alleanza Atlantica, influenzare l'esito delle prossime elezioni di vari paesi occidentali, e mantenere il sostegno interno in Russia. Oltre a queste classiche attività di disinformazione realizzate "tramite" il cyberspazio (in particolare tramite i social media), gli aggressori russi hanno intensificato le loro operazioni cibernetiche "contro" il cyberspazio, prendendo di mira il governo ucraino e i suoi membri, e lanciando attacchi distruttivi a infrastrutture critiche, sia militari che civili.

Infine, le agenzie russe hanno anche "messo a sistema" diversi gruppi cybercriminali, i quali hanno aumentato le proprie attività contro bersagli occidentali, confidando nella benevolenza del proprio governo nel momento in cui colpiscono obiettivi "nemici". Questa dinamica ricorda le "patenti da corsa" che i corsari ottenevano dai governi europei nel XVII e XVIII secolo e, considerate le capacità di questi gruppi, contribuisce a innalzare i livelli di rischio in modo apprezzabile.

Riassumendo le nostre impressioni sulla situazione attuale, dobbiamo sottolineare che, oltre all'incremento dei danni causato dal cybercrime e dalle "normali" attività di intelligence che osserviamo ormai da molti anni, dal 2022 siamo entrati in una nuova fase di "conflittualità cibernetica diffusa", che è ulteriormente cresciuta anche nel 2023 e si conferma anche nel primo semestre 2024, anche a causa dell'allargamento del conflitto tra Israele e le milizie islamiche supportate dall'Iran in vari paesi dell'area medio-orientale.

In questo scenario di minacce crescenti sia per numero che per intensità, il nostro Paese risulta tra i più colpiti, come dimostra il significativo incremento di attacchi andati a segno nel 2023. Fin dall'inizio del conflitto nel 2022 abbiamo scritto "l'Italia è nel mirino", e osservando i dati del 2023 avevamo concluso che il nostro Paese rappresenta un bersaglio particolarmente facile, dal momento che nel corso dello scorso anno ha subito ben l'11% degli incidenti rilevati a livello globale (contro un 3,4% del 2021 e un 7,6% del 2022). Il dato parziale del primo semestre 2024 mostra una leggera diminuzione degli incidenti avvenuti in Italia, segnale positivo ma che riteniamo prematuro considerare come un alleggerimento della pressione, e che potrebbe essere causato da una fluttuazione "stagionale" delle attività dei "bad actors". In ogni caso, anche nel primo semestre 2024 il numero di incidenti subiti dal nostro paese è sproporzionatamente alto rispetto alla nostra popolazione e al PIL nazionale in rapporto col PIL mondiale, il che certamente merita un'attenta riflessione e azioni concrete di mitigazione.

Per questa ragione abbiamo aggiunto un capitolo specifico e svolto alcune considerazioni puntuali su quanto osservato, nella speranza di contribuire a un incremento della consapevolezza nazionale e dell'efficacia delle contromisure adottate. I rischi cyber hanno ormai assunto una natura esistenziale, ed è urgente adeguare al nuovo scenario le misure di prevenzione e protezione, a tutti i livelli (pubblica amministrazione, aziende pubbliche e private), onde evitare di subire danni inevitabilmente crescenti.

Confidando che anche quest'anno il Rapporto CLUSIT possa apportare un contributo significativo al dibattito nazionale in merito alle problematiche della sicurezza cibernetica e alle sue importanti ricadute sul benessere del Paese, auguriamo a tutti una buona lettura.

Analisi dei principali incidenti cyber noti a livello globale dal 2019 al primo semestre 2024

13%
degli incidenti censiti a livello mondiale dal 2019 sono avvenuti nel I semestre 2024

In questa sezione offriamo una panoramica degli incidenti di sicurezza di pubblico dominio più significativi avvenuti a livello globale nel primo semestre 2024, confrontandoli con i dati raccolti nei 5 anni precedenti.
Lo studio si basa sull'analisi di incidenti cyber noti, andati a buon fine e di particolare gravità, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle Organizzazioni vittima degli stessi.

Nel periodo in esame, tra gennaio 2019 e giugno 2024, si sono verificati un totale di **12.495 incidenti**, così suddivisi:

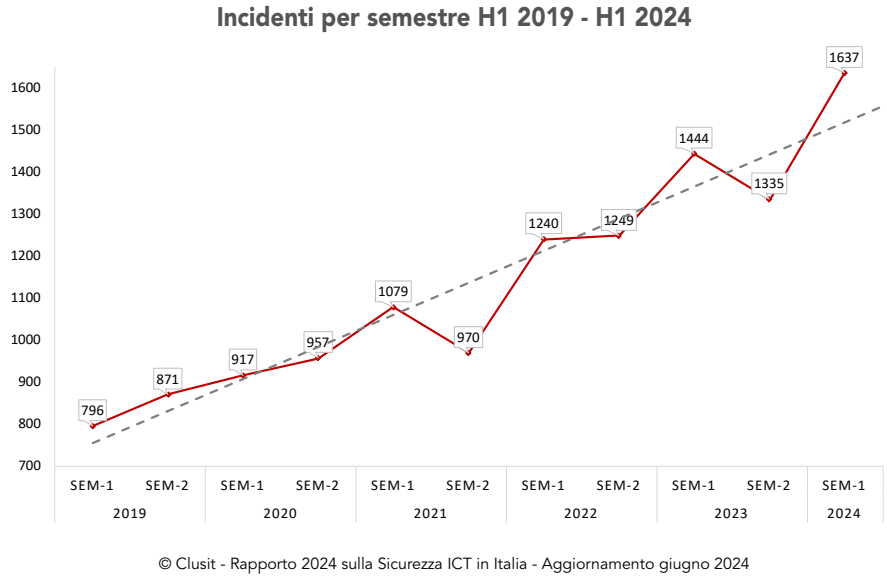


Fig. 1 - Andamento degli incidenti cyber nel periodo 2019-H1 2024

Nell'ultimo semestre abbiamo registrato 1.637 incidenti, il numero maggiore di sempre per un solo semestre, ed è interessante notare come già dal 2019 la realtà abbia iniziato a superare le previsioni indicate in grigio dalla linea di tendenza e solo in poche occasioni l'andamento ha mostrato un'inversione in questo trend.

A conferma di una costante recrudescenza dello scenario degli incidenti, gli eventi dell'ultimo semestre costituiscono da soli il 13% del totale dal 2019 e denotano una crescita del 23% rispetto al semestre precedente.

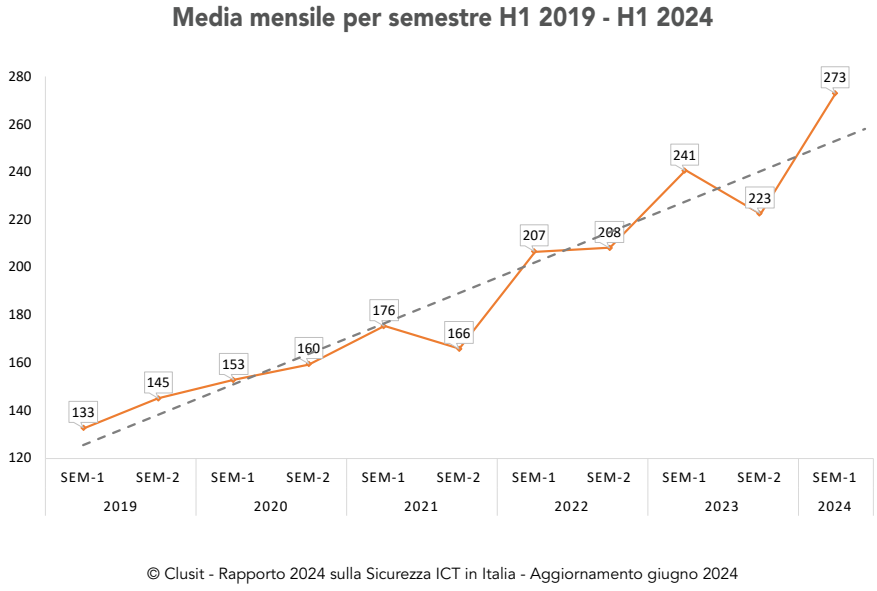
+23%

è la crescita degli incidenti dal II semestre 2023 al I semestre 2024

Conseguentemente, anche la media mensile degli incidenti cyber (**Fig. 2**) è aumentata considerevolmente, raggiungendo quota 273, più del doppio di quanto avveniva il I semestre 2019.

2x

è l'aumento della media mensile degli incidenti a livello mondiale rispetto al I semestre 2019



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Fig. 2 - Andamento delle medie mensili nel periodo 2019-H1 2024

Distribuzione degli attaccanti per tipologia

+23%

è la crescita del Cybercrime a livello mondiale dal I sem. 2023 al I sem.2024

La crescita in volume degli incidenti è sostenuta (**Fig. 3**) da un aumento del fenomeno *Cybercrime* (88% del totale, oltre 5 punti percentuali rispetto al 2023 e oltre 23 punti percentuali rispetto al primo semestre del 2023) e deve far riflettere su quanto questo ambito attiri le attenzioni della criminalità organizzata: da tempo ormai l'economia criminale sottesa ai reati informatici supera altre economie criminose di natura "tradizionale", forte anche delle dinamiche "as-a-Service" offerte agli affiliati, tanto da risultare "conveniente" anche per i criminali "non addetti" ai lavori cyber.

Espionage scende rispetto al 2023 di oltre 2 punti percentuali confermando il trend di diminuzione già osservato nel 2023, in cui avevamo rilevato 4 punti percentuali in meno rispetto al 2022, così come l'*Hacktivism*, che dopo un picco di crescita nel 2023, nel primo semestre torna in flessione di circa 3 punti percentuali, raggiungendo il 6% del totale.

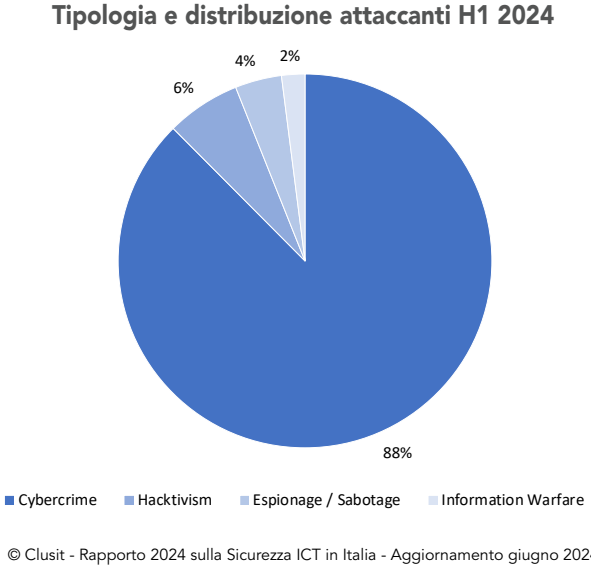


Fig. 3 - La distribuzione percentuale degli attaccanti nel primo semestre 2024

Nel I semestre 2024, considerando solo le informazioni di pubblico dominio, possiamo dire che la tendenza complessiva degli incidenti causati da attacchi a sfondo politico, sociale e di information warfare sembra tornare negativo, nonostante l'acuirsi

e l'estensione progressiva dei conflitti già attivi nel 2023. Occorre però ricordare che diversi governi, e in particolare Russia, Nord Corea e Cina, utilizzano gruppi cybercriminali come esecutori materiali di alcune attività di intelligence (p.es. economica), complicando il quadro dell'attribuzione delle reali motivazioni di un buon numero di incidenti.

Distribuzione delle vittime per categoria

1° Healthcare

il settore più colpito da incidenti cyber nel mondo nel I semestre 2024

1 su 5

è il numero degli incidenti nel mondo che colpisce il settore Healthcare

Confermando una tendenza già osservata nei semestri precedenti, il settore Healthcare nel I semestre 2024 continua a risalire la triste classifica dei settori che più subiscono incidenti cyber, raggiungendo, per la prima volta da quando realizziamo questo Rapporto, la prima posizione. Il 18% degli incidenti (poco meno di un incidente su cinque) colpisce questo settore, un aumento di quasi 4 punti percentuali sul totale, rispetto al 2023. Quanto sia consistente questa crescita lo rivelano i valori assoluti: 296 incidenti in soli 6 mesi, 100 in meno di tutto il 2023, pressoché lo stesso dato dell'intero 2022 (304 attacchi).

È la seconda volta dal 2019 che gli eventi di tipo *Multiple Target* sono superati da una specifica categoria. Nonostante perdano il loro "primato" in termini di incidenza sul campione complessivo, gli incidenti *Multiple target* continuano tuttavia a crescere in modo costante.

L'ambito *Governativo / Militare / Law Enforcement* mantiene stabilmente il terzo posto (13%, un calo di 1 punto percentuale rispetto al 2023), così come il settore Finance/Insurance al quarto.
In quest'ultimo caso, tuttavia, buone notizie: l'incidenza (8%) rispetto al totale si riduce di oltre 3 punti percentuali, e in valore assoluto i 130 incidenti nel semestre fanno sperare che al termine del 2024 non si raggiungano gli oltre 300 del 2023.

Stabili in classifica i comparti *ICT* (7%) ed *Education* (6%); dei due, il comparto *ICT* registra una leggera flessione, analogamente a *Finance/Insurance*, che potremo verificare al termine dell'anno: se si confermerà, questo potrebbe essere il segnale che i settori che vantano una maggiore maturità (anche grazie alla pressione regolatoria) in termini di sicurezza denotano più di altri la capacità di reagire all'aumento della pressione degli attacchi in tempi ragionevolmente brevi.

In linea con le considerazioni precedenti va letto il dato del settore *Manufacturing*, al settimo posto tra i settori più colpiti, con oltre il 5% degli incidenti rispetto al totale, è pressoché nell'identica posizione rispetto all'anno precedente: considerato che il numero in valore assoluto degli eventi è cresciuto, il settore non modifica la propria posizione in classifica, pur risultando maggiormente colpito.

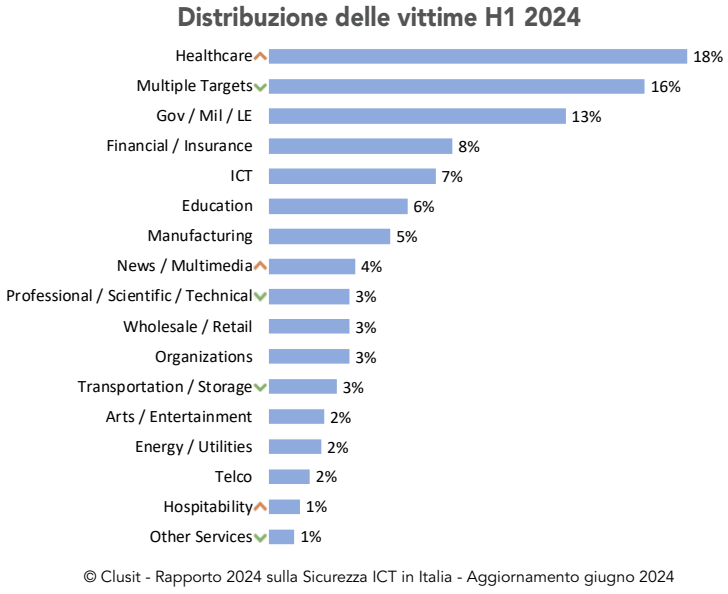


Fig. 4 - Distribuzione della tipologia di vittime nel H1 2024

È *News/Multimedia* che registra il triste primato di crescita di tutta la classifica: superando in un semestre il numero degli incidenti dell'intero anno precedente, raggiunge l'ottavo posto dal dodicesimo del 2023.
Questo non è l'unico caso di settori il cui numero di eventi nel *semestre* si avvicina pericolosamente al dato dell'anno precedente: negli ambiti *Organizations, Wholesale/Retail* ed *Energy/Utilities*, il numero degli incidenti del I semestre 2024 supera, in qualche caso in modo significativo, il 70% del totale dell'intero 2023.

Distribuzione generale delle vittime per area geografica

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 2023 i due fenomeni interessanti che abbiamo osservato sono stati la crescita

particolarmente accentuata del numero di vittime nel continente americano e il fatto che il continente europeo, per la prima volta da anni, passasse al secondo posto superando il numero di incidenti che hanno colpito località multiple.

Nel primo semestre 2024 (**Fig. 5**) si conferma la preponderanza di vittime nel continente americano (41%), sebbene in leggero calo di 3 punti percentuali rispetto all'anno precedente, ma il dato più interessante che emerge è il trend di crescita del numero di vittime in Europa che, con il 29% del totale, aumenta la propria quota sul totale di 6 punti percentuali: circa un terzo degli incidenti nel mondo avviene nel nostro continente.

1/3

degli incidenti a livello mondiale colpisce il continente europeo

In valore assoluto, con 469 incidenti che hanno avuto vittime in Europa, nel solo I semestre 2024 si sono registrati circa il 75% degli incidenti del 2023; se questo trend si confermerà, a fine 2024 l'Europa consoliderà e stabilizzerà la sua posizione di secondo continente più colpito.

L'Asia segue con l'8%: considerato il peso rilevante dell'economia del continente a livello mondiale, non possiamo non ritenere che questo valore sia influenzato dall'ancora limitata presenza/efficacia di normative che obbligano le organizzazioni a notificare gli incidenti più gravi. Il 17% degli attacchi è avvenuto parallelamente contro località multiple, mentre rimane marginale la componente, sul totale, degli incidenti riferibili a Oceania (4%), comunque in crescita, e Africa (1%).

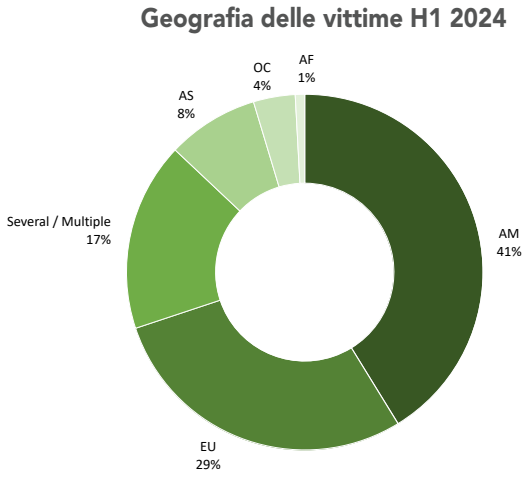


Fig. 5 - Distribuzione geografica delle vittime in percentuale nel H1 2024

Distribuzione delle tecniche di attacco

1/3
degli incidenti a livello mondiale ha il malware come primaria tecnica di violazione

Nel primo semestre 2024 il *Malware* continua a costituire la tecnica preferita dai cyber criminali (**Fig. 6**), utilizzata in oltre un terzo dei casi di incidenti registrati nel nostro campione, seppure con una leggera flessione (dal 36% nel 2023 al 34% in H1 2024). 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, che spesso collaborano fra loro con uno schema di affiliazione. Gli incidenti basati sullo sfruttamento di vulnerabilità costituiscono come nel 2023 la seconda tecnica più utilizzata (al 14%, in discesa di 4 punti percentuali rispetto al 2023). Il *phishing* risulta stabile (8%) al terzo posto, sebbene la crescita del numero degli eventi registrati in valore assoluto sia superiore alla media delle categorie precedenti.
DDoS e *Multiple Techniques* scendono di un punto percentuale.

Identity Theft
Nel I sem. 2024 sono avvenuti nel mondo più incidenti di questa categoria che negli anni precedenti

Gli incidenti basati su Identity Theft crescono di 1 punto percentuale, ma andando a osservare i dati in valore assoluto questa crescita assume un carattere preoccupante: nel solo I semestre 2024 sono avvenuti più incidenti basati su questa tecnica di tutti quelli rilevati nel 2023 e negli anni precedenti.

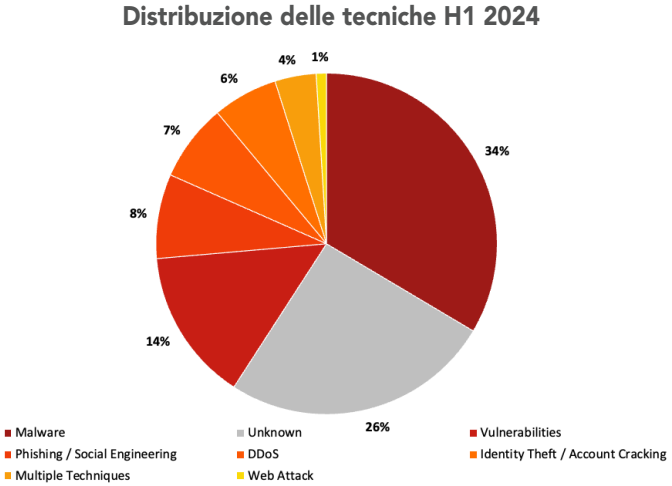


Fig. 6 - Distribuzione delle tecniche di attacco nel 2023

Per circa un incidente su quattro (26%) non è possibile, da fonti pubbliche, determinare la tecnica utilizzata (*Unknown*, in aumento di 5 punti percentuali rispetto al 2023).

Analisi della "Severity" degli attacchi

L'analisi della gravità degli incidenti si pone come obiettivo la valutazione degli impatti degli attacchi avvenuti con successo, che non necessariamente corrisponde con l'aumento dei numeri assoluti degli eventi, né si può banalmente dedurre dalla vittima o dalla tecnica utilizzata.
Il 2023 è stato caratterizzato, in linea con gli anni precedenti, dalla crescita consistente della gravità degli incidenti, in particolare del numero di quelli classificati come *Critical*, ovvero al massimo livello della nostra scala.
Nel I semestre 2024, questa tendenza sembrerebbe essersi arrestata (dato da confermare nella prossima edizione del Rapporto, riferita all'intero anno). Per quanto è possibile osservare nei primi sei mesi dell'anno, al crescere del numero degli attacchi non aumentano proporzionalmente gli incidenti *Critical* (che attestandosi al 31% perdono 7 punti percentuali), in favore degli eventi classificabili come High: questi costituiscono la metà degli incidenti registrati nel primo semestre dell'anno, con un incremento di 8 punti percentuali, sostanzialmente equivalente alla quota di incidenti Critical che si riduce.

81%

è il numero degli incidenti con Severity massima (Critical o High) rispetto al totale nel mondo

Per dare una concreta misura della crescita registrata, gli incidenti con gravità *High* nei primi sei mesi del 2024 considerati in valore assoluto sono circa il 70% di quanto censito in tutto il 2023.
Al netto della diversa distribuzione tra i due livelli più elevati della magnitudine degli incidenti, l'informazione più rilevante, che non cambia rispetto a quanto già descritto nel Rapporto riferito al 2023, è che l'area di maggior rischio (*Critical* e *High*) occupa al primo semestre 2024 ben l'81% del totale (era l'80% nel 2023).

A conferma della recrudescenza degli impatti determinati dagli incidenti registrati, grazie anche alla pervasività della digitalizzazione dei processi aziendali, gli incidenti a basso impatto sono di fatto scomparsi dal nostro campione che, lo ricordiamo, prende a riferimento gli attacchi noti con gravi conseguenze per le organizzazioni in tutto il mondo.

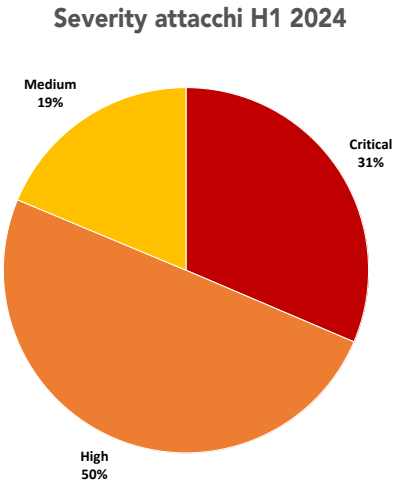


Fig. 7 - Distribuzione della Severity nel H1 2024

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 2024 (**Fig. 8**) rispecchiano in modo pressoché fedele quelle del 2023 (**Fig. 9**).

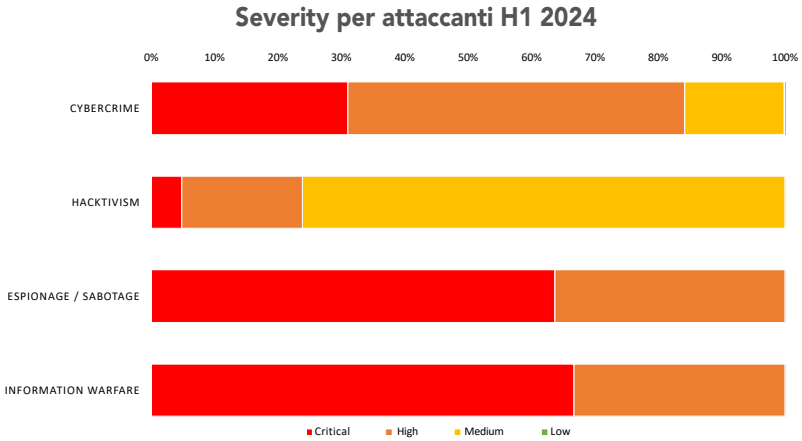
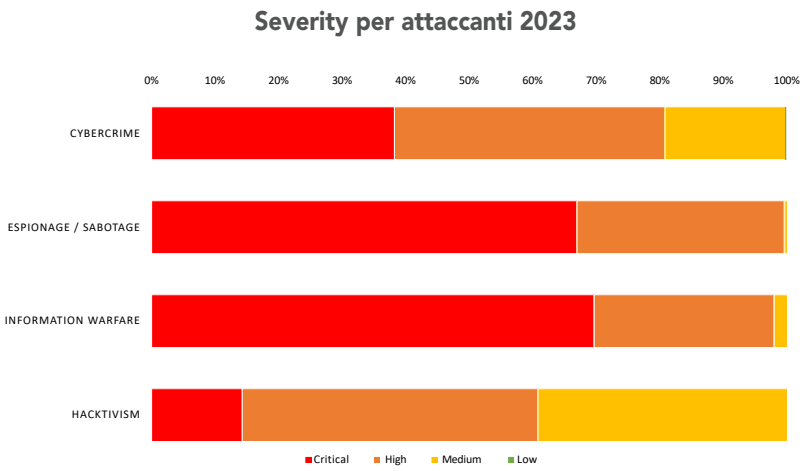


Fig. 8 - Distribuzione della Severity per attaccanti nel I sem.2024



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Fig. 9 - Distribuzione della Severity per attaccanti nel 2023

100%

Nel mondo, tutti gli incidenti Espionage e Information Warfare censiti hanno causato l'impatto massimo

Sebbene riferendosi ai numeri in valore assoluto è corretto sostenere che gli attacchi dal 2023 al I semestre 2024 condotti dai criminali informatici hanno determinato mediamente conseguenze maggiormente critiche (gli eventi classificati *Critical* e *High* sono superiori all'85% del totale), è evidente come gli incidenti con matrice *Espionage* e *Information Warfare* sono progettati ed eseguiti per massimizzare i successi degli attaccanti e gli impatti sulle vittime: in queste categorie, nessun evento ha una Severity inferiore al livello High.

Nel caso degli attacchi di *Hacktivism*, nel primo semestre dell'anno si manifesta una piccola inversione di tendenza, in continuità con quanto già si era verificato nel 2023: si riducono ancora gli incidenti *Critical* (da circa il 50% del 2022, passando a poco più del 10% del 2023, nel I semestre 2024 non superano il 5%) rispetto al totale, mentre aumentano quelli di livello Medium: tre incidenti su quattro sono classificabili a questo livello di Severity. Per tutte le categorie scompaiono di fatto gli attacchi a basso impatto.

Severity per tipologia di vittima

L'analisi della *Severity* per tipologia di vittima tra il primo semestre 2024 (**Fig. 10**) e l'anno 2023 (**Fig. 11**) mostra innanzitutto una flessione della criticità degli impatti complessivi a favore delle *severity High*, mantenendo di fatto inalterata la situazione se si considerano gli impatti rilevanti. *Healthcare*, *Gov / Mil / LE*, *Financial / Insurance*, *ICT*, *Education*, *Manufacturing*, *News / Multimedia*, *Professional / Scientific / Technical* e Wholesale mostrano infatti tutti impatti rilevanti nell'80% dei casi o più. In particolare, *ICT*, *Manufacturing*, e *Professional / Scientific / Technical* sono i settori maggiormente impattati della serie.

Multiple targets, sebbene in seconda posizione in termini numerici tra gli incidenti del semestre, è la categoria meno impattata rispetto alle altre, con "solo" il 70% di *severity Critical* o *High*.

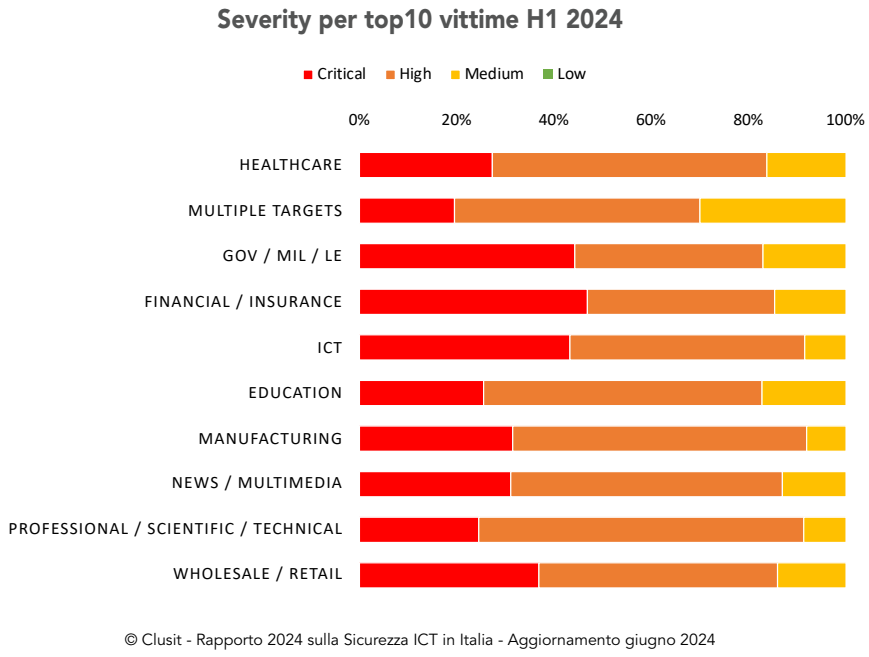


Fig. 10 - Distribuzione della Severity per prime 10 vittime nel H1 2024

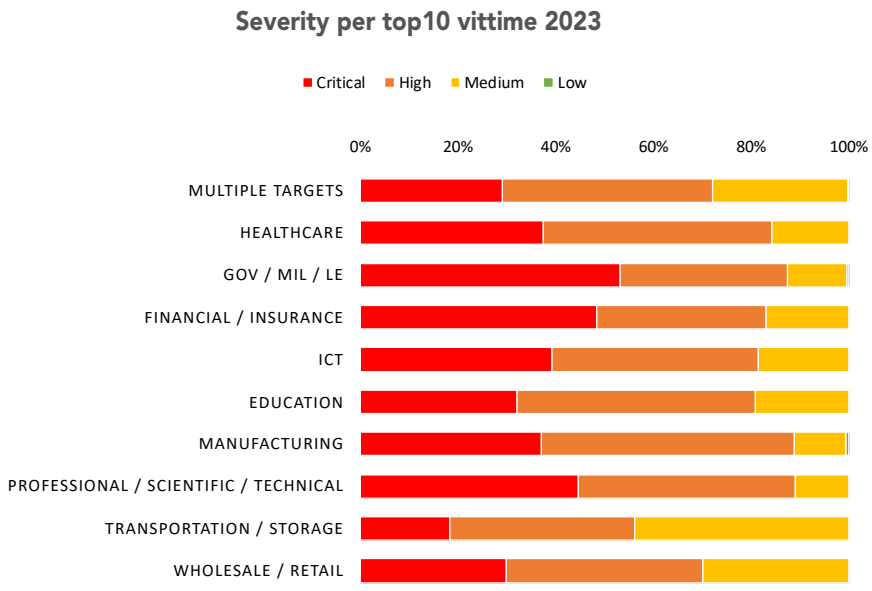


Fig. 11 - Distribuzione della Severity per prime 10 vittime nel 2023

Severity per tecniche di attacco

Esattamente come avvenuto nel 2023 (**Fig. 13**), nel primo semestre 2024 (**Fig. 12**) tutte le tecniche utilizzate per generare incidenti hanno determinato una percentuale significativa di impatti critici sulle vittime.

Se da una parte il Malware mantiene una costante del 40% di *severity* critica rispetto all'anno precedente, un dato di certo non rassicurante, diminuisce l'impatto degli incidenti basati sullo sfruttamento di vulnerabilità (dal quasi 60% di *severity* critica nel 2023 al 35% nel primo semestre di quest'anno).

40%

è la percentuale di incidenti malware censiti a livello mondo che genera impatti Critical

Rimane sostanzialmente costante la gravità degli incidenti basati su tecniche di *Phishing / Social Engineering (20%)*, DDoS (quasi 20%) e *Identity Theft / Account Cracking* (di poco superiore al 20%).
In calo invece gli impatti critici di incidenti che sfruttano tecniche multiple (40% rispetto al 50% del 2023) e Web Attack (dal 20% al 10%), così come le tecniche sconosciute (dal 40% degli impatti critici nel 2023 al 30% nel primo semestre di quest'anno).

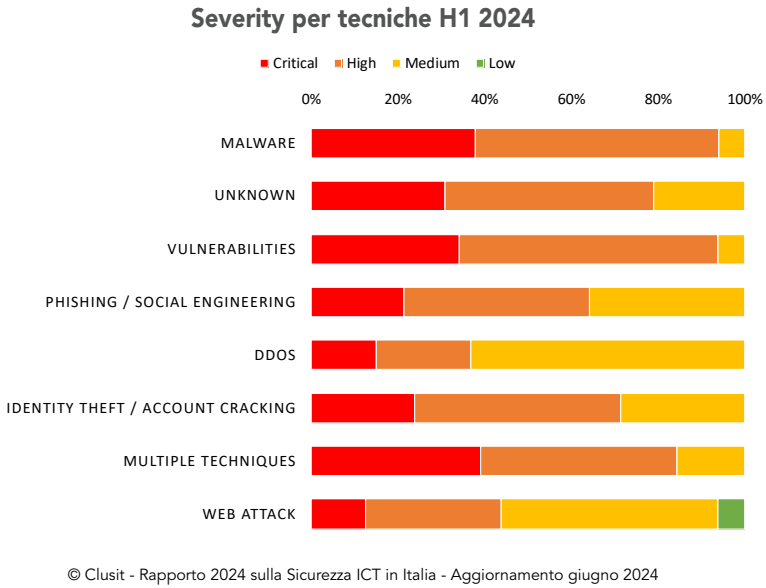


Fig. 12 - Distribuzione della Severity per tecniche di attacco nel H1 2024

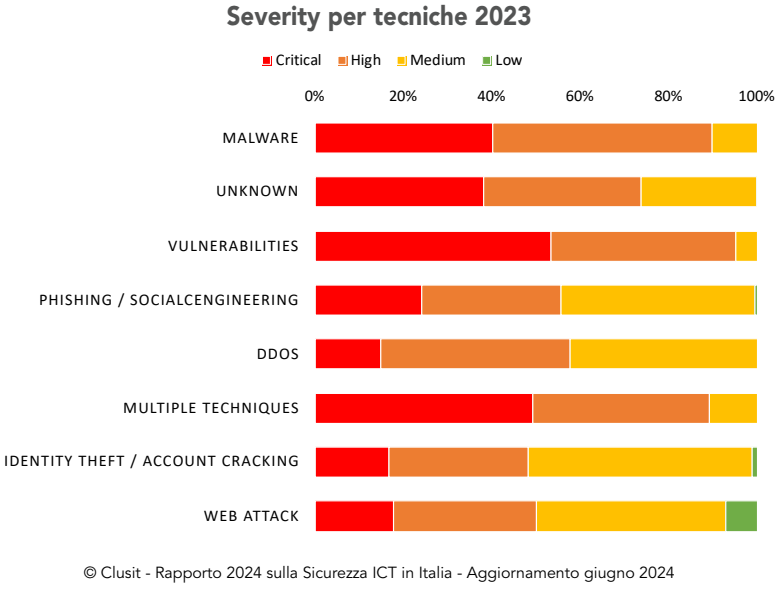


Fig. 13 - Distribuzione della Severity per tecniche di attacco nel 2023

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 2022 e il 2023: 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 2024.

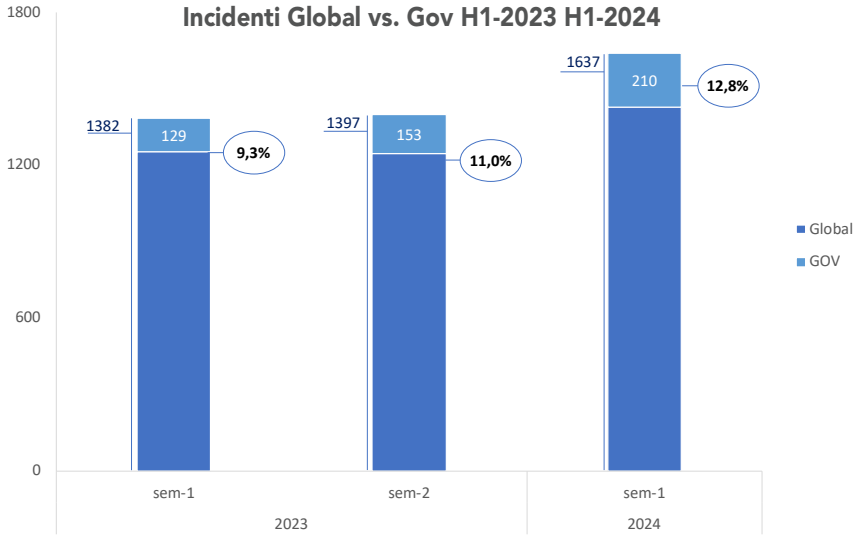


Fig. 14 - Attacchi al settore GOV *(CENTRAL/LOCAL) nel periodo H1 2023-H1 2024*

Tra il 2019 e il primo semestre 2024 il campione ha incluso 1.359 eventi noti di particolare gravità che hanno coinvolto realtà governative nel mondo; quelli nel primo semestre 2024 sono stati 210, con un incremento di quasi il 63% rispetto al primo semestre 2023. Il settore incide rispetto al totale degli incidenti del I semestre 2024 di circa il 13%, e tale percentuale risulta in crescita rispetto ai semestri precedenti.

+63%
è la crescita degli incidenti al settore GOV dal I semestre 2023 al I semestre 2024

La distribuzione degli attaccanti (**Fig. 15**) mostra un forte incremento del fenomeno cybercrime, che nel primo semestre 2024 ha sferrato un numero di attacchi pari a

oltre il 90% di tutto l'anno 2023; rimane invece grosso modo costante negli ultimi tre semestri, con solo un lievissimo calo, il fenomeno hacktivism, che in ogni caso si rivolge per propria natura a questo settore con particolare attenzione: il 30% degli incidenti a livello mondiale originati da attivisti, colpisce l'ambito GOV (Central/Local).

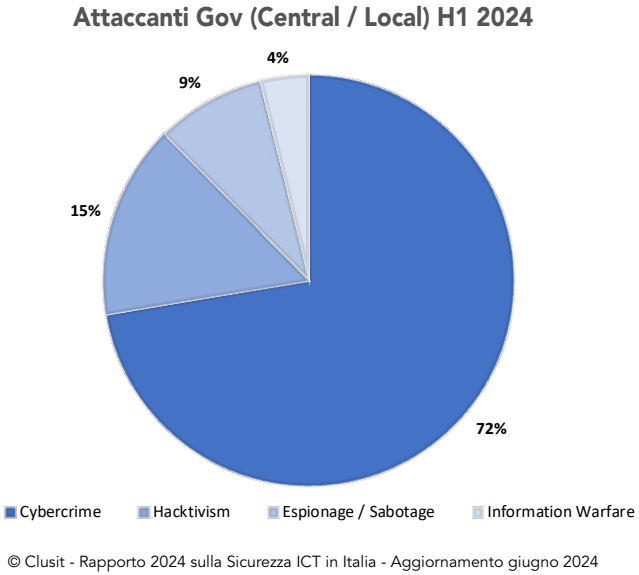
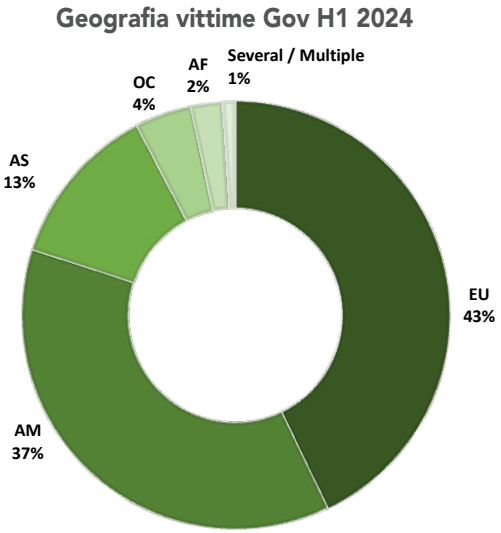


Fig. 15 - Distribuzione degli attaccanti per il settore GOV *(CENTRAL / LOCAL) nel H1 2024*

30%
degli incidenti di Hacktivism nel mondo, colpisce il settore GOV nel I semestre 2024

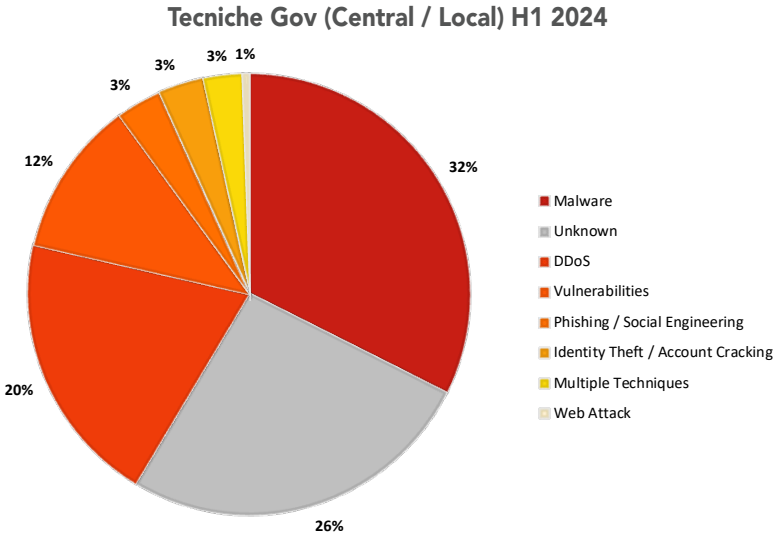
La distribuzione geografica delle vittime (**Fig. 16**) mostra che nel primo semestre 2024 gli incidenti sono cresciuti prepotentemente in Europa, mentre sono rimasti pressoché costanti nel resto del mondo: in particolare nel nostro continente si sono verificati, nei soli primi sei mesi del 2024, quasi tanti attacchi significativi quanti se ne erano verificati nel corso di tutto il 2023.

Per quanto riguarda le tecniche utilizzate (**Fig. 17**) notiamo che gli incidenti generati mediante *DDoS*, tipici dei fenomeni di attivismo, i quali erano più che raddoppiati nel 2023 rispetto al 2022, sono ancora cresciuti: nel primo semestre 2024 infatti se ne sono verificati 42, circa i due terzi di quanti se ne sono verificati in tutto il 2023. Crescono in proporzione ancora di più gli incidenti basati su Malware, *che nel primo semestre 2024 sono stati oltre l'86% di tutti quelli del 2023.*



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Fig. 16 - Distribuzione geografica delle vittime nel settore GOV *(CENTRAL / LOCAL) nel H1 2024*



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Fig. 17 - Distribuzione delle tecniche di attacco nel settore GOV *(CENTRAL / LOCAL) nel H1 2024*

Analisi degli incidenti cyber in Italia

In questa sezione, in continuità con quanto proposto per la prima volta nel nostro Rapporto relativo al 2023, offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti negli scorsi 6 mesi, confrontati con l'andamento dal 2019 in poi.

Nel primo semestre 2024, gli incidenti noti di particolare gravità che hanno coinvolto vittime italiane sono **124**. Complessivamente, tra il 2019 e il 2024 il campione ha incluso **777** eventi in Italia, andando (purtroppo) a costituire una base di analisi statistica ormai consistente e affidabile per fornire degli indicatori significativi per questo Rapporto.

Come si evince dal grafico in **Fig. 18**, il dato H1 2024 è comparabile, con una leggera diminuzione, al numero di incidenti rilevati nello stesso periodo del 2023 (132 attacchi). Non bisogna però abbassare la guardia: lo scorso anno, infatti, gli eventi registrati nella seconda parte dell'anno sono stati superiori a quelli dei primi 6 mesi, con una crescita del 35% circa tra il primo e il secondo semestre.

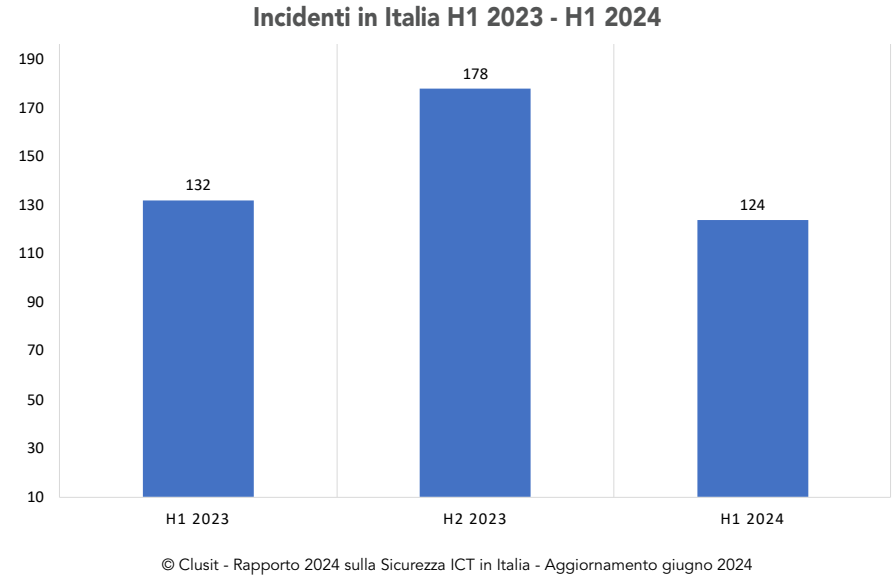


Fig. 18 - Distribuzione dei cyber attacchi in Italia semestre nel periodo H1 2023-H1 2024

Nei primi 6 mesi del 2024, gli attacchi avvenuti con successo contro le realtà del nostro Paese costituiscono il **7,6%** (Fig. 19) del totale degli eventi rilevati a livello globale (1.637). L'incidenza degli incidenti in Italia rispetto al campione complessivo risulta in lieve miglioramento (era pari al 9,6% nel primo semestre 2023 e al 12,7% nel secondo), seppure il numero corposo di eventi continui a evidenziare una situazione di allarme.

7,6%

è la percentuale degli incidenti riferiti all'Italia rispetto al resto del mondo

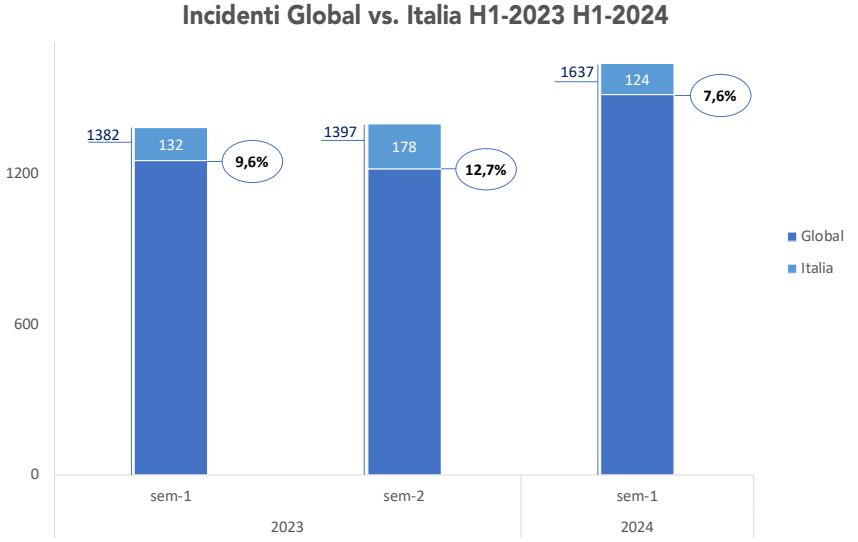


Fig. 19 - L'incidenza degli attacchi in Italia sul campione globale per semestre nel periodo H1 2023-H1 2024

Distribuzione degli attaccanti per tipologia

71%

è la percentuale di incidenti di matrice Cybercrime in Italia rispetto al totale

Per provare a evidenziare alcune tendenze che stanno caratterizzando il panorama degli attacchi 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. 20).

Tra quelli avvenuti In Italia, la maggioranza degli incidenti noti si riferisce alla categoria *Cybercrime*, che rappresenta il 71% del totale (17 punti percentuali in meno

rispetto al campione globale, che si attesta all'88%, vedere Fig. 3).
Il peso percentuale del *Cybercrime* (che nel 2023 rappresentava il 63% del totale degli eventi che interessano l'Italia) torna a crescere, continuando a rappresentare la principale minaccia a cui le organizzazioni – locali e non – sono esposte.

1/3+

degli incidenti Hacktivism nel mondo avviene contro realtà italiane

Conseguentemente, si riduce la quota rispetto al totale (29%) degli incidenti classificati come *Hacktivism* sebbene, in linea con quanto rilevato anche nel 2023, incidono in Italia in quota significativamente maggiore rispetto al campione complessivo, in cui costituiscono solo il 6% del totale. **Oltre un terzo (34%) del totale degli incidenti con finalità "Hacktivism" identificati a livello mondiale è avvenuto ai danni di organizzazioni italiane**. Queste ultime risultano quindi particolarmente vulnerabili a iniziative con finalità dimostrativa, di matrice politica o sociale.
Infine, nel nostro Paese non rilevano in modo significativo gli eventi nelle categorie *Espionage / Sabotage* o *Information Warfare*.

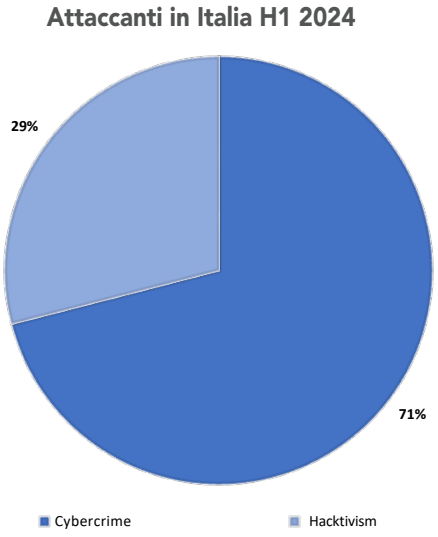


Fig. 20 - Attaccanti in Italia nel primo semestre 2024

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. 21), il primo semestre del 2024 in Italia risulta tristemente più "vivace" nelle variazioni, che interessano – in positivo o in negativo – pressoché tutti i settori.

1° Manifacturing

il settore più colpito da incidenti cyber in Italia nel I semestre 2024

La categoria merceologica per cui si rileva un maggior numero di incidenti cyber in Italia è *Manufacturing* (19% del totale), che per la prima volta occupa il primo posto della triste classifica delle vittime maggiormente prese di mira, superando l'ambito *Governativo / Militare / Law Enforcement* che si attesta al terzo posto (11% del totale). Questo dato può essere almeno in parte spiegato con la minore pressione del fenomeno *Hacktivism* nel primo semestre 2024. D'altro canto, è bene ricordare che nel II semestre 2023 gli attacchi di *Hacktivism* avvenuti con successo sono quasi raddoppiati rispetto al I semestre dello stesso anno: è ancora presto per avanzare pronostici positivi sul 2024 in questo ambito.

Al secondo posto si trova invece la categoria *Multiple Targets* (13% del totale), la cui rilevanza continua progressivamente ad aumentare, in linea con ciò che avviene a livello internazionale, dove occupa un'analoga seconda posizione (con il 16% degli incidenti). Ricordiamo che si tratta di campagne generalizzate utilizzate per causare attacchi non mirati, che continuano però a generare effetti consistenti e su larga scala.

1/4+

degli incidenti al settore Manifacturing nel mondo è avvenuto in Italia

Complessivamente, la ripartizione evidenzia alcune significative differenze rispetto a quella del campione a livello mondiale, in cui il settore manifatturiero raccoglie "solo" il 5% degli incidenti (occupando la settima posizione): ancora una volta, oltre un quarto (28%) del totale degli eventi cyber rivolti al *Manufacturing* globalmente riguarda realtà manifatturiere italiane, ricalcando la peculiarità del tessuto economico del nostro Paese.

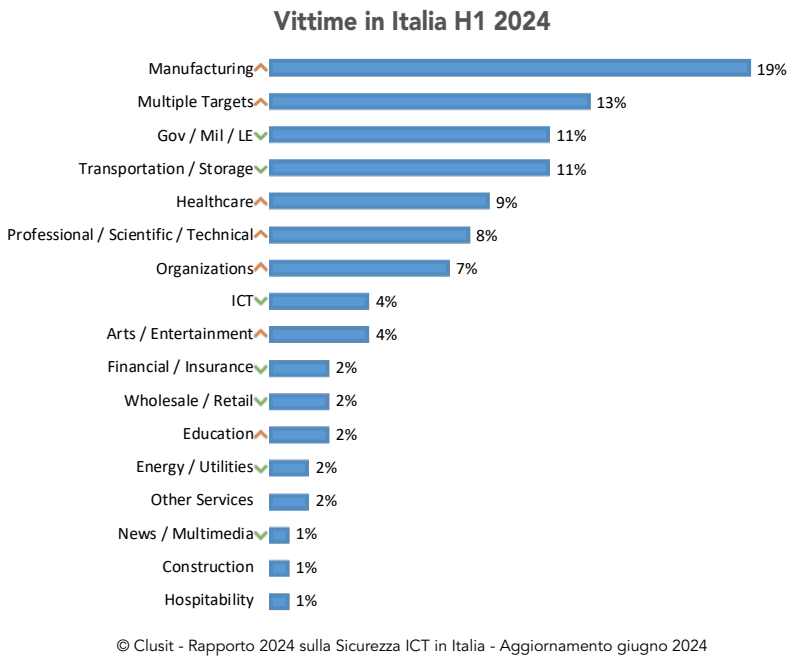


Fig. 21 - Distribuzione delle vittime in Italia H1 2024

La classifica delle categorie interessate in modo significativo dagli incidenti informatici risulta sempre più densa di settori, a evidenziare che gli attacchi colpiscono indistintamente vittime in quasi tutte le aree merceologiche.

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.

Proseguendo nell'analisi, appaiono particolarmente presi di mira anche i settori *Transportation/Storage* (11%), *Healthcare* (9%), che si trova invece al primo posto nel campione globale con il 18% degli incidenti, *Professional / Scientific / Technical* (8%) e *Organizations* (7%). Seguono i comparti *ICT* e *Arts / Entertainment* (entrambi al 4%) e *Financial / Insurance*, che si attesta poco sopra il 2%.

Esaminando l'evoluzione negli anni della distribuzione percentuale degli incidenti, uno dei settori a destare le maggiori preoccupazioni è *Healthcare*: nel primo semestre 2024, gli incidenti rilevati ai danni di questa categoria sono comparabili in numero a quelli individuati nell'intero anno 2023. La crescita rispetto allo stesso periodo dello scorso anno (H1 2023) è pari all'83%, confermando una preoccupante tendenza, identificata anche a livello globale, che vede un significativo aumento dell'attenzione da parte dei cybercriminali nei confronti di questo comparto critico. Anche il settore *Transportation* registra una crescita rispetto al primo semestre 2023, aumentando la propria incidenza di 7,5 punti percentuali, come già avvenuto anche nella seconda parte del 2023.

+83%

è la crescita degli incidenti al settore Healthcare in Italia rispetto al I semestre 2023

A confronto con i primi 6 mesi del 2023 registrano invece una diminuzione le categorie *Gov e Finance/Insurance*, con un decremento rispettivamente di 11 punti percentuali per la prima e di 6,7 p.p. per la seconda. In particolare, il settore finanziario segue la stessa tendenza già riscontrata a livello globale, contando – probabilmente – su un livello di resilienza più elevato della media, indotto anche dalla pressione regolatoria a cui è sottoposto.

-6,7%

è la diminuzione degli incidenti in Italia nel settore Finance/Insurance

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.

Come evidenziato dalla Fig. 22, il malware torna in Italia a occupare prepotentemente il primo posto con il 51% degli eventi, costituendo la tecnica dominante e preferita dai cybercriminali. Si tratta infatti di uno strumento che offre agli attaccanti una grande varietà di opzioni per compromettere i sistemi, spesso difficile da rilevare e con molte possibilità di successo e monetizzazione (per esempio, nel caso di attacchi di tipo ransomware). Nello stesso periodo del 2023, l'incidenza del malware era pari al 31%: la crescita registrata è di circa 20 punti percentuali.

51%

è la percentuale di incidenti censiti causati da Malware in Italia

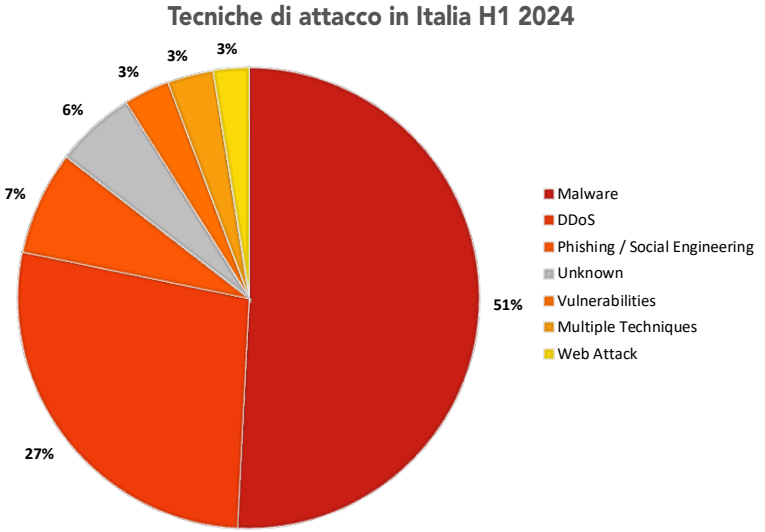


Fig. 22 - Tecniche di attacco in Italia H1 2024

Gli incidenti DDoS, al primo posto nel campione italiano sull'anno 2023, si attestano al 27%, con un peso significativamente maggiore rispetto a quello occupato a livello globale, dove costituiscono solo il 7% 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 la violazione di un sito web, messa in atto tramite attacco DDoS, può essere un mezzo efficace per rendere evidente al pubblico il proprio messaggio di denuncia o protesta.

Al terzo posto (7%) si trovano gli incidenti che fanno leva sulle tecniche di Phishing / Social Engineering, puntando sullo sfruttamento della vulnerabilità del fattore umano. Sebbene in lieve diminuzione, questa tipologia di attacchi continua a costituire una minaccia sostanziale per le organizzazioni, sia a livello italiano sia internazionale, evidenziando la necessità di potenziare e rendere più efficaci le campagne di sensibilizzazione e formazione rivolte ai dipendenti.

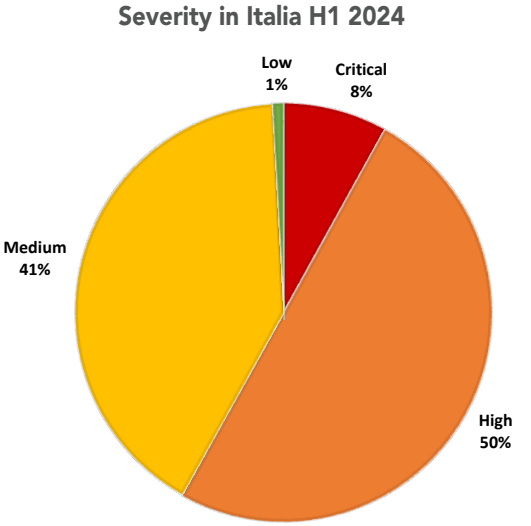
Diminuiscono significativamente gli incidenti di categoria "*Unknown*" (ovvero quelli per i quali le tecniche utilizzate non sono di pubblico dominio), ora al 6% contro il

18% del primo semestre 2023, **aspetto a cui contribuiscono le diverse normative che impongono l'obbligo di segnalazione di alcune tipologie di incidenti**.

Completano il quadro gli incidenti basatati sullo sfruttamento di vulnerabilità, la cui incidenza è come di consueto fortemente inferiore a quella riscontrata da questa tecnica nel campione globale (3% contro il 14% nel campione complessivo). Si attestano al 3% anche Multiple Techniques e Web Attack.

Analisi della "Severity" degli incidenti

Dal punto di vista della *Severity*, il dato italiano (**Fig. 23**) si distacca parzialmente da quello internazionale.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

Fig. 23 - Severity degli attacchi in Italia H1 2024

Se la *severity* High è infatti esattamente in linea con quella globale (50% degli incidenti), quella Critical è invece molto più bassa (8% contro 31%), mentre quella Medium, al contrario, è molto più alta: 41% contro 19%. Gli incidenti a basso impatto sono anche per l'Italia in percentuali trascurabili (1%). In generale quindi, appare un segnale positivo: come già riscontrato nell'anno passato, 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 2023, si rileva un ulteriore diminuzione dell'incidenza della categoria Critical, che passa dal 20% del campione nel primo semestre 2023 al 13% nel campione complessivo dell'anno fino all'8% nei primi 6 mesi del 2024, confermando una tendenza di decrescita che prosegue ormai dal 2022 (Fig. 38).
Al contrario, però, aumentano di 7 punti percentuali gli incidenti con *severity* Alta, che nel 2023 costituivano il 43% del campione, mentre le altre categorie evidenziano un andamento in linea con il passato.

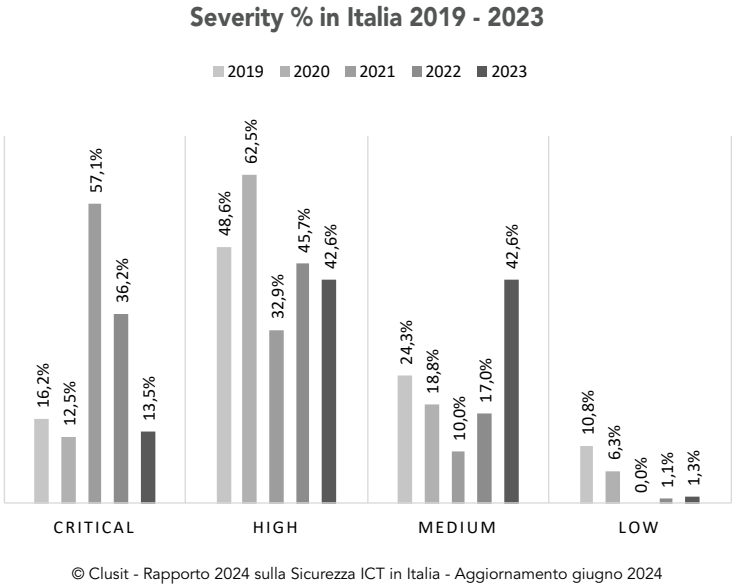


Fig. 24 - Severity degli incidenti in Italia nel periodo 2019-2023

Come ampiamente trattato anche nel Rapporto riferito al 2023, dobbiamo però analizzare queste tendenze nello scenario di insieme, ricordando che gli incidenti italiani costituiscono il 7,6% 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 ten-

dono mediamente a 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. 20**), gli attacchi di categoria Hacktivism che in Italia incidono particolarmente, sono tipicamente associati a una *severity 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 e i limiti.

L'analisi dei principali cyber attacchi 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 a 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 attacco arriva a 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 e 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 attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività

di cyber espionage, che tendono a 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 sotto rappresentati 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[1]. 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 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 e ampie. È quindi utile focalizzarsi su queste ultime e sull'andamento complessivo, piuttosto che su piccole fluttuazioni annuali. Per questo, quest'anno abbiamo aumentato l'attenzione ai fenomeni più significativi, riducendo la disamina di singole variazioni meno rilevanti.

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

Attività e segnalazioni del Servizio Polizia Postale e per la Sicurezza Cibernetica nel primo semestre del 2024

L'importanza della consapevolezza nella sicurezza informatica e nella lotta contro i crimini online

Viviamo in una società sempre più digitale, dove la sicurezza informatica è diventata una priorità fondamentale, non solo per ogni individuo, ma anche per le istituzioni e le aziende. Nell'ambito imprenditoriale, investire nella sicurezza non solo protegge i dati sensibili, ma salvaguarda anche la reputazione aziendale e la fiducia dei clienti. Le minacce informatiche, come attacchi hacker, frodi online e reati contro la persona, sono in continua evoluzione e possono colpire chiunque, indipendentemente dal ruolo ricoperto nella società, dal settore lavorativo o dalla dimensione dell'azienda o dell'amministrazione di appartenenza. La consapevolezza di queste minacce e l'adozione di misure preventive adeguate sono imprescindibili per garantire la continuità operativa e la sicurezza dei dati.

Parallelamente, è fondamentale sensibilizzare su fenomeni spesso sottovalutati o ignorati, come la pedofilia e la pedopornografia. Questi crimini, di cui si parla poco a causa della loro natura particolarmente ripugnante e atroce, tendono a essere psicologicamente allontanati fino a percepirli come inesistenti. Tuttavia, sono purtroppo una realtà presente e pericolosa. La falsa sensazione di sicurezza, alimentata anche dalla carenza di informazione, porta inevitabilmente a una mancanza di vigilanza e a una sottovalutazione del problema. È indispensabile che la società nel suo complesso sia informata e preparata a riconoscere e combattere questi fenomeni.
La creazione di consapevolezza passa attraverso una corretta e capillare informazione. Campagne educative, formazione continua e uso dei media per diffondere conoscenze sono strumenti essenziali.

Tuttavia, l'informazione da sola non è sufficiente. È necessario avviare un confronto attivo e partecipativo tra tutti gli attori coinvolti: aziende, istituzioni, educatori, genitori e giovani. Solo attraverso un dialogo costruttivo e una salda collaborazione è possibile affrontare in modo efficace le insidie e i rischi legati a un progresso tecnologico in continua evoluzione.

In questo contesto, è fondamentale mettere al centro di ogni considerazione sulla sicurezza informatica e il contrasto al crimine informatico l'essere umano, partendo proprio dalle persone più indifese, tra cui i bambini e gli anziani. Proteggere queste fasce vulnerabili della popolazione è il primo passo per creare una società più sicura e consapevole. Ripartendo da qui, il discorso può essere ampliato a tutto il mondo socio-politico ed economico, coinvolgendo le piccole e le grandi aziende.

La Polizia Postale e per la sicurezza cibernetica, con queste premesse, è chiamata a svolgere un ruolo rilevante in questo contesto. La collaborazione, basata sulla consapevolezza, sull'informazione e sul confronto tra le forze dell'ordine, le aziende e la società civile è essenziale per affrontare le sfide della sicurezza informatica e garantire un ambiente digitale sicuro per tutti.

In Italia, la Polizia Postale opera attraverso il Servizio centrale e le sue articolazioni territoriali, che comprendono 18 Centri Operativi per la Sicurezza Cibernetica nei principali capoluoghi di regione e 82 Sezioni Operative per la Sicurezza Cibernetica nelle più importanti province italiane.

Dal mese di maggio 2024, il Servizio Polizia Postale e per la sicurezza cibernetica è stato incardinato nella nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, istituita con il Decreto del 7 febbraio 2024 del Ministro dell'Interno, in collaborazione con il Ministro dell'Economia e delle Finanze. Questa nuova struttura rappresenta un'importante evoluzione nel campo della sicurezza nazionale, progettata per coordinare e ottimizzare le operazioni di sicurezza, inclusa quella cibernetica, a livello nazionale, fornendo supporto tecnico e operativo alle unità territoriali.
Gli altri servizi che, insieme al Servizio Polizia Postale, formano la nuova direzione sono:

- **Servizio Affari Generali**: si occupa della gestione amministrativa e contabile, della pianificazione strategica e della gestione delle risorse umane e logistiche; coordina le attività dei vari servizi della Direzione Centrale, garantendo un'azione unitaria e coerente.
- **Servizio Polizia Scientifica**: responsabile delle attività di polizia scientifica, questo Servizio si occupa della raccolta, analisi e conservazione delle prove scientifiche. Supporta le indagini con tecniche avanzate di analisi forense.
- **Servizio per la Sicurezza Cibernetica del Ministero dell'Interno**: assicura la protezione delle reti e dei sistemi informatici del Ministero dell'Interno, garantendo la sicurezza delle comunicazioni e delle operazioni interne.

Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)

La tutela dei diritti di bambini e adolescenti rappresenta una priorità per la Polizia di Stato, e richiede necessariamente un'analisi delle nuove e diverse minacce emergenti. È fondamentale adottare tecnologie avanzate e un approccio metodologico e operativo che si allinei all'evoluzione dei mezzi di comunicazione, i quali aprono nuove frontiere nella conoscenza e nella socializzazione.

Le competenze della Specialità, in merito alla protezione dei minori, hanno subito un significativo ampliamento grazie a nuove disposizioni normative volte a rafforzare il sistema di tutele. Questo approccio si concentra anche sulla prevenzione e sul contrasto a fenomeni come il cyberbullismo, nonché alle *challenge* — sfide pericolose diffuse sui social media — che aumentano notevolmente i rischi per il benessere dei giovani online.

I nuovi media, i social network e le applicazioni di messaggistica sono considerati dai ragazzi luoghi primari di socializzazione, occasioni per avviare e curare relazioni sociali. Tuttavia, i rischi a cui i minori sono esposti in rete sono molteplici e preoccupanti. Possono diventare vittime di *grooming*, un fenomeno in cui pedofili online li spingono a produrre immagini intime. Ciò li espone a minacce legate alla pedopornografia, al *revenge porn* e al *sexting*. Inoltre, potrebbero subire prepotenze, scherzi e molestie da parte di coetanei durante il gioco online (cyberbullismo). Inoltre possono anche affrontare violazioni della privacy o cadere vittime di truffe informatiche, come i *romance scam*.

In rete si possono trovare anche suggerimenti e luoghi virtuali di solidarietà tra coetanei, che possono offrire supporto emotivo, ma che a volte si trasformano in spazi dove condividere stati d'animo depressivi, atti di autolesionismo o disturbi alimentari. La rete facilita l'accesso a contenuti inappropriati, rendendo questi ultimi facilmente accessibili anche ai più piccoli, trasformandoli in manuali per esplorare la sessualità, spesso in modo prematuro. In alcuni casi, i ragazzi possono essere coinvolti in gruppi chiusi dove si scambiano immagini di ogni genere, inclusi contenuti di violenza estrema.

In qualità di organo del Ministero dell'Interno, il Servizio Polizia Postale detiene competenze istituzionali esclusive, riconosciute dalla legge istitutiva del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), responsabile del contrasto e della prevenzione dei reati di sfruttamento sessuale dei minori online. Questo Servizio opera utilizzando metodologie investigative all'avanguardia e mantiene un ruolo di coordinamento a livello internazionale, interagendo con omologhi esteri e, a livello nazionale, con i 18 Centri Operativi per la Sicurezza Cibernetica (COSC) e le 82 Sezioni Operative (SOSC) della Specialità. Sono stati attivati, inoltre, protocolli operativi di collaborazione con enti del terzo settore impegnati nel contrasto allo sfruttamento dei minori.

La Polizia Postale partecipa anche a numerosi tavoli di collaborazione interistituzionale per la tutela dei minori, tra cui il *Safer Internet Center Italy*, in partnership con il Ministero dell'Istruzione e del Merito, l'Osservatorio Nazionale per l'Infanzia e

l'Adolescenza, nonché l'Osservatorio per la Prevenzione e il Contrasto della Pedofilia e della Pornografia Minorile, in collaborazione con il Ministero della Famiglia. Il Gruppo di Lavoro dedicato alle Sfide e Opportunità del Gaming, istituito dal Dipartimento per la Trasformazione Digitale, testimonia ulteriormente che fenomeni complessi e multidimensionali richiedono sinergie per essere compresi e affrontati efficacemente.

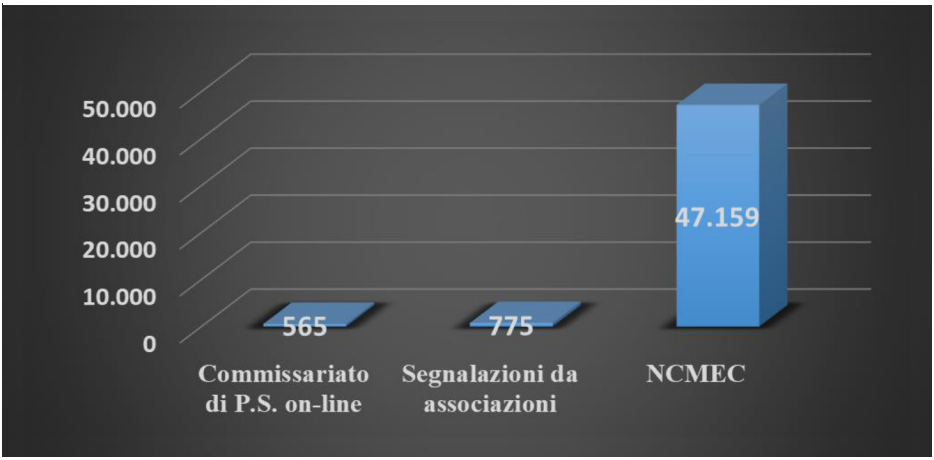
Considerando la natura transnazionale di questi reati, è diventato imperativo incentivare, attraverso gli uffici di Europol ed Interpol, lo scambio informativo nei canali di cooperazione internazionale, al fine di promuovere a livello nazionale un'azione coordinata tra gli uffici della Specialità, distribuiti su tutto il territorio, con l'obiettivo di identificare autori e vittime di abusi. Alla priorità di identificazione delle vittime si dedica un'area investigativa specifica, in cui specialisti svolgono attività di analisi e gestione dei file multimediali illeciti all'interno della Banca Dati ICSE (*International Child Sexual Exploitation Database*), accessibile tramite l'agenzia Interpol e integrata dalle segnalazioni di forze di polizia di tutto il mondo.

Le informazioni necessarie per l'analisi e le indagini provengono anche dall'Unità di Informazione Finanziaria (U.I.F.) della Banca d'Italia, relativa a sospetti pagamenti per la commercializzazione di materiale legato allo sfruttamento sessuale dei minori su internet. Le indagini condotte sulla scorta delle numerose segnalazioni ricevute quotidianamente da diverse fonti hanno portato a risultati operativi significativi. Nel primo semestre del 2024, sono stati identificati **619** soggetti e sono stati eseguiti **532** provvedimenti di perquisizione.

L'impegno preventivo volto a contrastare la diffusione di foto e video a contenuto sessuale che coinvolgono minori di 18 anni, attraverso le attività di monitoraggio del C.N.C.P.O. in collaborazione con le articolazioni territoriali della Polizia Postale, ha registrato un significativo incremento rispetto allo stesso periodo del 2023. Questo aumento riguarda sia il numero di siti esaminati che il numero di siti inseriti in blacklist, segnalati da enti accreditati e ONG per la presenza di contenuti illeciti[1].
In particolare, le procedure relative all'applicazione dei sistemi di "filtraggio" del web, attuate in sinergia con i provider coinvolti, vengono costantemente aggiornate per garantire conformità ai più elevati standard internazionali di navigazione sicura per gli utenti. Ciò è reso possibile anche grazie a un'analisi approfondita delle diverse fenomenologie criminali rilevate dagli operatori in questo settore.

[1] Il C.N.C.P.O. si occupa del monitoraggio e della raccolta delle segnalazioni relative ai siti che diffondono materiale pedopornografico su Internet, in conformità con la Legge n. 38/2006. Inoltre, è responsabile della creazione e della gestione di una ***blacklist*** destinata agli Internet Service Provider, i quali sono obbligati a impedire ai propri utenti l'accesso ai siti inclusi in tale lista.

SEGNALAZIONI - FONTI dal 1° gennaio al 30 giugno 2024



Numero di segnalazioni e relative fonti per contenuti pedopornografici o episodi di grooming.
Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

Nel periodo in esame, sono stati monitorati **15.170** spazi web, di cui **2.759** sono stati inseriti nella *blacklist* e oscurati, con l'obiettivo di impedire l'accesso a tali contenuti per gli utenti italiani.

Pedopornografia e adescamento primo semestre 2024

CNCP	Primo Semestre 2023	Primo Semestre 2024
Casi trattati	1.440	1.418
Persone indagate	579	619
Perquisizioni	403	532
Siti in Black List	2.675	2.759
Siti visionati	14.054	15.170

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024


Ministero dell'Interno
Dipartimento della Pubblica Sicurezza
Servizio Polizia Postale e delle Comunicazioni

polizia delle comunicazioni

STOP !!

PAGINA INTERDETTA DAL CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA SULLA RETE INTERNET

Il tuo browser sta tentando di raggiungere un sito Internet contenente immagini e filmati pedopornografici.
La detenzione, la distribuzione, la produzione, la commercializzazione di tale materiale prevedono l'applicazione di gravi sanzioni in base alla legge penale italiana e sono perseguibili anche ad opera di forze di polizia estere.

Nessun dato relativo al tuo ip address od altra traccia utile ad identificarti verrà registrato.

L'inibizione dell'accesso a questo sito è prevista dalla legge n. 38/2006 ed è stata operata al fine di impedire la commissione e la documentazione di violenze sessuali a minori degli anni diciotto. Questo servizio di protezione della navigazione sulla rete Internet è predisposto grazie alla collaborazione tra il "Centro Nazionale per il Contrasto alla Pedopornografia sulla rete Internet" e gli Internet Service Provider italiani.

Your browser is trying to contact an Internet site that is used in connection with distribution of photos depicting sexual abuse of children. This is a criminal offence in accordance with the italian penal code.

No information about your ip address or any other information that can be used to identify you will be stored when you this page is displayed.

The purpose of blocking access to these pages is only to prevent the commission of criminal dissemination of documented sexual abuse, and to prevent the further exploitation of children who have already been abused and photographed. This is a prevention service provide from italian Internet Service Provider and the italian "National Centre for Combating On-line child pornography".

EUROPOL

C.I.R.C.A.M.P.
Cospol Internet Related Child Abusive Material Project

Il filtro anti distribuzione del materiale pedopornografico è parte dell'iniziativa "CIRCAMP" (Cospol Internet Related Child Abusive Material Project).
Tale progetto è stato avviato dalla "Task-Force" dei capi delle polizie europee per combattere la criminalità organizzata che gestisce il commercio di materiale prodotto mediante l'utilizzo sessuale dei minori.
The Child sexual abuse anti-distribution filter in part of the "CIRCAMP" (Cospol Internet Related Child Abusive Material Project). The project is initiated by the european police chief task-force - aimed at combating organized criminal group behind commercial sexual exploitation of children.

Pagina di blocco per un sito con contenuti pedopornografici.

Alla luce degli strumenti normativi[2] che consentono di condurre indagini sotto copertura in ambito online, il personale specializzato degli Uffici territoriali e del CNCPO ha realizzato numerose operazioni volte a contrastare i reati relativi allo sfruttamento sessuale dei minori, sia nel *dark web* che nel *deep web*. Tali attività sono state effettuate in sinergia con gli Uffici territoriali e frequentemente hanno coinvolto le principali agenzie estere attive nel monitoraggio e nello scambio di informazioni, in particolare Europol, per garantire un adeguato coordinamento delle operazioni investigative, talvolta svolte in modalità undercover.

In particolare, le indagini condotte in collaborazione con le controparti estere e con le agenzie europee e internazionali hanno rivelato forme di sfruttamento e abuso minorile sempre più violente e subdole. Tra le numerose operazioni eseguite da questa Specialità, merita particolare attenzione quella che ha permesso di accertare, grazie alla cooperazione con l'*Homeland Security Investigations* (*HSI*) statunitense, l'emergere del preoccupante fenomeno del c.d. "*live streaming child abuse*".

[2] Ai sensi dell'art. 14. L. n. 269/98 (Attività d'indagine in modalità sotto copertura online)

L'indagine condotta dal C.N.C.P.O. e dal Centro Operativo per la Sicurezza Cibernetica di Bologna ha portato alla luce gravi atti di abuso sessuale su minori, perpetrati in diretta online e a pagamento, da parte degli utenti. Inoltre, è emerso il coinvolgimento di due genitori, uno di origine filippina, i quali, in cambio di una somma di denaro, offrivano sessioni di live streaming di abusi sessuali sui propri figli minori. Gli elementi raccolti durante l'indagine sono stati ritenuti sufficienti per l'emissione di misure restrittive nei confronti di entrambi i genitori coinvolti.

Adescamento online

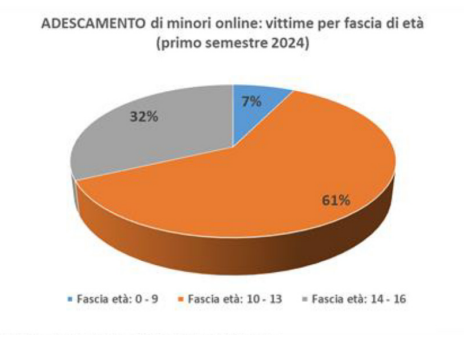
Il rischio che bambini e preadolescenti possano essere vittime di attenzioni sessuali da parte di adulti durante la navigazione in rete rappresenta una problematica di crescente preoccupazione, richiedendo un'attenzione costante e una cooperazione attiva tra genitori, educatori e autorità competenti. È fondamentale implementare strategie efficaci di prevenzione, che forniscano ai minori le competenze necessarie per identificare e segnalare comportamenti inappropriati.
Tra i principali contesti di contatto tra minori e adulti predatori, emergono con sempre maggiore incidenza i social network e i videogiochi, sia attraverso applicazioni mobili che tramite console di gioco connesse a Internet. Questi ambienti virtuali, sebbene offrano opportunità di socializzazione e intrattenimento, possono anche esporre i minori a rischi significativi.

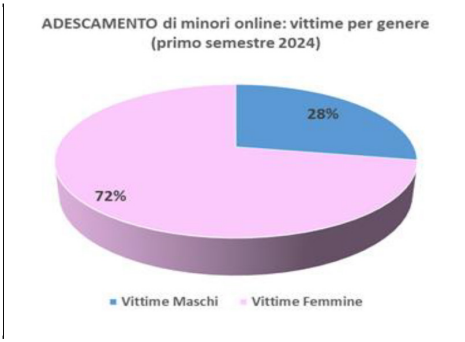
Un'analisi dei dati nel corso degli anni consente di evidenziare le evoluzioni nel panorama del fenomeno del *grooming*. Nonostante il numero complessivo di casi di adescamento si mantenga relativamente stabile rispetto agli anni precedenti, è importante segnalare che, dopo una lieve flessione registrata nel corso dell'anno scorso, si osserva un incremento dell'incidenza di tali atti nei primi sei mesi del 2024. Questo andamento sottolinea l'urgenza di rafforzare le misure di protezione e sensibilizzazione, al fine di salvaguardare la sicurezza dei minori nel contesto digitale.

ADESCAMENTO MINORI online	TOTALE casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-16 anni
Primo Semestre 2022	210	18	115	77
Primo Semestre 2023	184	20	106	58
Primo Semestre 2024	191	14	116	61

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

Appaiono in diminuzione i casi relativi ai bambini adescati di età inferiore ai 9 anni, mentre un sensibile aumento si registra per la fascia di età preadolescenziale (10-13 anni).
La lettura dei dati evidenzia che l'incidenza maggiore dei casi risulta nella fascia di età preadolescenziale e ai danni di vittime prevalentemente di sesso femminile.





Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

Tra le recenti attività operative sotto copertura condotte dal Centro Operativo per la Sicurezza Cibernetica (COSC) del Veneto, si segnala l'Operazione Viper, realizzata con il coordinamento di Europol. Questa indagine ha avuto come obiettivo gruppi attivi nello scambio di materiali pedopornografici sulla piattaforma di messaggistica Viber, focalizzandosi su contenuti realizzati mediante sfruttamento di minori di età inferiore ai 18 anni. Durante l'operazione, è emerso un allarmante interesse degli utenti verso il materiale che ritrae torture inflitte alle giovani vittime. L'inchiesta ha coinvolto 44 Paesi, attuando una strategia di azione congiunta con le autorità straniere, culminando con l'esecuzione di 57 decreti di perquisizione sul territorio nazionale. Questo ha portato all'arresto di 28 indagati per detenzione di ingente quantità di materiale pedopornografico e alla denuncia di ulteriori 24 soggetti in stato di libertà.
Un'ulteriore conferma dell'estesa diffusione di contenuti pedopornografici è fornita dall'Operazione "Ontario 3", condotta dal Centro Operativo per la Sicurezza Cibernetica di Milano in collaborazione con le forze di polizia canadesi e il C.N.C.P.O.. Questa operazione ha riguardato la piattaforma Kik, nota per lo scambio di contenuti pornografici coinvolgenti minori. Complessivamente, sono stati identificati **112** utenti, di cui **94** denunciati e **17** arrestati per detenzione di materiali di contenuto pedopornografico.

Nel contesto delle attività di contrasto, interessanti spunti operativi sono emersi dall'operazione sotto copertura "*Meet up 3*", condotta dal Centro Operativo di

Torino in canali dedicati alla diffusione di contenuti legati allo sfruttamento sessuale di minori, anche attraverso abbonamenti a pagamento. Durante la fase operativa, sono stati arrestati **2** soggetti e denunciate **11** persone in stato di libertà.

In modo analogo, l'Operazione "Tabu" del COSC di Catania ha investigato una rete di soggetti dediti allo scambio di materiale pornografico realizzato tramite l'utilizzo di minori. Le attività, coordinate dal C.N.C.P.O., hanno portato alla denuncia di **24** persone di cui **9** tratte in arresto, tutti accusati di detenzione e divulgazione di materiale pedopornografico.

Particolarmente efficace si è rivelata la collaborazione con le autorità spagnole riguardante un'applicazione per dispositivi Android, denominata "Mundo CAPAX", contenente materiale pornografico realizzato con minori. L'operazione di polizia che ne è scaturita e che ha preso il nome di "Malo Mundo" ha permesso di rintracciare diversi autori degli accessi, segnalati alla Procura della Repubblica di Roma, che ha emesso **22** decreti di perquisizione per detenzione di materiale pedopornografico. L'azione condotta dai Centri Operativi per la Sicurezza Cibernetica e dalla Polizia Postale ha portato all'indagine di **15** persone in stato di libertà e all'arresto immediato di **5** soggetti in flagranza di reato.

Fra le diverse attività di polizia giudiziaria, spicca la complessa operazione di identificazione e localizzazione di un individuo responsabile di oltre **50** casi di adescamento online di ragazze minorenni, contattate tramite social network e piattaforme di messaggistica, utilizzando molteplici alias. L'obiettivo era ottenere immagini sessualmente esplicite tramite minacce e ricatti. Questa attività, condotta dal COSC di Bologna in sinergia con il C.N.C.P.O., ha portato all'emissione di un Mandato di Arresto Europeo nei confronti del soggetto, il quale, spostatosi in vari Paesi europei, è stato localizzato in Irlanda ed arrestato grazie a operazioni di cooperazione internazionale.

Sextortion – Vittime minori

Un approccio precoce e massiccio all'uso della tecnologia sembra avere effetti negativi sullo sviluppo cognitivo, sociale ed emotivo dei bambini, dando origine a una serie di problematiche. In particolare, durante la preadolescenza, si manifestano comportamenti violenti, una mancanza di rispetto verso l'autorità, comportamenti disprezzanti verso gli altri e una sessualità precoce.

In rete, i giovani possono facilmente accedere a contenuti inadeguati e si sentono liberi di esplorare autonomamente, senza la supervisione di adulti. Questo porta a esperienze intime con coetanei e sconosciuti, aumentando il rischio di imbattersi in individui senza scrupoli. Si tratta di una fenomenologia particolarmente pervasiva che

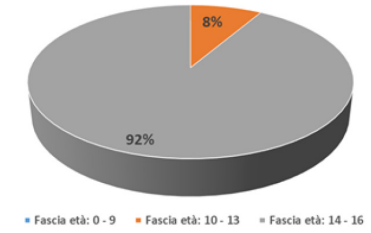
colpisce il mondo giovanile, facendo leva sulle fragilità e le necessità di esplorazione che caratterizzano questa fase della vita.

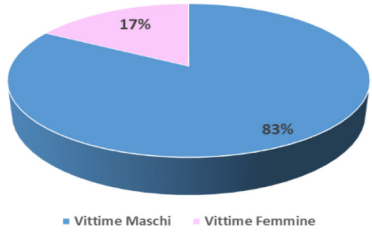
In passato, le problematiche riguardavano prevalentemente il mondo degli adulti, mentre oggi l'attenzione si sposta anche sugli adolescenti. Questo cambiamento produce effetti lesivi e destabilizzanti, poiché le vittime, spesso giovani, si sentono colpevoli per essersi fidate di sconosciuti e nonostante si trovino a fronteggiare richieste di denaro da parte di estorsori, spesso non chiedono aiuto a genitori o coetanei per imbarazzo o vergogna.

La quasi totalità dei casi registrati riguarda minori di età compresa tra i 14 e i 17 anni, con una prevalenza di maschi.

SEXTORTION Vittime minori	TOTALE casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Primo semestre 2022	**41**	0	8	33
Primo semestre 2023	**66**	1	10	55
Primo semestre 2024	**59**	0	5	54

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024





Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

È fondamentale che gli adolescenti siano adeguatamente informati sui rischi legati all›invio di immagini o video privati, nonché sulle conseguenze legali e psicologiche della *sextortion*. Allo stesso modo, è essenziale che genitori ed educatori sviluppino le competenze necessarie per affrontare questo fenomeno in modo efficace.

La *sextortion*, per la sua particolare insidiosità, rappresenta una minaccia altrettanto grave rispetto ad altri reati che colpiscono i minori, considerando il profondo coinvolgimento emotivo e le conseguenze negative che infligge alle vittime. La serietà di questa problematica ha spinto la Polizia Postale a organizzare giornate informative e di sensibilizzazione sui pericoli della rete, rivolte a studenti, genitori, insegnanti e operatori del settore. Queste iniziative hanno lo scopo di promuovere la sicurezza online, potenziare le conoscenze e rafforzare la collaborazione tra le istituzioni coinvolte.

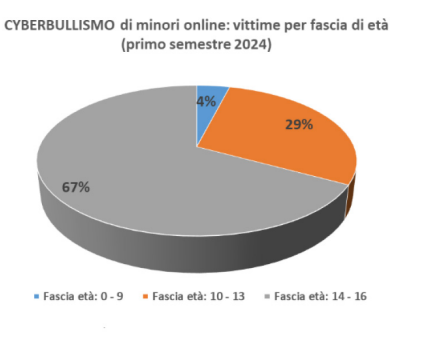
Cyberbullismo

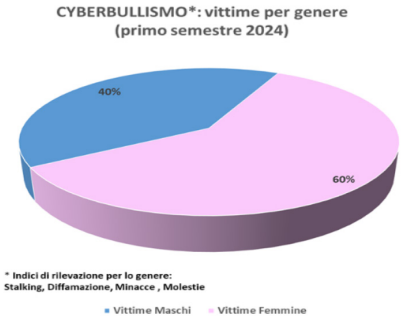
Per affrontare il fenomeno del bullismo e del cyberbullismo, sia nel mondo reale che in rete, il 14 giugno 2024 è entrata in vigore la Legge 17 maggio 2024, n. 70. Questa legge ha introdotto nuove misure preventive e disposizioni specifiche mirate a proteggere le vittime di tali comportamenti.
Dall'analisi dei dati, si evidenzia nel primo semestre del 2024 un aumento dei casi di bullismo e cyberbullismo, con un incremento significativo nella fascia di età compresa tra 10 e 13 anni. Ciò dimostra che l'età dei minori che accedono a Internet si è notevolmente abbassata, rendendo essenziale l'attività di informazione e sensibilizzazione nelle scuole.
La Polizia Postale ha intensificato le attività di sensibilizzazione nelle scuole, creando occasioni di formazione anche per i genitori, raggiungendoli nei luoghi di lavoro. Inoltre, è stato sviluppato un programma di comunicazione mirato al personale scolastico, con specifici momenti di formazione. Queste azioni preventive si affiancano alle investigazioni e alle misure repressive, adottando un approccio multidisciplinare che vede la collaborazione tra diversi "*stakeholders*" nella tutela dei minori come elemento centrale.

Nel primo semestre del 2024, sono state esaminate 176 denunce di cyberbullismo, con una predominanza di casi che ha coinvolto minori in età adolescenziale (14 -17 anni) e di sesso femminile, perpetrati da adolescenti nella fascia di età 15-17 anni. Sebbene il numero complessivo dei casi sia in aumento, si osserva una maggiore propensione dei ragazzi di età compresa tra 14 e 17 anni a cercare supporto e tutela di fronte a aggressioni virtuali dai coetanei, suggerendo un incremento della consapevolezza tra i giovani.
Tuttavia, persiste un utilizzo meno frequente della querela riguardo episodi di cyberbullismo, e si ricorre spesso a strategie di mediazione guidata da adulti, soprattutto nei casi che coinvolgono vittime e bulli non imputabili, ovvero minori di età inferiore ai 14 anni. In questa fascia di età, infatti, emergono con particolare intensità situazioni di rivalità, conflitto e antipatia, amplificate dal potere diffusivo delle nuove tecnologie.

CYBERBULLISMO Vittime minori	TOTALE casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Primo semestre 2022	**160**	11	41	108
Primo semestre 2023	**164**	5	35	124
Primo semestre 2024	**176**	7	51	118

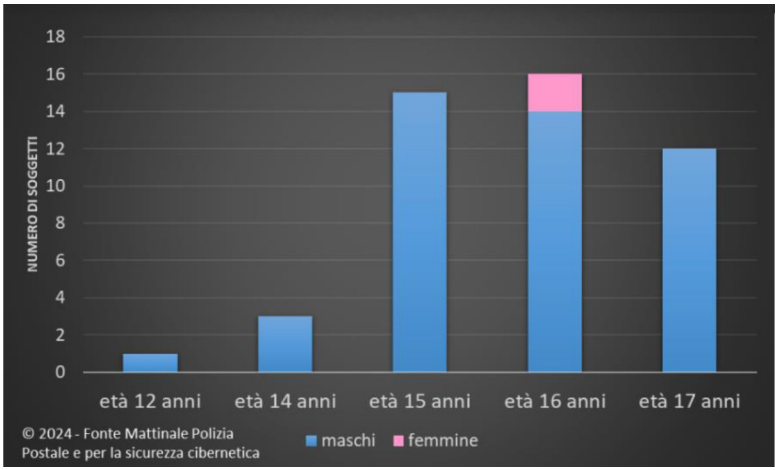
Fonte - Polizia Postale e per la sicurezza cibernetica © 2024





Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

PRIMI SEI MESI DEL 2024 - Minori indagati per cyberbullismo



Come negli anni precedenti, continuano ad arrivare segnalazioni tramite canali informali e attraverso il portale istituzionale www.commissariatodips.it, in cui si richiede supporto per la gestione di aggressioni virtuali, esclusioni e difficoltà relazionali tra ragazzi di età inferiore ai 14 anni. Tali segnalazioni provengono dalla collaborazione con il privato sociale attivo nella tutela dei minori.

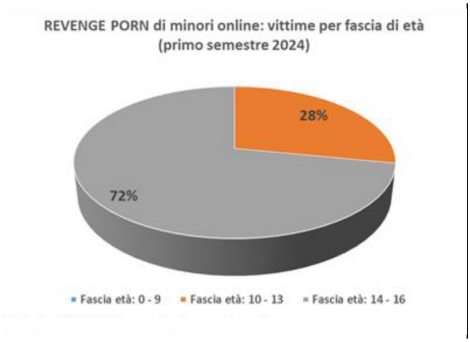
Revenge Porn – Vittime minori

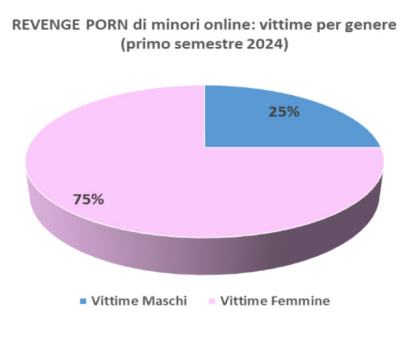
Il *revenge porn* è un fenomeno che si verifica quando contenuti intimi, come foto o video a carattere sessuale, vengono divulgati senza il consenso della persona coinvolta, spesso da un ex partner con l'intento di umiliare o vendicarsi. Questo problema ha assunto proporzioni allarmanti, soprattutto con l'aumento dell'accesso dei minori a Internet, che avviene a una età sempre più precoce. Analizzando i dati, emerge un incremento preoccupante delle denunce di *revenge porn* nel primo semestre dell'anno corrente, con una crescita significativa tra gli adolescenti di età compresa tra i 14 e i 17 anni, di cui il **75%** delle vittime sono ragazze.

Durante il primo semestre del 2024, è stata conclusa un'indagine articolata e complessa dal C.O.S.C. di Bologna, mirata all'identificazione e localizzazione di un soggetto responsabile di oltre **50** casi di adescamento online di adolescenti. Queste ragazze venivano contattate attraverso i social network e le piattaforme di messaggistica, utilizzando vari nickname, con l'obiettivo di estorcere loro immagini sessualmente esplicite mediante minacce e ricatti. Grazie a un'operazione di cooperazione internazionale, si è giunti all'emissione di un Mandato di Arresto Europeo, che ha portato all'arresto del responsabile in Irlanda.

REVENGE PORN VITTIME MINORI	TOTALE casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Primo Semestre 2022	**15**	1	2	12
Primo Semestre 2023	**16**	0	2	14
Primo Semestre 2024	**32**	0	9	23

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024





Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

Unità Di Analisi Crimine Informatico (U.A.C.I)

In un mondo sempre più dominato dalla tecnologia, i rapporti umani, i fenomeni criminali, così come ogni aspetto della vita quotidiana, assumono connotati di complessità in cui le peculiarità dell'essere umano si legano strettamente al mezzo informatico, costruendo una realtà sempre più articolata in cui persino bambini e ragazzi diventano protagonisti di rischi e minacce che attentano alla loro crescita.

In tale complessità, fenomeni come l'adescamento online di minori e il cyberbullismo, per esempio, richiedono un approccio multidisciplinare nel quale le azioni di repressione debbano adeguatamente integrarsi con quelle di sensibilizzazione e di prevenzione, usando linguaggi e metodi che attingono anche alla psicologia e alle scienze sociali.

L'Unità di Analisi del Crimine Informatico (UACI) del Servizio Polizia Postale e per la sicurezza cibernetica è un'équipe composta da psicologi della Polizia di Stato, che svolge sin dagli anni 2000 un'opera di affiancamento alle principali attività svolte nella direzione della protezione dei minori e delle vittime fragili dai rischi online.

Le principali attività svolte dall'Unità hanno lo scopo di massimizzare l'efficacia delle attività operative, valorizzare l'impegno degli operatori e capitalizzare la conoscenza criminologica dei fenomeni per aumentare la consapevolezza della società civile in merito a questi rischi.

L'UACI, quindi, si occupa dell'analisi dei dati di contrasto delle forme di aggressione online in danno di minori e di vittime fragili, per la descrizione, lo studio e la valutazione dei fenomeni, anche in collaborazione con enti pubblici, accademici e organizzazioni private di ricerca. Effettua attività di profiling e supporto investigativo per reati

di aggressione tecnomediata ai minori e a vittime fragili, violenza di genere, cyberterrorismo, hate speech, cyberbullismo, ecc. Provvede a fornire supporto operativo nell'approccio alle vittime in casi di violenza online ad alto impatto emotivo; assicura ascolto, sostegno psicologico e formazione al personale esposto a materiale ad alto impatto emotivo (pedopornografia, immagini violente, esecuzioni, ecc.) attraverso l'ideazione, la strutturazione e la realizzazione di specifici percorsi progettuali. Supervisiona contenuti e strategie comunicative nelle iniziative di sensibilizzazione ai rischi di Internet per minori, caregiver e operatori del privato e pubblico sociale; realizza iniziative di formazione del personale in riferimento ai correlati psico-criminologici dei fenomeni di cybercrime.

Sezione Operativa

Nel corso del primo semestre del 2024, l'attività svolta dalla Polizia Postale nel contrasto dei reati contro la persona, commessi attraverso l'utilizzo di dispositivi informatici e social network, si è rivelata incisiva. Lo sforzo operativo si è concentrato, da un lato, sul monitoraggio attivo degli spazi web, in particolare delle piattaforme social, finalizzato alla prevenzione, e, dall'altro, allo studio delle varie fenomenologie per un'azione di contrasto più efficace.

Con riferimento a questa tipologia di reati, particolare attenzione è stata rivolta al *revenge porn*, al *cyberstalking* e a tutte le forme di aggressione esplicitamente previste dalla recente normativa denominata "codice rosso", che ha introdotto una maggiore tempestività nella risposta giudiziale, orientandosi verso un'azione di protezione più rapida per le vittime.

Anche per le cosiddette truffe romantiche (*romantic scam*), l'attività di contrasto è stata particolarmente attenta, considerando anche le delicate conseguenze psicologiche che tali fenomeni producono nella vita personale delle vittime dopo la scoperta del raggiro, tra cui frustrazione, inadeguatezza e vergogna.
L'età delle vittime attratte dai falsi corteggiatori sui social si aggira intorno ai 50 anni e spesso coinvolge donne di diversa estrazione sociale, che subiscono danni psicofisici oltre a quelli economici. L'aumento dei casi segnalati è certamente collegato all'uso sempre crescente dei social network e dei siti di incontri.

Lo studio analitico, alla luce di recenti indagini, ha evidenziato che gli autori, pur provenendo da paesi nordafricani, in particolare Nigeria e Costa d'Avorio, operano in modo strutturato sul territorio italiano e mantengono collegamenti operativi con Paesi dell'Unione europea, principalmente la Francia, esportando ingenti somme di denaro anche attraverso servizi di Money Transfer verso i loro paesi d'origine.

Tale connotazione transnazionale ha reso necessario incentivare, tramite gli uffici di Europol e Interpol, lo scambio informativo nei canali di collaborazione internazionale, finalizzato a un'azione di coordinamento capillare a livello nazionale delle attività svolte dagli uffici della Polizia Postale dislocati su tutto il territorio.

Le indagini effettuate dalla Specialità in questo ambito sono dirette non solo a identificare e perseguire i responsabili dei reati, ma anche a intervenire tempestivamente per rimuovere contenuti dal web o, quanto meno, limitarne la diffusione massiva.

Si segnala infine che, con l'entrata in vigore della Legge 24 novembre 2023 n. 168, sono state introdotte importanti novità nel contrasto alla violenza sulle donne e alla violenza domestica, potenziando procedure e strumenti per la tutela anticipata delle vittime. In particolare, questa legge ha ampliato la gamma di reati per i quali è possibile richiedere l'applicazione dell'ammonimento del Questore.

È stata anche introdotta la possibilità, da parte della Polizia giudiziaria, di «arresto facoltativo in flagranza differita», previsto per specifiche tipologie di reati, tra cui i maltrattamenti e gli atti persecutori (stalking). Tale impianto normativo ha permesso un significativo impulso sia alle attività operative che a quelle di carattere preventivo, finalizzate al contrasto del fenomeno, anche in una fase antecedente alla denuncia di reato, con risultati apprezzabili.

Numerose sono state le iniziative rivolte agli operatori del settore, ai dirigenti e ai funzionari delle articolazioni territoriali dei COSC e delle SOSC, finalizzate alla sensibilizzazione sulle metodologie operative nella gestione dei casi sin dalle prime fasi e all'aumento della sensibilità nel riconoscere tempestivamente i cosiddetti "reati-spia".

Particolare attenzione è stata prestata a specifiche iniziative di prevenzione e contrasto agli atti intimidatori nei confronti della categoria dei giornalisti e ai servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e YouTube), per arginare la diffusione del linguaggio d'odio (hate speech), in costante collaborazione con l'Osservatorio per la Sicurezza contro gli Atti Discriminatori.

La partecipazione al 13° *Meeting dell'High Level Group* - sull'hate speech e i reati d'odio è stata proficua; oltre a riassumere le attività svolte da vari Stati dell'Unione, ha rappresentato un contesto fertile per scambi informativi e per nuove iniziative di contrasto a tali fenomeni.

Sono state gestite numerose segnalazioni riguardanti intenti suicidari, pervenute tramite il Commissariato di P.S. online, diversi social network e il Servizio di Cooperazione Internazionale. Questo fenomeno ha registrato un significativo aumento, dando luogo a interventi di soccorso pubblico. Durante la fase finale delle operazioni di soccorso, hanno collaborato anche uffici di altre Forze di Polizia su tutto il territorio nazionale. In alcune situazioni, sono stati attivati sistemi di tracciamento (noti come positioning) associati ai dispositivi elettronici, come *smartphone*, utilizzati nel contesto delle segnalazioni.

Sextortion

La sextortion è un fenomeno di estorsione sessuale che avviene principalmente online. Gli estorsori, spesso attraverso l'uso di falsi profili sui social media, manipolano le vittime raccogliendo informazioni personali o facendole sentire in situazioni compromettenti. Una volta che la vittima è stata ingannata, i criminali minacciano di diffondere immagini o video compromettenti se non ricevono denaro o altre forme di riscatto.

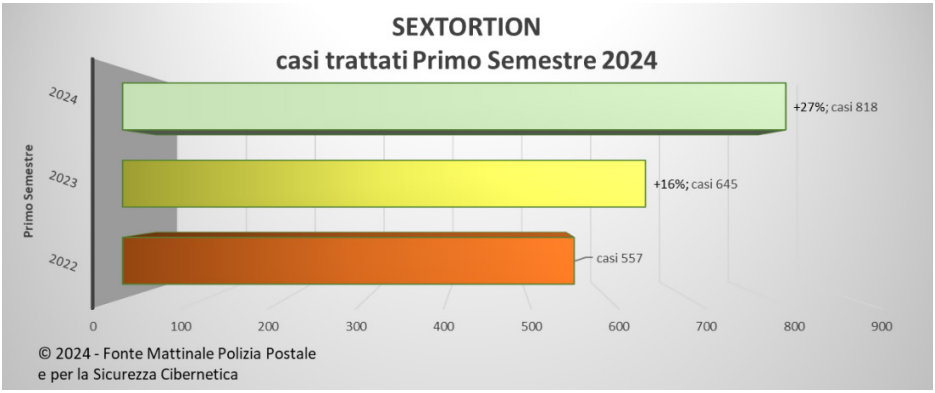
Questo fenomeno continua a essere particolarmente pervasivo, colpendo principalmente adulti in modo subdolo e sfruttando fragilità personali. Le vittime, spesso oppresse da sentimenti di vergogna per essere state ingannate, si trovano in situazioni difficili: tra gli 818 casi esaminati, 759 hanno riguardato persone adulte, in particolare di genere maschile. I sentimenti di impotenza e frustrazione sono ulteriormente amplificati dalla difficoltà nel richiedere aiuto a familiari o amici, complice il timore di essere giudicati.

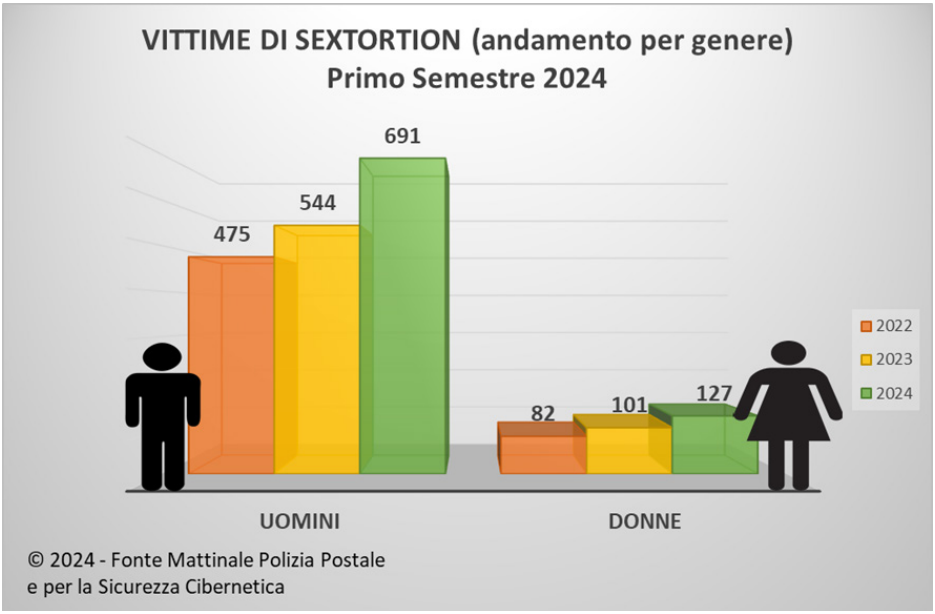
SEXTORTION	Primo Semestre 2022		Primo Semestre 2023		Primo Semestre 2024	
Uomini/ Donne	Vittime Uomini 475 (85%)	Vittime Donne 82 (15%)	Vittime Uomini 544 (84%)	Vittime Donne 101 (16%)	Vittime Uomini 691 (84%)	Vittime Donne 127 (16%)
Casi trattati	**557**		**645**		**818**	
Variazione percentuale		*+16%*		*+27%*		

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

	Primo Semestre 2022	Primo Semestre 2023	Primo Semestre 2024
Persone indagate	**37**	**72**	**68**
Variazione percentuale		*+95%*	*-6%*

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024





Romance Scam

La truffa romantica è un fenomeno insidioso che ha gravi effetti sulla vita personale ed economica delle vittime. Le persone colpite, molte delle quali hanno un'età intorno ai 50 anni, sono principalmente donne di diversa estrazione sociale. Spesso, queste vittime potrebbero essere reduci da relazioni sentimentali ormai concluse o avere figli che vivono in autonomia, rendendole più vulnerabili mentre navigano online.

In questo tipo di truffa, i criminali si avvicinano alle vittime tramite i social network, inviando richieste di amicizia e utilizzando foto di uomini attraenti che si spacciano per imprenditori o militari impiegati in zone di conflitto. Questi truffatori si presentano come single, vedovi o separati, al fine di ingannare le vittime e creare un legame emotivo.

Nei primi sei mesi del 2024, la Polizia Postale ha indagato su 293 casi di truffe romantiche, deferendo all'Autorità giudiziaria 101 persone.

Revenge Porn

Con il termine "revenge porn" (derivato dall'unione dei vocaboli inglesi "*revenge*" - vendetta e "*pornography*" - pornografia), si fa riferimento a una più ampia gamma di condotte che si realizzano essenzialmente con la condivisione di immagini e video intimi, tramite internet, senza il consenso della persona rappresentata. Sebbene questa locuzione faccia riferimento a specifiche finalità estorsive, in alcuni casi le immagini sono state prodotte da un partner e con il consenso della vittima, in altri, senza che la vittima ne avesse conoscenza, in altri ancora la realizzazione è avvenuta a seguito di diversi *e più gravi reati (es. violenza sessuale). Inoltre, può essere connessa alle pratiche di sexting*, che, pur essendo una pratica di coppia, possono fuoriuscire da tale ambito, causando danni del tutto analoghi.

La maggior parte delle vittime è di genere femminile, con effetti significativi sulla sfera emotiva e personale, in considerazione della peculiare pervasività di tali condotte. Il legislatore, accogliendo il forte grido di allarme generato dai numerosi casi emersi nel corso degli ultimi anni e colmando un vuoto normativo, nell'agosto 2019 ha introdotto nell'ordinamento giuridico italiano una norma penale (art. 612 ter) in grado di punire l'autore di condotte qualificabili come "*revenge porn*". Tale norma è parte integrante di un insieme di norme giuridiche noto come "Codice Rosso" (L. n. 69/2019), che ha individuato, oltre al "*revenge porn*", anche altre figure di reato, quali la "deformazione dell'aspetto della persona mediante lesioni permanenti al viso", la "costrizione o induzione al matrimonio" e la "violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa".

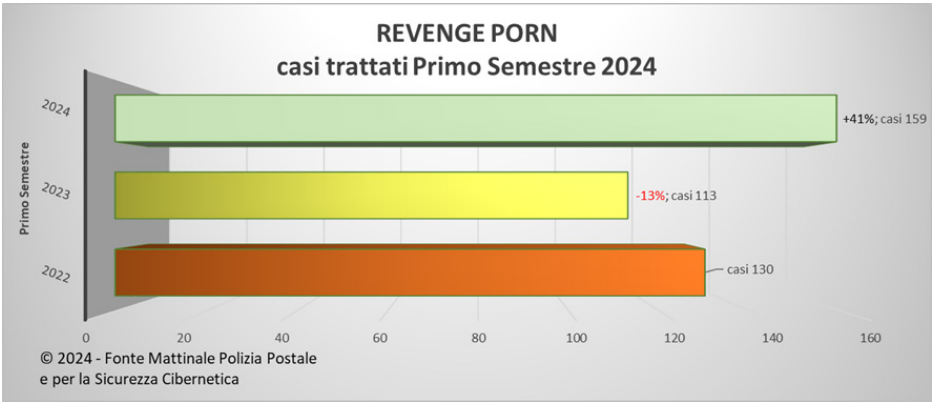
Sono state inoltre accresciute le pene previste per tali reati, così come si è intervenuti per ridurre i tempi "tecnici" per la comunicazione della notizia di reato da parte della Polizia Giudiziaria all'Autorità Giudiziaria.

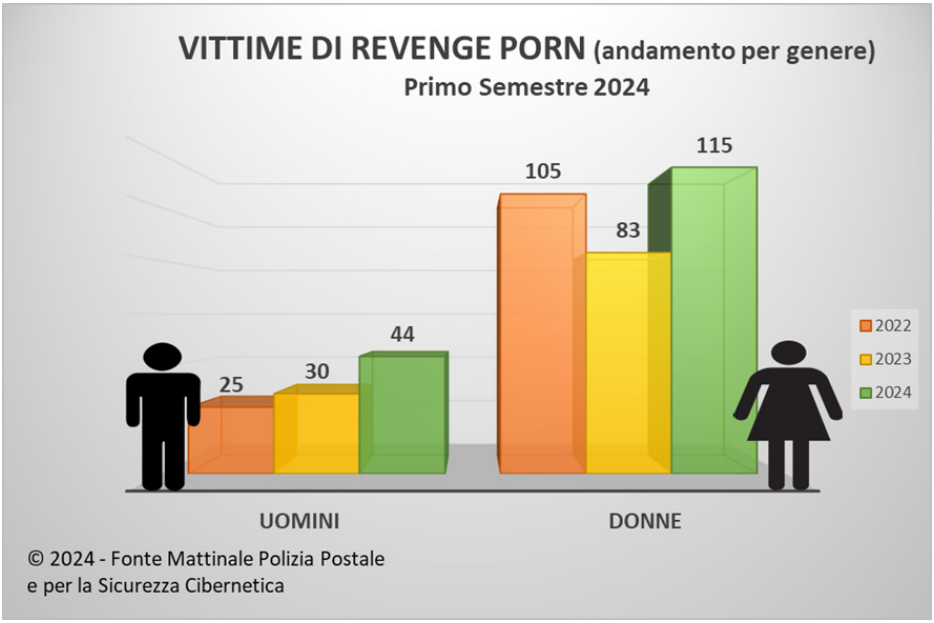
REVENGE PORN	Primo Semestre 2022		Primo Semestre 2023		Primo Semestre 2024	
Uomini/ Donne	Vittime Uomini 25 (19%)	Vittime Donne 105 (81%)	Vittime Uomini 30 (27%)	Vittime Donne 83 (73%)	Vittime Uomini 44 (28%)	Vittime Donne 115 (72%)
Casi trattati	**130**		**113**		**159**	
Variazione percentuale		*-13%*		*+41%*		

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

	Primo Semestre 2022	Primo Semestre 2023	Primo Semestre 2024
Persone indagate	**37**	**45**	**51**
Variazione percentuale		*+22%*	*+13%*

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024





Anche per i fenomeni come il *romance scam*, la *sextortion* e il *revenge porn*, per la loro insidiosità, il profondo coinvolgimento emotivo e le gravi conseguenze che infliggono alle vittime, la Polizia Postale ha organizzato giornate formative e divulgative rivolte a studenti, genitori, insegnanti e operatori.

Di seguito, vengono elencate le principali attività svolte nel settore specifico nel periodo compreso tra il 1° gennaio e il 30 giugno 2024.

Atti persecutori e stalking digitale: arrestato un romano dopo le denunce di una ex collega

Arresto di un cittadino romano di 31 anni, sospettato di atti persecutori contro una ex collega. La vittima, impiegata in una multinazionale di consulenza, aveva denunciato una serie di episodi allarmanti, tra cui l'invio di fiori da parte di un ammiratore sconosciuto, oltre a condotte che avevano ingenerato uno stato di profonda agitazione, tanto da indurla a modificare le proprie abitudini. A sua insaputa, erano stati effettuati alcuni tentativi di acquisti e-commerce ed era stata attivata una serie di servizi on line, fra i quali registrazioni su siti web pornografici o di incontri a sfondo sessuale. L'uomo aveva inoltre tentato di effettuare acquisti a nome della vittima, nascondendo la propria identità attraverso l'utilizzo di una VPN. Grazie alla c.d. "Legge Roccella",

è stato possibile effettuare l'arresto del soggetto in stato di flagranza differita, grazie anche alle prove digitali rinvenute sul dispositivo mobile.

Appropriazione indebita: coppia arrestata per circonvenzione di incapace nel Bellunese

Arresto di un uomo e una donna accusati di circonvenzione di incapace nei confronti di una donna residente nel bellunese. La coppia si era approfittata della fragilità emotiva della vittima, inducendola a consegnare loro denaro. L'indagine è partita grazie a una segnalazione di movimenti bancari sospetti da parte di Poste Italiane. Durante una perquisizione, è stata trovata una somma di denaro consistente, e la coppia è stata arrestata mentre tentava di fuggire verso una località turistica del Sud Italia.

Estorsione via minacce: arrestati due giovani per ricatti su foto intime

Arresto di un ventiquattrenne georgiano e di un diciottenne per estorsione, per minaccia di pubblicazione di foto intime. Un minorenne è stato denunciato per lo stesso reato. L'indagine è iniziata dopo la denuncia di un trentenne, costretto a ricaricare carte di credito e cedere buoni acquisto per evitare la diffusione delle sue immagini. Dopo un primo pagamento di 2.000 euro e una successiva richiesta di 800 euro, la vittima ha chiesto aiuto alla Polizia, che ha arrestato gli estorsori in Puglia.

Stalking e violazione della privacy: arrestati due persone per minacce e diffamazione online

Ordinanza di custodia cautelare nei confronti di due individui accusati di *stalking* nei confronti di una vittima che aveva condiviso la sua esperienza di cambio di una prestazione sessuale sui social media. La persona offesa ha denunciato, in più occasioni, di essere stata vittima di *stalking*, consistente in pedinamenti, ripetute offese, minacce gravi e pubblicazione di dati personali su una nota piattaforma di streaming, anche con contenuto transfobico, ad opera di un interlocutore che si spacciava per "funzionario del Ministero dell'Interno". Le indagini, condotte tempestivamente dagli specialisti della Polizia Postale, attraverso un'analisi incrociata degli elementi investigativi e delle tracce informatiche acquisite, hanno portato all'identificazione dei due indagati. Uno di loro era responsabile delle dirette streaming denigratorie, mentre l'altro, che aveva accesso a banche dati contenenti informazioni personali a causa della sua attività lavorativa, è accusato di accesso abusivo a sistemi informatici.

Truffa dei bonus culturali e vacanze: cinque denunciati per monetizzazione illecita

Denuncia di cinque soggetti residenti in diverse Regioni italiane per la monetizzazione illecita dei "*Bonus Cultura 18 app*" e "*Bonus Vacanze*". L'indagine, avviata a

Vercelli, ha rivelato che due indagati, titolari di un portale di conversione dei titoli, avevano creato un meccanismo fraudolento per convertire oltre 250 buoni, ciascuno del valore di 500 euro, realizzando profitti per decine di migliaia di euro. Gli indagati, di cui uno coinvolto per truffa aggravata per il conseguimento di erogazioni pubbliche, erano riusciti ad eludere l'esecuzione delle procedure necessarie per l'incasso dei buoni, senza prestare il servizio previsto.

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 ed Enti sensibili consorziati, mediante un continuativo contatto e scambio di informazioni, anche di natura tecnica, rilevanti sulla minaccia cibernetica.

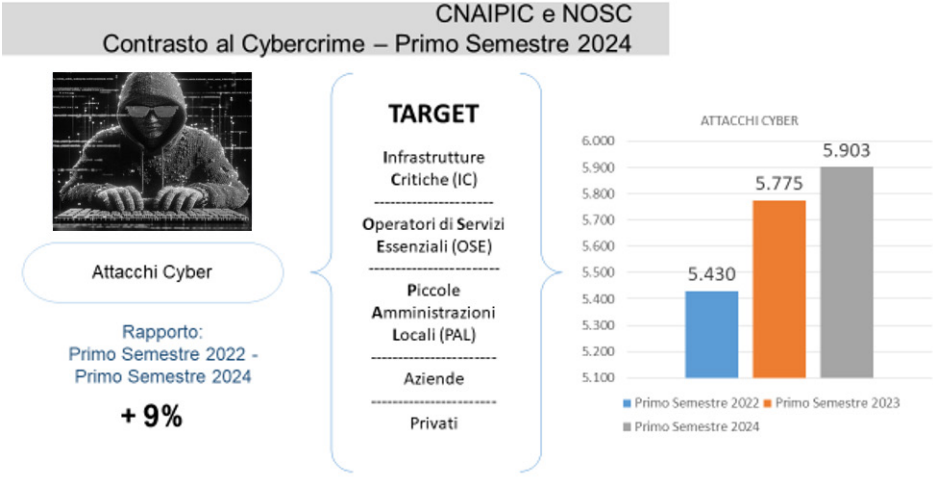
Negli anni, il processo riorganizzativo della Specialità si è adeguato alla natura variegata e mutevole delle minacce cibernetiche, con l'emersione sempre più impellente di una rimodulazione interna degli *asset*, al fine di garantire una maggiore vicinanza alle realtà da proteggere e un intervento ancor 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 n. **5.903** attacchi, nonché di diramare n. **30.933** *alert*. Le indagini avviate esclusivamente dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche sono state n. **36**, mentre n. **101** sono le persone indagate, con la collaborazione delle articolazioni territoriali e n. **23** le richieste di cooperazione internazionale in ambito Rete 24/7 High Tech Crime (Convenzione di Budapest) pervenute, a cui si è dato corso.

	Primo Semestre 2022	Primo Semestre 2023	Primo Semestre 2024
TOTALE ATTACCHI RILEVATI	**5.430**	**5.775**	**5.903**
Variazione percentuale per anno		*+6%*	*+2%*
Variazione percentuale nel biennio		*+9%*	

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024



Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

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 ed esponenziale evoluzione della minaccia informatica, quale fenomeno in costante crescita e sempre più influenzato dall'avanzamento tecnologico e dalla digitalizzazione della vita quotidiana. È un dato facilmente riscontrabile che la rete internet, fonte e motore del progresso, è anche e sempre più frequentemente strumento utilizzato per commettere reati di qualsiasi genere.

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 ed 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 ed 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 ad 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 recenti tendenze negli attacchi DDoS mostrano l'uso crescente di botnet sofisticate e il ruolo degli attacchi DDoS nei conflitti geopolitici, in particolare il conflitto Russia-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 e 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 ad 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 disporre 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 impor-

tanti 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 ad 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 ed 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 consessi 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 ed 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.

74° 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 74° 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 per la "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.

G7 Summit – Riunione Borgo Egnazia

In occasione del Vertice del G7, svoltosi a Borgo Egnazia, nel comune di Fasano (BR) in Puglia, dal 13 al 15 giugno 2024 e che ha visto la partecipazione dei Capi di Stato e di Governo dei sette Stati Membri (oltre al Presidente del Consiglio Europeo e alla Presidente della Commissione Europea, in rappresentanza dell'Unione Europea), il Servizio Polizia Postale e per la sicurezza cibernetica ha impiegato un'importante aliquota di personale per garantire una costante attività di monitoraggio della rete internet alla ricerca di minacce - sia fisiche che cyber - rivolte all'infrastruttura tecnologica predisposta per l'evento.
L'attività di monitoraggio si è dispiegata all'interno di un più ampio dispositivo integrato, che ha operato anche mediante la predisposizione di una Sala Operativa dedicata, che ha visto coinvolto personale operante del C.N.A.I.P.I.C. del Servizio Polizia Postale - supportato dalle dipendenti articolazioni territoriali (COSC) - avvalersi di tecnologie di elevato livello e di personale altamente qualificato.

In particolare, gli operatori specialisti della Postale hanno garantito:
- l'analisi preliminare dello stato dei sistemi informatici deputati alla gestione dell'evento, delle relative vulnerabilità e la ricognizione di elementi di possibile criticità, in collaborazione con le figure tecniche titolari dell'infrastruttura;
- costante supporto operativo, durante lo svolgimento del summit, per ridurre al minimo il rischio del verificarsi di emergenze cyber di natura tecnico-investigativa.

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 cam-

pagne 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 e 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.

Financial Cybercrime

In relazione ai fenomeni criminali connessi al cosiddetto *financial cybercrime*, il semestre in analisi ha messo in luce le consuete dinamiche delinquenziali, prevalentemente riconducibili al fenomeno del "*man in the middle*". In particolare, si evidenziano le varianti rappresentate dal *Business Email Compromise* (BEC) e dal *CEO Fraud* (Chief Executive Officer Fraud).

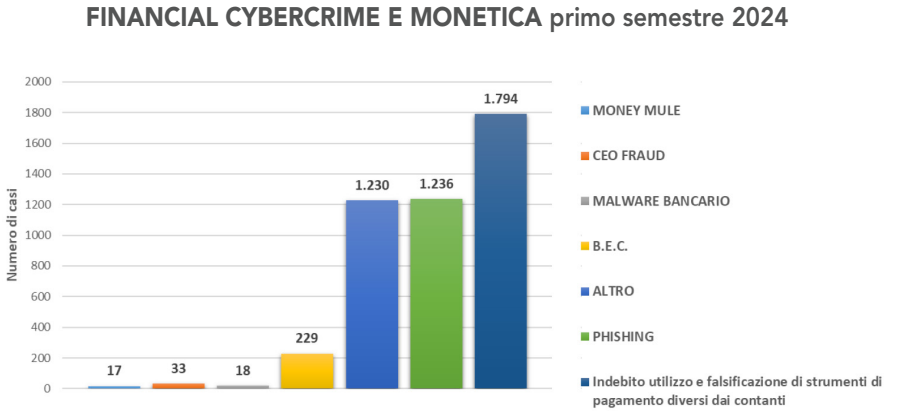
Il Servizio Polizia Postale e per la sicurezza cibernetica ha altresì monitorato l'evoluzione di fenomeni criminali già noti e consolidati, come il falso *trading online*. L'avvento delle nuove tecnologie, in particolare dell'intelligenza artificiale (IA), ha consentito ai *cyber* criminali di alterare in modo credibile immagini e audio di figure pubbliche di rilievo. Tale capacità ha reso più verosimili informazioni false, inducendo in errore un ampio numero di utenti del web e causando gravi danni.

Nei primi sei mesi del 2024, la Polizia Postale ha rilevato a livello nazionale **4.557** casi di frode informatica e monetica[3]. Per questi reati, sono state indagate **532** persone, con un totale di € **22.382.693** sottratti.

[3] Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti

	Primo Semestre 2022	Primo Semestre 2023	Primo Semestre 2024
Casi di frodi Informatiche e monetica (Ril. nazionale)	4.734	5.354	4.557
Persone indagate	438	388	532
Somme sottratte	€ 14.314.647	€ 21.536.551	€ 22.382.693

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024



Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024

BEC Fraud (Business e-mail compromised)

Consiste nell'intercettare le comunicazioni fra aziende o privati (attraverso un accesso abusivo ad una delle caselle di posta elettronica delle potenziali vittime), individuare eventuali richieste di pagamento, sostituirsi ad una delle parti e dirottare i bonifici modificando le fatture con l'indicazione di nuove coordinate bancarie; tale modalità presuppone, sovente, la creazione di altro indirizzo mail (che si differenzia dall'originale in modo impercettibile) attraverso cui si trae in inganno la controparte per consentire il dirottamento dei bonifici su altri conti.

CEO Fraud (Chef Executive Officer)

In questo caso i criminali, sfruttando le evidenze offerte dall'analisi di fonti aperte (legate soprattutto agli spostamenti ufficiali dei CEO di grandi aziende o alla partecipazione degli stessi ad eventi finanziari di grande rilievo), avendo cura di creare un indirizzo mail quasi identico a quello del capo dell'azienda, o talora utilizzandone uno reale (del quale si sono impossessati), contattano un alto funzionario o dirigente di altra azienda inducendolo, con l'inganno (caratterizzato da un linguaggio strettamente confidenziale), a fare uno o più bonifici correlati ad una inesistente operazione finanziaria riservata ed urgente. Sovente, tali strategie criminali prevedono l'intervento di una figura con il ruolo di un avvocato specializzato nei contratti internazionali, nonché la formazione di documenti completamente falsi che supportano la strategia dell'inganno posta in essere.

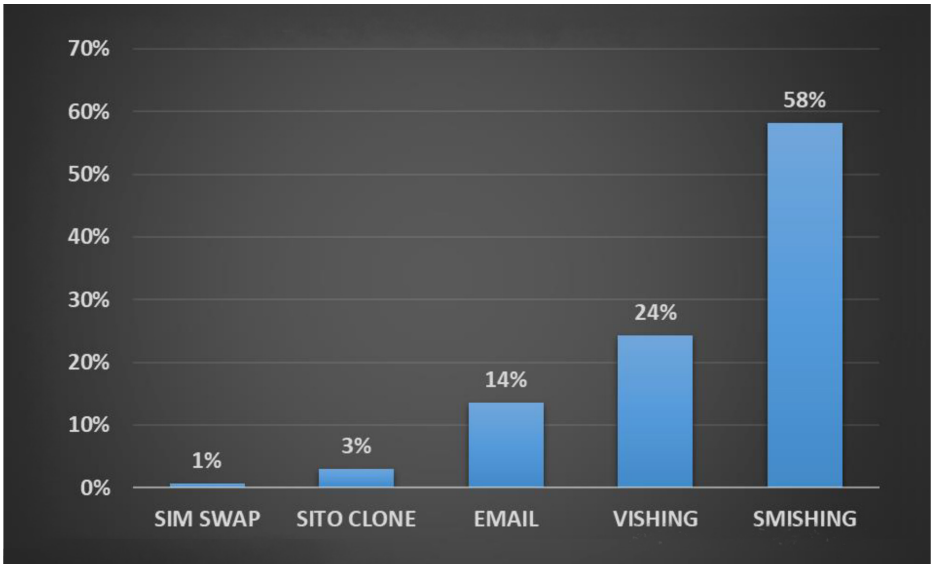
Phishing

Tra le principali condotte criminose, si registra l'indebita acquisizione di dati sensibili che consentono l'accesso ai sistemi di home banking. Questi attacchi sono generalmente indicati con i termini "*phishing*", "*smishing*" e "*vishing*", a seconda dello strumento utilizzato: email, SMS o contatti diretti vocali. Lo scopo di queste attività è ottenere le credenziali finanziarie delle vittime, per poter poi operare sui loro conti correnti online, effettuare prelievi con carte di credito/debito o completare acquisti online.

È ancora presente, seppur in misura residuale, anche la tecnica del c.d. «*sim swap***"**: una variante del *phishing* che si è sviluppata in seguito all'innalzamento della sicurezza da parte delle banche, che sempre più frequentemente implementano sistemi di "doppia autenticazione". Questi sistemi richiedono che l'utente verifichi la propria identità utilizzando un codice che viene inviato sul proprio *smartphone*. Poiché è necessario ottenere i codici autorizzativi, i criminali, dopo aver rubato indebitamente i dati sensibili necessari per effettuare un'operazione bancaria, riescono a farsi emettere dai gestori un duplicato della SIM (simulando un furto o uno smarrimento della stessa). In questo modo, riescono ad ottenere anche i codici per la doppia autenticazione e portare a termine operazioni fraudolente.

Il grafico seguente presenta, in forma percentuale, i casi di furto d'identità digitale investigati dalla Polizia Postale e per la sicurezza cibernetica nei primi sei mesi del 2024. Tale analisi si colloca all'interno del contesto dei crimini economico-finanziari online e distingue tra diversi metodi impiegati.

FURTO IDENTITÀ primo semestre 2024



Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024

- ***Smishing*** (58%): Questo metodo, che consiste nell'invio di messaggi di testo fraudolenti per ottenere informazioni personali, è il più utilizzato, in ragione della facilità con cui le persone rispondono ai messaggi di testo, spesso senza sospettare che possano essere fraudolenti.
- ***Vishing*** (24%): Il *vishing* utilizza chiamate telefoniche per ingannare le vittime e ottenere informazioni sensibili; questo metodo è il secondo più comune, indicando che le chiamate telefoniche fraudolente sono ancora molto efficaci.
- **Email** (14%): Le email fraudolente rappresentano una parte significativa dei casi. Nonostante le numerose campagne di sensibilizzazione, molte persone continuano a cadere vittime di email ingannevoli.
- **Sito clone** (3%): La creazione di siti web clonati per ingannare gli utenti è meno comune, ma comunque presente; questo metodo richiede più competenze tecniche rispetto agli altri.
- ***Sim swap*** (1%): Il furto d'identità tramite la sostituzione della SIM è il meno comune, ma può avere conseguenze gravi, permettendo ai truffatori di accedere a numerosi account collegati al numero di telefono della vittima.

Deep Fake

Nato dallo sviluppo dell'intelligenza artificiale, questo fenomeno si concentra nella creazione di contenuti ingannevoli destinati alla diffusione tramite i principali social media, con l'intento di trarre profitto.

In particolare, con il termine "*deepfake*", ci si riferisce a contenuti che risultano più difficili da identificare come falsi poiché generati utilizzando volti di personaggi noti: l'utilizzo di volti conosciuti conferiscono maggiore credibilità ai contenuti veicolati; tra i maggiori exploit riscontrati, si evidenzia l'uso delle immagini di celebrità come Elon Musk e personalità istituzionali quali la Presidente del Consiglio Giorgia Meloni e l'amministratore delegato Pier Silvio Berlusconi, i cui volti sono stati impiegati in video promozionali sulle principali piattaforme social per pubblicizzare investimenti finanziari.

L'impiego dell'intelligenza artificiale sta contribuendo, inoltre, all'evoluzione del fenomeno noto come CEO *Fraud*: i cybercriminali, sfruttando informazioni disponibili pubblicamente relative ai cd "soggetti bersaglio", ricreano la voce e i gesti dell'amministratore per impartire istruzioni ai dipendenti dello stesso per effettuare bonifici legati a inesistenti operazioni finanziarie riservate e urgenti.

Le truffe online

Le truffe online rappresentano una minaccia sempre più rilevante nel panorama digitale, colpendo quotidianamente milioni di utenti in tutto il mondo e causando danni economici significativi. L'analisi delle tipologie di truffe più comuni non solo evidenzia l'evoluzione delle tecniche impiegate dai criminali, ma anche la vulnerabilità delle vittime.

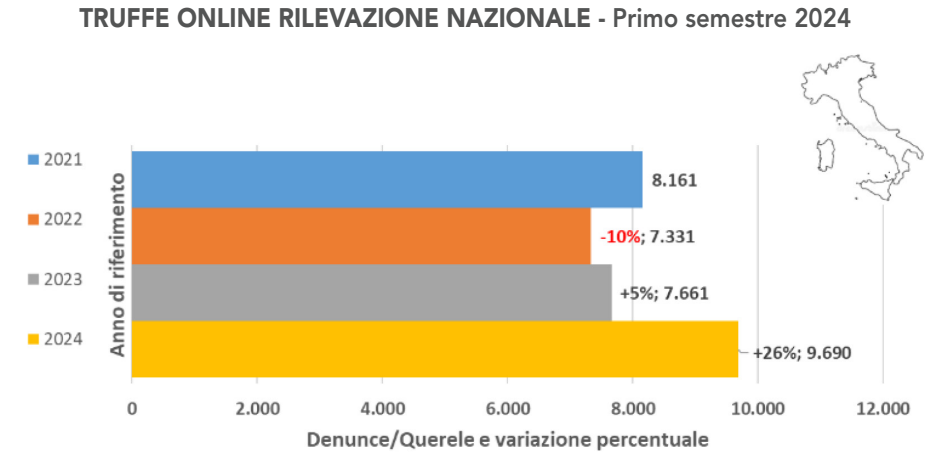
Le truffe online, rilevate quotidianamente dagli operatori della Specialità durante i monitoraggi costanti del *World Wide Web* o segnalate dai cittadini tramite l'apposita sezione del sito del Commissariato di P.S. online, mostrano un aumento numerico direttamente proporzionale alle denunce raccolte giornalmente dagli uffici territoriali della Specialità.

Tra le tipologie di truffe più preoccupanti ci sono quelle legate al commercio elettronico (e-commerce), al falso *trading online*, alle già citate truffe "sentimentali" (*romance scam*) e alle frodi immobiliari. Questi fenomeni destano particolare allerta, non solo per le ingenti somme sottratte dai sempre più sofisticati e organizzati gruppi criminali, spesso con ramificazioni transnazionali, ma anche per la vulnerabilità psicologica delle vittime, particolarmente suscettibili alle tecniche di manipolazione messe in atto dai truffatori.

I cyber-criminali utilizzano sofisticate tecniche di ingegneria sociale per identificare i loro target, facendo leva sui bisogni e sulle debolezze delle persone. Offrono facili guadagni, investimenti miracolosi o relazioni sentimentali illusorie, inducendo le vittime tramite artifici e inganni a investire somme considerevoli, ad acquistare prodotti inesistenti a prezzi nettamente inferiori rispetto a quelli di mercato, o a completare transazioni su siti web abilmente contraffatti.
Nei primi sei mesi del 2024, la Polizia Postale ha registrato a livello nazionale **9.690** casi di truffe perpetrate attraverso le tecnologie della comunicazione e dell'informazione. Di questi reati sono state indagate **1.761** persone, con un ammontare totale di € **98.555.935** sottratti.

	Primo Semestre 2021	Primo Semestre 2022	Primo Semestre 2023	Primo Semestre 2024
Truffe OnLine (Ril. nazionale)	8.161	7.331	7.661	9.690
Persone indagate	1.861	1.856	1.853	1.761
Somme sottratte	€ 33.807.810	€ 49.798.189	€ 58.253.567	€ 98.555.935

Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

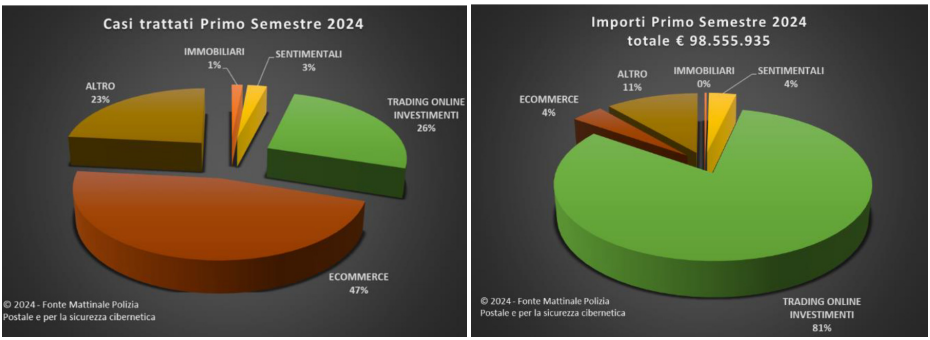


Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024

PRIMO SEMESTRE 2024 TRUFFE ONLINE - Rilevazione Nazionale

		IMPORTI SOTTRATTI	
IMMOBILIARI	**CASI TOTALI 9.690**	263.662 €	**PERSONE INDAGATE 1.761**
SENTIMENTALI ROMANCE SCAM		3.299.714 €	
TRADING ONLINE		79.939.451 €	
E COMMERCE		3.908.776 €	
ALTRO		11.144.332 €	
		TOTALE 98.555.935 €	

Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024



Fonte - Polizia Postale e per la sicurezza cibernetica © 2024

Il Falso Trading Online

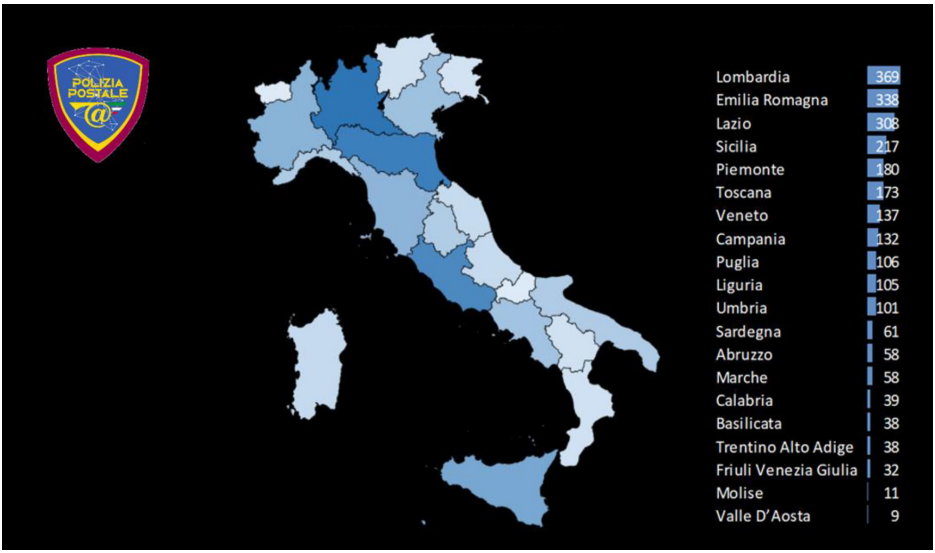
L'attività più redditizia e in preoccupante crescita per la criminalità organizzata nel campo delle truffe online è senza dubbio il falso trading online, con un totale di **79.939.451** euro sottratti e **2.510** casi registrati nei primi sei mesi del 2024. Rispetto allo stesso periodo dell'anno precedente, durante il quale erano stati segnalati **1.492** casi, si segnala un aumento del **+68%**.

Questo fenomeno criminale si sviluppa principalmente attraverso la promozione su piattaforme social di grande diffusione, come Facebook e YouTube, di finti investi-

menti finanziari. I cybercriminali, utilizzando diverse tecniche, tra cui l'ingegneria sociale, riescono a convincere gli utenti, attratti dalla prospettiva di facili guadagni, a investire in piattaforme di trading online. Una delle metodologie più comuni è rappresentata dalle telefonate di marketing, durante le quali falsi broker esercitano pressioni sugli utenti affinché depositino soldi su conti pilotati o investano in specifici *asset*, spesso criptovalute, caratterizzati da elevati livelli di volatilità e anonimato.

In particolare, viene chiesto agli utenti di iscriversi a una piattaforma di trading online che appare semplice e intuitiva, facilitando così l'esecuzione delle operazioni; spesso, il falso operatore propone di completare l'iscrizione a nome dell'utente o proporre l'installazione di software per il controllo da remoto dei dispositivi della vittima. Inizialmente, vengono richieste piccole somme di denaro, che sembrano produrre buoni profitti. Tuttavia, ben presto le somme richieste diventano sempre più consistenti, fino a che la vittima non riesce più ad accedere ai fondi investiti.

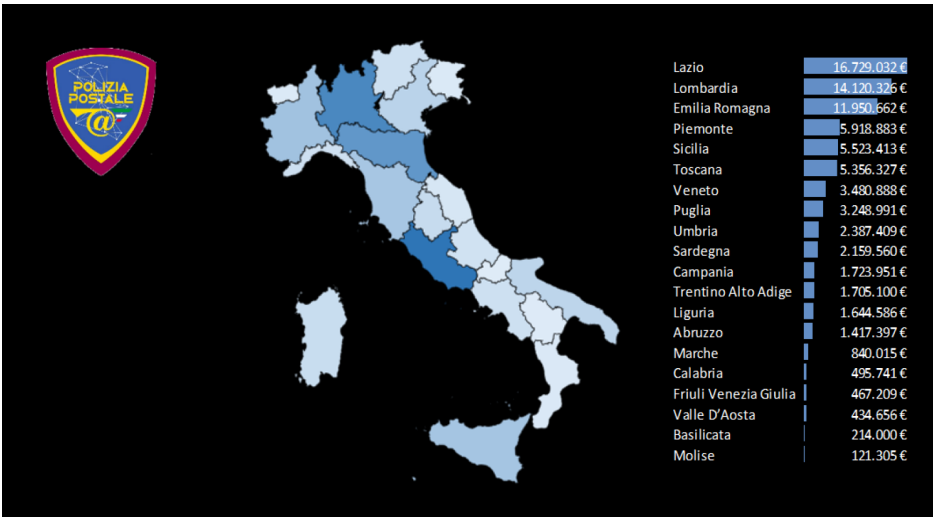
CASI DI TRUFFE NEL TRADING ONLINE - Primo semestre 2024



La cartina termica illustra la distribuzione geografica dei casi di truffe nel trading online denunciati presso gli uffici territoriali della Polizia Postale nel primo semestre del 2024.

Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024

SOMME SOTTRATTE CON LE TRUFFE DI TRADING ONLINE
Primo semestre 2024



La cartina termica illustra la distribuzione geografica delle somme sottratte tramite le truffe nel trading online denunciate presso gli uffici territoriali della Polizia Postale nel primo semestre del 2024.

Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2024

Prevenzione e contrasto

Allo scopo di innalzare i livelli di contrasto delle specifiche fenomenologie criminose, l'azione della Specialità, anche nel settore del *Financial Cybercrime*, non si distingue solo per i profili repressivi, ma anche per la particolare attenzione rivolta alla prevenzione, attraverso campagne di informazione destinate alle forze di polizia e al pubblico, utilizzando anche i canali social.

Parimenti significativa, soprattutto ai fini della tempestività dell'azione, è la collaborazione internazionale, sia in ambito europeo che extraeuropeo: spesso, in caso di prontezza di reazione da parte delle vittime e, quindi, nell'immediatezza degli eventi, la Polizia Postale e per la sicurezza cibernetica riesce a conseguire buoni risultati in termini di recupero delle somme distratte e di identificazione degli autori, grazie alla cooperazione con le forze di polizia dei paesi stranieri in cui vengono indirizzate le somme sottratte o dove operano gli autori dell'illecito.

In questo contesto di collaborazione internazionale, si segnala la partecipazione a vari tavoli di lavoro, tra cui EMMA (*European Money Mule Action*), a cui aderiscono

diversi Stati europei e l'Agenzia Europol. Tale partecipazione consente di realizzare indagini congiunte con risultati investigativi di notevole rilevanza, grazie a un impegno sinergico.

L'attività di contrasto alle truffe online e alle frodi informatiche

Di seguito, le principali attività svolte nello specifico settore nel periodo 1° gennaio - 30 giugno 2024.

Perquisizioni Roma

Nel mese di gennaio 2024, il personale del Servizio Polizia Postale e per la sicurezza cibernetica ha eseguito a Roma un decreto di perquisizione locale emesso dalla locale Procura della Repubblica nei confronti di due soggetti, ex dipendenti di una società, indagati per i reati di accesso abusivo al sistema informatico aziendale e per indebito utilizzo di strumenti di pagamento aziendali. L'attività è scaturita dalla denuncia presentata dall'amministratore unico e legale rappresentante della società, che cura, tra le altre attività, anche le campagne elettorali di diversi partiti politici.

Operazione Portorico

Nel mese di febbraio 2024, personale del Servizio Polizia Postale e dei Centri Operativi per la Sicurezza Cibernetica (COSC) di Milano, Roma, Firenze e Napoli, ha dato esecuzione a 18 decreti di perquisizione emessi dalla Procura della Repubblica di Milano, nei confronti di altrettanti soggetti indagati per il reato di truffa aggravata in concorso.

L'indagine è scaturita a seguito di una denuncia presentata da un cittadino italiano vittima di una truffa perpetrata attraverso le tecniche dello "*smishing*" e del "*vishing*".

I malfattori, attraverso l'invio di un sms contenente un *link* apparentemente riconducibile alla banca Findomestic (e successive telefonate effettuate da un finto operatore della medesima banca), hanno indotto la vittima a credere che stesse subendo un attacco informatico sul proprio dispositivo mobile, persuadendola ad effettuare, attraverso l'applicazione bancaria presente sul proprio telefono cellulare, 19 bonifici verso conti correnti amministrati dai frodatori, per una somma totale di circa 250.000 euro. Le perquisizioni sono state eseguite nelle province di Napoli, Caserta, Salerno e Livorno.

Arresti Milano

Nel mese di febbraio 2024 personale del Centro Operativo per la Sicurezza Cibernetica di Milano ha eseguito quattro ordinanze di custodia cautelare agli arresti domici-

liari, emesse nei confronti di altrettanti soggetti indagati, in concorso, per il reato di furto aggravato e continuato.
L'indagine, coordinata dalla Procura della Repubblica di Firenze, è stata avviata a seguito di una denuncia prodotta, presso il citato COSC, dal gruppo *Mediaworld* per il furto di materiale informatico sottratto presso l'esercizio commerciale di Bergamo.
L'attività investigativa ha permesso di acquisire evidenze indizianti utili a radicare la competenza territoriale presso la Procura della Repubblica del capoluogo toscano e a riscontrare il coinvolgimento degli indagati in altri cinque episodi di furto consumati nei centri *Mediaworld* di Firenze, Lucca, Benevento, Padova e Avezzano.
I provvedimenti sono stati eseguiti nella provincia di Napoli con l'ausilio di personale del locale Centro Operativo per la Sicurezza Cibernetica.

Perquisizioni Latina

Nel mese di febbraio 2024, personale del Centro Operativo per la Sicurezza Cibernetica (COSC) del Lazio, unitamente agli operatori della Sezione Operativa per la Sicurezza Cibernetica di Latina, hanno dato esecuzione a quattro decreti di perquisizione, personale, locale e su sistemi informatici, emessi dalla Procura della Repubblica di Roma nei confronti di soggetti indagati per reato di truffa aggravata per il conseguimento di erogazioni pubbliche e accesso abusivo a sistema informatico.
Una delle perquisizioni è stata estesa anche alla sede del Centro di Assistenza Fiscale "Valore Donna" con sede a Latina.
Il complesso di attività delegate origina dalle investigazioni condotte dalla Sezione Operativa di Latina. In particolare, le evidenze indizianti concernevano la formazione di falsa documentazione atta ad ottenere il riconoscimento della Carta di Reddito di Cittadinanza, realizzata accedendo nel sistema telematico dell'INPS – Ufficio Provinciale di Latina.

Oscuramento di 473 siti e perquisizione Roma

Nel mese di febbraio 2024, personale del Centro Operativo per la Sicurezza Cibernetica di Roma, a seguito di una mirata attività investigativa coordinata dalla locale Procura della Repubblica, ha sequestrato preventivamente, mediante oscuramento, 473 contenuti riconducibili a siti *web*, *account* e annunci sul *social network Facebook*, afferenti a compagne pubblicitarie volte a promuovere falsi investimenti finanziari, attraverso piattaforme di *trading online* artatamente realizzate.
In particolare, l'attività illecita veniva realizzata sfruttando il marchio ENI, nonché video *deepfake* appositamente realizzati, con l'ausilio dell'intelligenza artificiale, utilizzando l'immagine dell'Amministratore Delegato di ENI S.p.a., dott. Claudio Descalzi.
Nel medesimo contesto operativo è stato eseguito ad un decreto di perquisizione

locale, personale e informatica nei confronti di un soggetto, residente nel capoluogo campano, che, a seguito delle evidenze investigative, è risultato beneficiario di € 183.000,00 ottenuti dalle frodi di cui in premessa.

Operazione Repass

Nel mese di febbraio 2024, personale del Centro Operativo per la Sicurezza Cibernetica (COSC) del Lazio ha eseguito a Roma, Torino e Benevento, con la collaborazione dei locali Centri Operativi per la Sicurezza Cibernetica (COSC) un decreto di perquisizione personale e locale, emesso dalla Procura della Repubblica di Roma nei confronti di quattro soggetti, indagati per utilizzo in frode di buoni "Repass" in danno di appartenenti alla Polizia di Stato.
Le attività di indagine sono scaturite dalle denunce presentate da alcuni operatori della Polizia di Stato, i quali, dopo aver riscontrato anomalie riconducibili all'inserimento di credenziali errate all'atto del tentativo di accesso alla pagina riservata sul portale *Repass*, avevano rilevato l'ammanco dei buoni, spesi fraudolentemente, utilizzando il servizio online "*PayRepass*" fornito dalla società Repass Lunch Coupon s.r.l.
I truffatori, dopo aver effettuato l'accesso abusivo alla pagina personale delle parti offese sul portale Utilizzatori *Repass*, si impossessavano dell'account violato con il quale spendevano fraudolentemente i buoni residui, mediante l'attivazione del pagamento "*cardless*" negli esercizi commerciali aderenti al circuito.

Operazione Rolex

Nel mese di marzo 2024 personale del Centro Operativo per la Sicurezza Cibernetica di Perugia ha eseguito otto misure cautelari nei confronti di altrettanti soggetti residenti a Napoli e provincia. A carico dei destinatari dei provvedimenti giudiziari (uno dei quali già ristretto presso la Casa circondariale di Napoli) sono state acquisite gravi evidenze indizianti che riscontravano il coinvolgimento dei medesimi in un sodalizio criminoso dedito alla commissione di truffe aggravate, perpetrate attraverso l'acquisto, mediante assegni circolari falsi, di orologi "Rolex" posti in vendita da privati su siti di e - commerce.
Le misure sono state eseguite nel territorio napoletano con l'ausilio di personale del Servizio Polizia Postale e del Centro Operativo per la Sicurezza Cibernetica di Napoli.

Operazione Money Box

Nel mese di marzo 2024 sono stati notificati 48 avvisi di conclusione delle indagini preliminari e informazione di garanzia, nell'ambito di un'indagine scaturita dalla denuncia per frode informatica, presentata al Centro Operativo per la Sicurezza Cibernetica Liguria dal rappresentante legale dell'azienda "IL PESTO DI PRA' – Bruzzone &

Ferrari", produttrice di prodotti alimentari della provincia di Genova.
Gli approfondimenti investigativi, coordinati dalla Procura della Repubblica presso il Tribunale di Napoli e condotti con l'ausilio del Servizio Polizia Postale e la collaborazione della Stazione Carabinieri di Marcianise, sono stati effettuati prevalentemente a Napoli, Caserta e in Spagna.
L'attività illecita riscontrata nel corso delle indagini è stata caratterizzata dal *phishing*, dall'*hacking* e dallo *smishing*, condotti con tecniche idonee a carpire fraudolentemente i dati personali sensibili di accesso alle piattaforme "*home banking*".
Le indagini effettuate dai predetti Uffici, anche in regime di cooperazione giudiziaria internazionale per il tramite di Eurojust ed Europol, hanno consentito di rilevare una complessa organizzazione criminale, suddivisa in due macro cellule, una delle quali radicata in Spagna, nei pressi della città di Alicante, l'altra ubicata in Italia, a Villa Literno (CE).
Le cellule italiana e spagnola per compiere le proprie attività si avvalevano di ulteriori cinque cellule situate in Italia, ognuna delle quali deputate allo svolgimento di diversi ruoli.
Nel corso delle indagini, sono state effettuate 35 perquisizioni in Italia che hanno consentito di arrestare, in flagranza di reato, quattro persone per la commissione dei reati di falso documentale, frode informatica e porto abusivo di armi e di sequestrare ingente materiale informatico, relativo alle frodi ed agli accessi abusivi ai conti correnti delle vittime.
Tra gli indagati è stato altresì individuato un cittadino albanese, facente parte della cellula spagnola, responsabile dell'attività di *hacking* ai danni delle vittime italiane, considerato uno degli hacker più pericolosi nel panorama criminale europeo con numerosi precedenti specifici in Italia.
Lo stesso, per evitare l'arresto, si era trasferito in Spagna nella città di Alicante, dove aveva riorganizzato la propria attività criminale, nel corso della quale è stato tratto in arresto dalla polizia spagnola.
Nel corso della detenzione, mostrando una particolare inclinazione criminale, aveva ordinato ai membri della cellula di assoldare nel "*dark web*" un killer professionista per uccidere il giudice spagnolo titolare del procedimento penale a suo carico.
Il progetto criminale non è stato attuato per l'attività investigativa condotta dal COSC di Genova e dalla *Guardia Civil* spagnola.

CEO Fraud Società Fremantle Media Group

Nel mese di marzo 2024 il Servizio Polizia Postale e per la sicurezza cibernetica veniva interessato dalla Questura di Roma a seguito di una frode informatica del tipo *CEO fraud* subita dalla società *Fremantle Media Group*.

In particolare ignoti, sostituendosi al Presidente della citata società, avviavano interlocuzioni *whatsapp* con il rappresentante legale in Italia della società medesima inducendolo ad effettuare un bonifico di euro 940.000 verso un conto corrente greco, per una inesistente operazione societaria. L'immediata attivazione dei canali internazionali di cooperazione permetteva di congelare circa 100.000 euro ancora presenti sul conto corrente.

Smishing/vishing Società Scandiuzzi Steel Constructions S.p.a.

Nel mese di marzo 2024 il Servizio Polizia Postale veniva interessato dal Gabinetto del Ministro della Giustizia per una frode subita dalla società Scandiuzzi Steel Constructions S.p.a., realizzata con la tecnica del *smishing/vishing*, per un importo totale di euro 795.000,00.

La condotta delittuosa, denunciata presso la Stazione dei Carabinieri di Volpago del Montello, veniva avviata attraverso un messaggio fraudolento indirizzato all'A.D. della società (apparentemente proveniente dalla banca) che segnalava problemi sul conto corrente societario, con invito a contattare urgentemente un numero telefonico indicato nel testo del messaggio per le opportune verifiche.

Nei conseguenti contatti, i truffatori acquisivano i dati sensibili per poter effettuare i bonifici in frode, atterrati su un conto corrente attestato presso una banca della Lituania. L'immediato interessamento della Sezione Operativa per la Sicurezza Cibernetica di Treviso, contattata anche da personale dell'Arma dei Carabinieri, permetteva al Servizio Polizia Postale di attivare i consueti canali di cooperazione internazionale e di avviare immediate interlocuzioni con la banca lituana. L'esito del tempestivo intervento permetteva di intercettare integralmente la somma di denaro sottratta per la restituzione alla citata società.

CEO Fraud Gruppo Ticketone S.p.a.

Nel mese di aprile 2024 il Servizio Polizia Postale e per la sicurezza cibernetica si attivata in seguito alla denuncia presentata dal Gruppo Ticketone S.p.a. – EVENTIM per una patita frode informatica di tipo CEO Fraud.

In particolare, ignoti malfattori, spacciandosi per il Presidente del Gruppo, inviavano tramite *WhatsApp* un messaggio vocale, generato tramite l'utilizzo di intelligenza artificiale, all'Amministratore delegato inducendolo, anche con ulteriori raggiri, ad effettuare un pagamento, in via riservata, per l'acquisizione di una azienda all'estero. Indotto in errore, l'Amministratore delegato disponeva in data 10 aprile 2024, un bonifico di euro 797.755,26 su un conto corrente attestato presso la banca greca *Piraeus Bank S.A.*.

L'immediata attivazione dei canali di cooperazione internazionale di polizia e della UIF italiana, consentiva il blocco cautelativo del conto corrente con l'intera somma frodata.

Operazione 10 Denari

Nel mese di aprile 2024, il Centro Operativo per la Sicurezza Cibernetica di Bologna, a conclusione di un'articolata attività di indagine per truffa informatica in danno di numerosi clienti degli istituti di credito BPER Banca e Intesa San Paolo ha eseguito, con l'ausilio di personale del Centro Operativo per la Sicurezza Cibernetica di Napoli, un'ordinanza emessa dal G.I.P. del Tribunale di Salerno che disponeva l'esecuzione di tre misure cautelari degli arresti domiciliari e di due misure cautelari dell'obbligo di firma e l'esecuzione di 16 decreti di perquisizione locale e personale nei confronti di un gruppo criminale radicato nella provincia di Salerno, Potenza e Torre del Greco (NA), ma operante su tutto il territorio nazionale.
In particolare le vittime dei reati, contattate tramite l'invio di sms apparentemente riconducibili alla banca di appartenenza, venivano indotte a disinstallare dal proprio *device* l'applicazione della home banking, consentendo così ai truffatori, una volta reinstallata su propri dispositivi, di ottenere il controllo dei conti correnti ed effettuare le operazioni illecite, i cui importi totali raggiungevano i 450.000 mila euro.

Operazione Polo Est

Nel mese di maggio 2024, il Centro Operativo per la Sicurezza Cibernetica di Milano - a conclusione di un'articolata attività di indagine - ha eseguito, con l'ausilio di personale del Centro Operativo per la Sicurezza Cibernetica di Napoli e Reggio Calabria, 12 decreti di perquisizione personale, locale e di ispezione informatica a carico di soggetti di origine italiana, nigeriana e senegalese, attivi nelle province di Bergamo, Caserta, Milano, Reggio Calabria e Vicenza, a cui venivano contestati i reati previsti e puniti dagli artt. 61 n.7, 61 bis, 110, 629, 640 e 648 bis c.p.
L'attività in questione è ricollegabile al noto fenomeno degli invii massivi di email ad ignari cittadini, apparentemente provenienti da Autorità istituzionali, contenenti falsi riferimenti ad inesistenti procedure legali. Nella corrispondenza telematica oggetto di investigazione, riproducente falsi documenti governativi a firma di magistrati e funzionari di polizia, venivano contestate gravi violazioni, commesse attraverso la rete internet, legate a condotte penalmente rilevanti, riferite a delitti di pedopornografia e molestie sessuali, con la contestuale richiesta di denaro per far "decadere" le accuse e l'indicazione delle coordinate bancarie verso le quali corrispondere le somme estorte.

Smishing/vishing Croce Rossa Italiana – Comitato di Milano

Nel mese di maggio 2024 il Centro Operativo per la Sicurezza Cibernetica di Milano si attivava per una patita truffa, per un importo di 309 mila euro, subita dalla Croce Rossa Italiana - Comitato di Milano.

In particolare, un dipendente della Croce Rossa veniva indotto con l'inganno a collegarsi ad una pagina *web* riproducente la schermata di *login* della Banca Popolare di Sondrio, all'interno della quale l'ignara vittima inseriva le credenziali di accesso al conto. Successivamente, un falso operatore bancario, attraverso contatto telefonico, riusciva ad ottenere i codici OTP autorizzativi necessari al perfezionamento di vari ordini di pagamento verso IBAN di altri istituti di credito.

L'immediata attivazione del personale della Polizia Postale consentiva di bloccare la somma di circa 300 mila euro.

Operazione Spin Profiles

Nel mese di maggio 2024, il Centro Operativo per la Sicurezza Cibernetica di Milano - a conclusione di un'articolata attività di indagine - ha eseguito, con l'ausilio di personale del Centro Operativo per la Sicurezza Cibernetica di Napoli, Roma, Pescara e Reggio Calabria, 18 decreti di perquisizione locale e di ispezione informatica a carico di soggetti di origine italiana e rumena, attivi nelle province di Caserta, Frosinone e Napoli, a cui venivano contestati i reati previsti e puniti dagli artt. 81 cpv 110, 640 comma 1, comma 2 nr. 2 e nr. 2 bis, 61 nr. 5, 640 ter c.p.

L'attività in questione è da ricollegare al noto fenomeno del *phishing,* attraverso il quale i frodatori entrano in possesso delle credenziali dell'home banking degli ignari cittadini e dispongono operazioni in frode al fine di svuotare i loro conti. In particolare l'attività in questione ha avuto origine da una denuncia di Banca Profilo che aveva rilevato diversi episodi di *phishing* in danno di loro clienti, titolari di utenze Tinaba[4].

CEO Fraud Società tedesca NAKANISHI Jager GMbh

Nel mese di maggio 2024, la Sezione Operativa per la Sicurezza Cibernetica di Padova, riceveva una querela dal responsabile commerciale per l'Italia della Società tedesca NAKANISHI Jager GMbh, con la quale denunciava che la sede centrale della società per cui lavorava, era stata vittima di una truffa di tipo CEO Fraud, ed era stato disposto un bonifico di € 477.853 verso un IBAN italiano.

---

[4] Acronimo di "This is not a bank", questa non è una banca. Si tratta di una App fintech innovativa, sviluppata per offrire uno strumento completo per gestire il proprio denaro e sfruttare diversi servizi finanziari. Nata nel 2015, nel corso degli anni si è arricchita di numerose funzioni, tra cui un conto deposito e la compravendita di criptovalute. L'App è collegata a un conto corrente con IBAN italiano e a una carta prepagata e consente di inviare denaro ai propri contatti, nonché effettuare pagamenti in ambiente digitale, risparmiare e controllare le spese, raccogliere fondi, investire e sfruttare tutte le funzionalità tipiche di un conto bancario.

L'immediata attivazione del SOSC di Padova permetteva di far rientrare nella piena disponibilità della Società NAKANISHI l'intero importo frodato.

Operazione Black Hat

Nel mese di giugno 2024, personale del Centro Operativo per la Sicurezza Cibernetica di Trento, unitamente a personale del Comando Gruppo della Guardia di Finanza del medesimo capoluogo e con l'ausilio di personale della Sezione Operativa per la Sicurezza Cibernetica di Salerno, ha dato esecuzione - a conclusione di un'articolata, congiunta, attività di indagine - a un'ordinanza applicativa della misura cautelare degli arresti domiciliari emessa dal G.I.P. presso il Tribunale di Salerno a carico di due soggetti, di origine italiana e ucraina, a cui venivano contestati i reati in oggetto indicati previsti e puniti dagli artt. 615 ter e 640 ter c.p..

L'attività in questione è ricollegabile al noto fenomeno c.d. "*man in the middle*", una minaccia informatica in cui l'offensore è in grado di intercettare e manipolare il traffico internet e le comunicazioni di posta elettronica delle potenziali vittime.

In particolare, le indagini hanno avuto origine da due denunce presentate da società italiane che, rimaste vittime del fenomeno, permettevano di ricostruire circa 20 episodi in cui i criminali, mediante l'impiego di sofisticate tecniche informatiche e di *social engineering*, si intromettevano tra le comunicazioni *email* intrattenute da diverse società ed i loro fornitori, sostituendosi ai reali beneficiari dei pagamenti dei corrispettivi dovuti per beni e servizi acquistati e fornendo riferimenti bancari riconducibili a conti correnti nella loro disponibilità, realizzando complessivamente un giro d'affari quantificabile in circa 300.000 euro.

Operazione Energy Switch

Nel mese di giugno 2024, il Centro Operativo per la Sicurezza Cibernetica di Milano, a conclusione di un'articolata attività di indagine transnazionale, coordinata dal Servizio Polizia Postale ed effettuata in collaborazione con l'Ufficio dell'Esperto per la Sicurezza presso l'Ambasciata d'Italia a Tirana, ha eseguito nove decreti di perquisizione nei confronti di 21 indagati e delle sedi di due società energetiche e di 12 call center appaltati, tre dei quali ubicati in Albania.

Le attività sono state attuate attraverso un'azione congiunta a livello nazionale e internazionale, con l'esecuzione di una rogatoria finalizzata allo svolgimento delle perquisizioni a Tirana.

Le attività sul territorio italiano sono state svolte con l'ausilio di personale dei COSC di Roma, Napoli, Palermo e Venezia, a carico di soggetti di origine italiana, bulgara e albanese.

Agli indagati, attivi nelle province di Milano, Roma, Napoli, Caserta, Caltanissetta,

Venezia, Vicenza, Rovigo e Padova, è stato contestato il reato di associazione per delinquere, finalizzata alla truffa ed alla sostituzione di persona.
L'attività investigativa, scaturita dalla denuncia di un utente per attivazioni fraudolente di contratti luce e gas, ha consentito di disvelare una vera e propria organizzazione criminale, i cui sodali, fra i quali figurano amministratori, commercialisti, consulenti e dipendenti di società energetiche e di call center, adottavano una serie di condotte illecite, caratterizzate da un approccio professionale, con il fine di attivare falsi contratti luce e gas a nome di ignari cittadini.
In particolare, gli operatori dei call-center, utilizzando i dati delle vittime, interloquivano con le stesse, simulando di essere operatori del reale fornitore energetico, al fine di attivare contratti, attraverso la produzione di registrazioni artefatte anche con l'uso dell'intelligenza artificiale e l'apposizione di firme false.
Il giro di affari è quantificabile in circa nove milioni di euro ed ha riguardato oltre 1000 utenti truffati.

Cyberterrorismo

Il Servizio Polizia Postale svolge in via continuativa il monitoraggio del web al fine di individuare contenuti di propaganda estremista e di matrice terroristica; tale attività è svolta dalla I ^ Sezione Cyberterrorismo, incardinata presso il Servizio e dai dipendenti Centri Operativi per Sicurezza Cibernetica dislocati sul territorio.
Il target operativo di tale settore si concretizza nella prevenzione e repressione dei reati che utilizzano la dimensione virtuale per fini terroristici, minando l'ordine e la sicurezza pubblica per ragioni riconducibili sia a forme di fondamentalismo religioso, sia a forme di estremismo politico ideologico, anche in contesti internazionali.
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 **138.000** spazi web oggetto di approfondimento investigativo; tra questi, oltre **480** risorse digitali sono state oscurate poiché caratterizzate da un contenuto illecito.

Cooperazione internazionale

La I^ Sezione Cyberterrorismo costituisce il punto di contatto nazionale della rete *Europol IRU - Internet Referral Unit*, coordinata dal Centro E.C.T.C. di *Europol (European Counter Terrorism Center*), per il monitoraggio dei contenuti terroristici *online*. Partecipa, insieme agli operatori di polizia di altri paesi, ai cd. "*action day*" promossi in tale ambito, con notevoli risultati operativi.
Durante il primo semestre del 2024, si è provveduto a censire molteplici spazi di natura estremista; tale monitoraggio ha consentito di svolgere un "*RAD - Referral*

Action Day" sotto l'egida di Europol, che ha condotto all'oscuramento di 2000 contenuti dal tenore negazionista e suprematista, corrispondenti a circa 160 *url* riferibili a account presenti sui social e *app* di messaggistica.
L'Action Day è stato coordinato dall'Unità di riferimento per Internet dell'Unione Europea (EU IRU) e ha coinvolto le forze dell'ordine di 18 Paesi, che hanno lavorato in collaborazione con i principali fornitori di servizi online. L'attività in argomento ha rilevato un'ampia gamma di contenuti illeciti, tra cui il c.d. *hate speech* e la negazione dell'Olocausto, con l'obiettivo principale di rimuovere i contenuti illegali presenti sulla rete e garantire l'adesione delle piattaforme *online* alle normative europee in materia di discriminazione razziale.
Risulta necessario, pertanto, garantire l'esecuzione di una costante attività di monitoraggio investigativo della rete per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione *online* dei contenuti illeciti, assicurando uno scambio informativo strutturato con la Direzione Centrale della Polizia di Prevenzione e con le agenzie di *intelligence*, competenti in materia di contrasto al terrorismo.

Estremismo religioso

L'attività funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione estremista di tipo religioso ha permesso di acquisire ampi spazi informativi in contesti eterogenei.
Nello scenario contemporaneo, contraddistinto dal perseverare di diversi conflitti bellici, tra cui i principali, (Russo-Ucraino e Israelo-Palestinese), si possono annoverare diverse diramazioni dell'Islam radicale. Alcune di esse sono associate a specifici spazi territoriali del Medio Oriente, Penisola Araba, Africa, Asia centrale e meridionale; in questi contesti, i gruppi islamisti possono esprimere risorse logistiche, militari o addirittura para-statuali. Altre diramazioni, risultano estese a contesti occidentali, in cui il fenomeno diventa meno geo-referenziabile e, al contempo, più sensibile ad una propagazione *online*. Tra le principali correnti dell'Islam jihadista e relativi centri mediatici monitorati si annoverano tanto i gruppi afferenti ad *Al Qaeda* (AQAP - Al-Qaida in Yemen, JNIM - Jamaat Nusrat al Islam) quanto l'organizzazione terroristica *Daesh,* attiva principalmente con le formazioni Islamic State Khorasan Province (ISKP) in Afghanistan, ISIS-Khorasan in Pakistanz, le province IS – West Africa, Sahel, Mozambico e Sham (Siria).
Con riferimento specifico al conflitto Israelo-Palestinese e, soprattutto, dall'inizio dell'operazione *"al-Aqsa Flood"*, peculiare attenzione è stata riservata al movimento islamico - radicale HAMAS e alle formazioni militanti delle Brigate Izz al-Din al-Qassam, le Brigate Al-Quds, le Brigate dei Martiri di al-Aqsa, il gruppo Jund Ansar Allah e altri collegati.

Oltre all'Hamas Media Office e ai suoi canali ufficiali, va rilevato come la propaganda estremista anti-Israeliana e pro Hamas sia incrementata sulla chat Telegram, anche con la trasmissione in live di azioni di guerriglia verso le comunità israeliane.
La propaganda radicale di Hamas è, inoltre, a volte oggetto di adesione da parte di gruppi e movimenti antagonisti che si riconoscono nella narrativa della resistenza Palestinese (c.d "intifada studentesca"), condividendo anche il ricorso a tecniche violente.
L'attività di ricerca e acquisizione informativa svolta da parte della Sezione cyberterrorismo e dai dipendenti COSC sulle tematiche descritte fa ricorso in via sistematica all'ausilio di mediatori culturali di lingua araba, il cui apporto consente di interpretare in tempo reale i contenuti multimediali originali diffusi sul web dai centri di propaganda citati.

Terrorismo accelerazionista

Sono state svolte attività investigative sul fenomeno del cyberterrorismo di matrice accelerazionista/neo-nazista, che hanno consentito di delinearne l'estrema attualità, individuando con opportuno anticipo il pericoloso decorso di processi di radicalizzazione individuale, in particolare, nelle fasce di utenti minorenni o di giovane età.
Il fenomeno ha assunto un'importante dimensione, in particolare negli USA, nel Regno Unito e in alcuni paesi dell'Unione Europea, stati in cui le note sigle *"AWD - AtomWaffenDivision"* e *"The Base"* hanno dimostrato un maggiore radicamento territoriale, oltre che la presenza di figure di vertice e di esponenti protagonisti di atti violenti. Si sottolinea, inoltre, che la sigla "The Base" è stata di recente riconosciuta come sigla terroristica dall'Unione Europea, con la decisione nr. 2024/2055 del Consiglio.
Le diramazioni di tali gruppi, in numerosi *spin off* derivati, nonché le affiliazioni estemporanee di singoli soggetti, sono agevolate da una propagazione di fondo di contenuti mediatici (video, locandine, meme, audio) con una forte attrattiva visiva, mutuata dall'estetica del *gaming* online di tipo "*warfare*".

Contrasto alla disinformazione

È noto come le piattaforme virtuali di comunicazione rappresentino uno degli ambienti più agevoli per la diffusione di notizie false, inattendibili o non verificabili, che possono incidere sui processi di formazione del consenso elettorale nonché, più in generale, sulla percezione dei fenomeni sociali da parte della sfera pubblica, tali da orientare correnti di opinione e pensiero. A ciò si aggiunga, inoltre, che la divulgazione e replicazione virale di contenuti falsi, oltre a disorientare la cittadinanza, impedendo la corretta comprensione di fatti sensibili, può comportare ripercussioni nella

gestione dell'ordine e sicurezza pubblica.
Tra le tematiche sensibili di più stringente attualità per un potenziale inquinamento mediatico, anche in correlazione ai conflitti bellici in corso, si possono annoverare le consultazioni elettorali, momento critico di formazione del consenso democratico della cittadinanza.
Per quanto attiene le specifiche attività di competenza del Servizio Polizia Postale, la tematica della disinformazione ha assunto peculiare rilievo a seguito della diffusione di tecnologie improntate sui modelli dell'intelligenza artificiale generativa, che consentono di generare con rapidità immagini e video di tipo "*deepfake*", solo in apparenza attendibili, che possono indurre in errore anche gli esperti di comunicazione mediatica, oltre che la cittadinanza. A ciò si aggiunga l'esistenza di servizi di tipo "*crime as a service*", quali, ad esempio, l'attivazione virale di bot, finalizzati a generare confusione e dubbio nella platea elettorale, diminuendo la fiducia negli attori politici, spesso vittime di mirate strategie di "impersonificazione", anche attraverso tecniche di *hacking* volte a sottrarre la disponibilità degli account istituzionali per la successiva pubblicazione di *fake news*.
Tale volume informativo nocivo impedisce di cogliere le informazioni autentiche e costringe le fonti attendibili ad una continua opera di smentita dei contenuti falsi posti in circolazione.
L'uso malevolo dell'intelligenza artificiale, volta a tecnica di misinformazione / disinformazione, è stato già individuato dal *Global Risks Perception Survey* 2023-2024 del *World Economic Forum* come grave pericolo a livello globale, scalando significativamente il ranking delle minacce.
Si consideri, ad esempio, l'incidenza che le strategie di disinformazione possono assumere sui processi di composizione democratica degli organi dell'Unione Europea e delle assemblee rappresentative nazionali, in particolare nel caso in cui vadano a determinare situazioni di astensionismo diffuso, che di fatto impediscono a monte la percezione dell'orientamento politico degli elettori.
Nell'ambito della disinformazione, il Servizio Polizia Postale ha svolto un monitoraggio dei profili *fake* di soggetti istituzionali, quali, ad esempio, il Presidente della Repubblica Mattarella, segnalando ai social network, nel semestre, oltre 50 profili per la conseguente chiusura in quanto ingannevoli.

Si riepilogano di seguito le attività di maggiore rilievo condotte nel corso del primo semestre del 2024.

Operazione internazionale contro l'extremismo neonazista

Il Centro Operativo per la Sicurezza Cibernetica di Torino ha svolto un'articolata attività investigativa nel contesto dell'estremismo accelerazionista di matrice neonazista,

sotto il coordinamento delle Agenzie Eurojust ed Europol. L'operazione ha coinvolto diversi paesi europei e ha portato all'arresto dei principali esponenti di una rete terroristico-accelerazionista denominata "*SturmJager Division*", affine a sigle note quali *"Atom Waffen Division"*, *"Sonnenkrieg Division"*, *"FeuerKrieg Division"* e *"The Base"*.
In tale contesto, si è proceduto ad eseguire nei confronti di due indagati italiani la misura cautelare dell'obbligo di permanenza domiciliare.

Indagine sul profilo instagram: incitamento alla violenza e costruzione di esplosivi

Il Centro Operativo per la Sicurezza Cibernetica di Roma ha svolto un'attività investigativa originata da una segnalazione pervenuta al Commissariato di PS online nel mese di febbraio, inerente un profilo Instagram che, a seguito dei disordini verificatisi a Pisa durante le manifestazioni studentesche del 23 febbraio, incitava al ricorso alla violenza nei confronti delle forze dell'ordine, invitando anche alla realizzazione domestica di esplosivi con materiale facilmente reperibile in commercio. Il titolare veniva identificato e sottoposto a perquisizione ex art. 41 TULPS.

Indagine su minacce antisemite: identificato responsabile

I Centri Operativi per la Sicurezza Cibernetica di Roma e Bologna, a seguito di segnalazione giunta dall'Unione delle Comunità Ebraiche Italiane, hanno svolto un'indagine concernente alcune mail minatorie indirizzate ai referenti della Comunità, in cui il mittente faceva riferimento esplicito alla disponibilità di armi e alla possibilità concreta di utilizzarle per atti violenti. Gli accertamenti hanno consentito altresì di verificare che il responsabile, identificato per un cittadino residente a Parma, gestiva un blog di matrice esplicitamente antisemita.

Operazione del C.O.S.C. di Bologna: sequestro di sostanze chimiche e video-tutorial su hacking

Il Centro Operativo per la Sicurezza Cibernetica di Bologna ha svolto un'attività investigativa che ha condotto alla perquisizione di un soggetto attivo nella pubblicazione online di istruzioni per la costruzione di ordigni artigianali. Nel corso della perquisizione, sono stati rinvenuti e sottoposti a sequestro sostanze chimiche idonee alla preparazione di esplosivi. L'indagato è risultato altresì amministratore di un canale all'interno del quale venivano pubblicati video-tutorial inerenti a un software idoneo a svolgere attività di *hacking*.

Arresto di un indagato per detenzione di armi 3d e contenuti terroristici

Nel mese di maggio, nell'ambito di un'attività investigativa coordinata dalla Procura

di Roma, il Servizio Polizia Postale ha eseguito, congiuntamente alla DIGOS di Roma, alla D.C.P.P., alla Polizia Scientifica e al Reparto Cinofili, una perquisizione nei confronti di un soggetto detentore di armi realizzate attraverso la tecnica della stampa 3D. L'indagato risultava altresì detenere, sui propri dispositivi, file video riproducenti esecuzioni capitali, decapitazioni e mutilazioni corporali, video a tema terroristico, razziale e antisemita. In considerazione della disponibilità di armi, il soggetto è stato tratto in arresto in flagranza di reato per "produzione e detenzione di arma clandestina" ex art. 23 L 110/1975.
Il GIP del Tribunale di Roma ha provveduto a disporre la misura degli arresti domiciliari.

Attività di contrasto all'hate speech e ai crimini d'odio nel primo semestre del 2024

Nell'ambito del contrasto al c.d "*hate speech*" e ai crimini d'odio sono state trattate, nel primo semestre del 2024, 18 segnalazioni provenienti dall'OSCAD.
Sono state avviate inoltre, d'iniziativa della Sezione cyberterrorismo del Servizio Polizia Postale, trenta attività d'indagine concernenti profili attivi, in particolare sul social network russo *VKontate*, responsabili di propaganda xenofofa, antisemita e negazionista dell'olocausto.

Attività di contrasto alla disinformazione durante le elezioni europee

Nel solco del contrasto alle campagne di disinformazione, il Servizio Polizia Postale ha individuato e gestito, in via preventiva, un'iniziativa di boicottaggio delle ultime elezioni europee da parte di un gruppo già noto per le posizioni negazioniste in materia di Covid 19, per il contrasto alle correlate campagne vaccinali, nonché per la forte impronta anti-sistemica.

Commissariato di P.S. online

L'uso crescente delle nuove tecnologie ha reso necessario il potenziamento di nuovi strumenti di comunicazione che consentissero il contatto diretto tra Polizia di Stato e utenti del web.

In tale ottica, il portale del Commissariato di PS online, raggiungibile attraverso la url https://www.commissariatodips.it/, permette a chiunque di rivolgersi agli operatori della Polizia Postale preposti alla ricezione delle segnalazioni e delle richieste di informazioni, in qualsiasi momento della giornata e ovunque si trovi.

Il sito, infatti, costituisce ormai da anni un importante strumento di interazione con i cittadini che ogni giorno inviano in media **300** messaggi per segnalare siti con con-

tenuti illegali o possibili reati informatici, esprimere il proprio disagio per un torto subito, evidenziare comportamenti che giudicano illeciti e chiedere aiuto per superare difficoltà e problematiche.

È proprio in questi ultimi casi che l'accesso al portale esprime al meglio le sue potenzialità, favorendo l'emersione di problematiche che, per la loro delicatezza, difficilmente sarebbero rappresentate attraverso un contatto *de visu* e sicuramente non senza un estremo disagio per l'utente.

La facilità con cui il cittadino interagisce con la piattaforma dedicata rende possibile, inoltre, la raccolta delle segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione, si rivolgono alla Polizia Postale in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti possano cadere nelle trappole della Rete.

L'analisi delle **oltre 56.000 richieste tra segnalazioni e informazioni** ricevute dal portale nel primo semestre dell'anno 2024 ha evidenziato che in molti casi gli utenti del web non adottano quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose.

In tal senso, al fine di migliorare l'attività preventiva, è stata ampliata la sezione dedicata agli *alert* dove vengono raccolti e pubblicati gli avvisi agli utenti che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela e prevenzione messo a disposizione del cittadino.

Tra i fenomeni riscontrati con maggior frequenza nel primo semestre dell'anno 2024 si possono annoverare, a titolo esemplificativo, le truffe basate sulla tecnica dello *spoofing* che, replicando numerazioni di uffici di polizia o istituti di credito, inducono le vittime a trasferire i loro risparmi su conti fraudolenti; le campagne massive di *smishing*, sms fraudolenti che informano di presunti accessi anomali su conti correnti bancari al fine di carpire i dati di accesso delle vittime; i furti di profili social e false comunicazioni di assistenza per il recupero degli account rubati. È in progressiva crescita il numero delle segnalazioni di estorsioni a sfondo sessuale, di truffe sugli acquisti online e di false proposte di investimenti online.

L'attività più delicata che gli operatori del Commissariato di PS online sono chiamati a svolgere quotidianamente riguarda la gestione delle numerose segnalazioni di cittadini che manifestano situazioni di disagio, minacciando di compiere gesti estremi. Nel primo semestre del 2024 gli **interventi dedicati** alla prevenzione correlata a

intenti suicidari sono stati **118**. Le richieste di aiuto, in alcuni casi, vengono inviate direttamente dagli utenti sul sito tramite il servizio "Segnala online"; in altri casi, sono ricevute dalla redazione di note trasmissioni televisive che, successivamente, le inoltrano al Commissariato di PS online. In tali circostanze agli operatori del Centro è richiesto un tempestivo e coordinato intervento che coinvolge anche gli uffici territoriali delle Forze dell'ordine per raggiungere nel più breve tempo possibile la persona in pericolo.

La popolarità del sito è avvalorata dal numero degli accessi[5] che, nel periodo di riferimento, sono stati **26.392.596**.

Segnalazioni pervenute al Commissariato di P.S. online nel primo semestre 2024	**ANTITERRORISMO**	673
	HACKING	13.661
	PEDOPORNOGRAFIA	955
	PHISHING	12.844
	SOCIAL	16.380
TOTALE		**44.513**

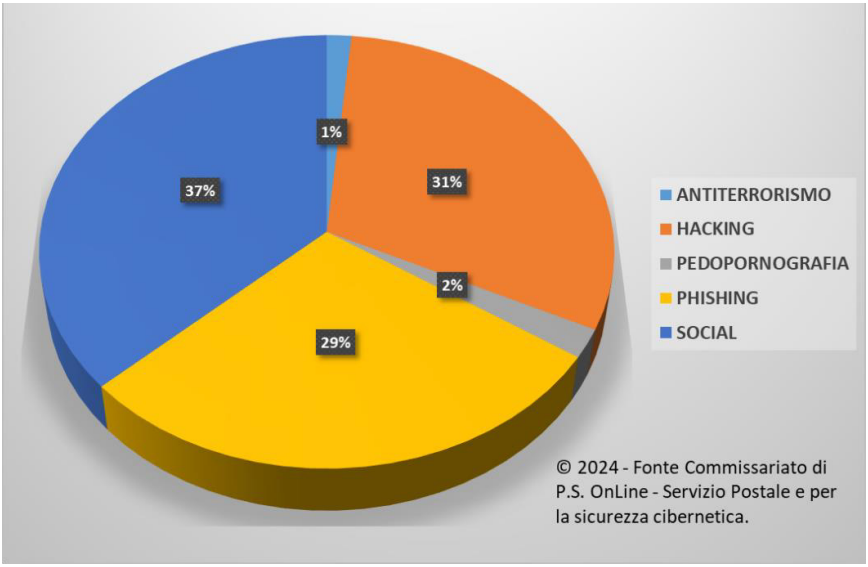
Richieste di informazioni pervenute al Commissariato di P.S. online nel primo semestre 2024	**11.843**

Visite al portale web del Commissariato di P.S. online nel primo semestre 2024	**1.359.185**

Accessi al portale web del Commissariato di P.S. online nel primo semestre 2024	**26.392.596**

[5] Riferibile al numero di pagine visionate in occasione di una "visita" al sito.

TIPOLOGIA SEGNALAZIONI INOLTRATE DAI CITTADINI ATTRAVERSO IL PORTALE www.commissariatodips.it
Primo semestre 2024



Campagne preventive di sensibilizzazione

Nell'ambito dell'attività di prevenzione svolta dalla Specialità, oltre al monitoraggio continuo della rete, la Polizia Postale e per la sicurezza cibernetica è impegnata costantemente nella progettazione e realizzazione di campagne di sensibilizzazione e di educazione al corretto uso delle tecnologie, nel tentativo di far comprendere agli adolescenti, che talora non ne percepiscono a pieno il disvalore, le conseguenze che possono derivare dall'uso distorto della rete.
Una coinvolgente campagna realizzata periodicamente è il format teatrale **#cuoriconnessi**, dedicato agli studenti delle scuole, con il quale, attraverso uno spettacolo in cui il conduttore concentra l'attenzione del pubblico sull'importanza delle parole in tutte le sue sfumature, con filmati, letture, musiche e testimonianze dirette, vengono fornite agli spettatori informazioni utili alla corretta navigazione in rete, volte anche a stimolare nei ragazzi una sempre maggiore consapevolezza della gravità delle azioni commesse online, in relazione all'impatto prodotto nella vita dei loro coetanei.
Nell'anno 2024, l'evento relativo alla **8^ edizione** della campagna "Cuoriconnessi" si è svolto lo scorso **6 febbraio** nell'ambito del "***Safer Internet Day - giornata mon-***

diale per la sicurezza in rete" ed è stato seguito **in diretta *streaming*** da **più di 225 mila studenti**.

Permane tra le iniziative più significative, la campagna itinerante per l'Italia, denominata **"Una vita da Social"**, in collaborazione con il Ministero dell'Istruzione e del Merito nell'ambito del progetto "Generazioni Connesse", che ha travalicato negli ultimi anni anche i confini nazionali e della quale sono state già realizzate undici edizioni. A bordo dell'iconico *truck* simbolo dell'iniziativa, che si trasforma in una vera e propria aula multimediale, gli operatori della Specialità incontrano numerose scolaresche e cittadini, a cui illustrano le più attuali insidie della rete e forniscono utili strumenti per un corretto utilizzo del *web*.

Nel corso dell'**11^ edizione,** relativa all'**anno scolastico 2023/2024**, sono stati veicolati contenuti educativi a circa **400.000 studenti, a oltre 25.000 docenti** e circa **28.000 tra genitori e partecipanti**.

Oltre all'esperienza estera nell'ambito di "Una vita da social", nel maggio di quest'anno, operatori del Servizio Polizia Postale e per la sicurezza cibernetica si sono recati ad Atene per degli incontri educativi di prevenzione e sensibilizzazione sui rischi e pericoli della rete, rivolti agli studenti della Scuola Italiana di Atene[6], che è una delle 8 scuole italiane attive all'estero.

Dopo l'intenso lavoro svolto durante il periodo scolastico, è proseguito l'impegno a favore dei ragazzi per limitare la loro esposizione ai possibili rischi derivanti da un uso inappropriato di Internet, anche nel periodo estivo.
Il 28 giugno u.s. a Roma ha avuto inizio il "***Cybersummer***", una nuova iniziativa di educazione al digitale, promossa dalla Polizia Postale e per la sicurezza cibernetica presso i centri estivi e i luoghi di aggregazione giovanile sostitutivi dell'attività scolastica. Considerato che, nel periodo estivo, i ragazzi, liberi dai tanti impegni scolastici, tendono a trascorrere molto tempo sul web, si è inteso rivolgere a loro questa iniziativa, per discutere insieme dei rischi e delle opportunità che la rete offre e per renderli più consapevoli e responsabili nell'uso dei dispositivi informatici.

Sono state realizzate, infine, con enti e aziende di trasporto pubblico, anche a livello locale con il coinvolgimento delle strutture territoriali della Specialità, "pillole" sulla sicurezza in rete per la diffusione dei contenuti attraverso i loro canali informativi rivolti all'utenza. È stato così possibile per il cittadino ascoltare consigli su come proteggere le proprie password, difendersi dalle truffe on line, non cadere nelle trappole della rete, sui mezzi pubblici, nelle sale di attesa degli aeroporti e presso le Università.

---

[6] Istituto composto dalla scuola primaria, secondaria di primo grado e dal Liceo Scientifico.

Analisi dei principali attacchi noti del primo semestre 2024 verso il settore Manufacturing a livello globale e in Italia

Presentiamo qui alcune informazioni a complemento dei dati del rapporto Clusit 2024 con la situazione degli 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 (2018-23).
Nel rapporto sono presentati i dati globali, separando poi gli attacchi globali da quelli verso il nostro paese.
Nelle tabelle, la prima a livello globale e la seconda in Italia, sono indicati 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	1H 2024	TOTALE
Cybercrime	21	24	58	68	116	149	76	512
Hacktivism	0	0	0	0	4	7	5	16
Espionage / Sabotage	10	12	6	4	9	6	1	48
Information Warfare	3	0	1	0	0	0	0	4
Totale MFG per anno	34	36	65	72	129	162	82	580
Totale attacchi per anno	1554	1667	1874	2049	2489	2779	1557	13969
% attacchi MFG su Totale dell'anno	2.2%	2.2%	3.5%	3.5%	5.2%	5.8%	5.3%	4.2%
% Crescita MFG anno su anno	0.0%	5.9%	80.6%	10.8%	79.2%	25.6%		

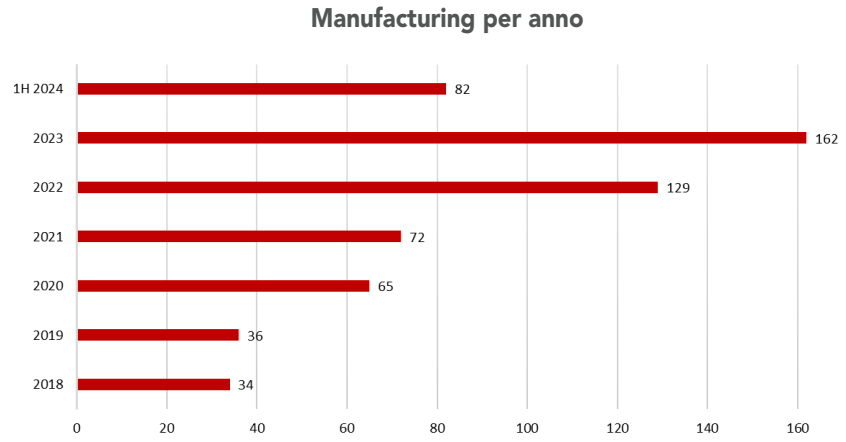
A livello Italia

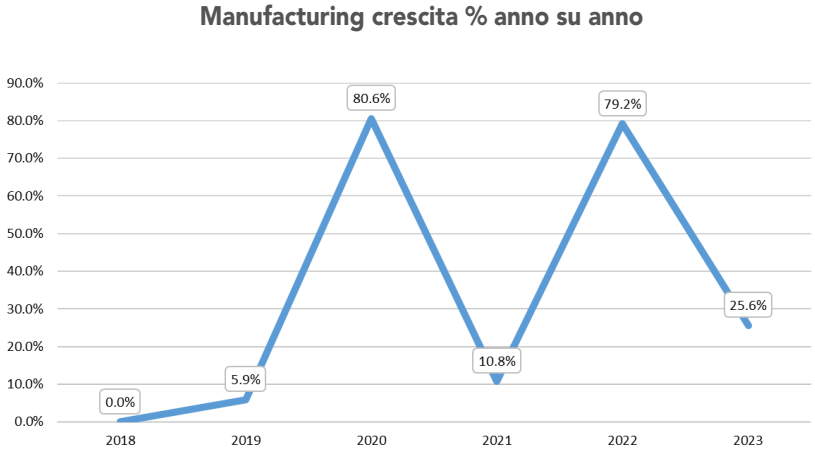
ATTACCANTI	2018	2019	2020	2021	2022	2023	1H 2024	TOTALE
Cybercrime	0	0	8	12	35	41	21	117
Espionage / Sabotage	2	2	1	0	0	0	0	5
Information Warfare	0	0	0	0	0	0	0	0
Hacktivism	0	0	0	0	0	0	1	1
Totale MFG per anno	2	2	9	12	35	41	22	123
Totale attacchi per anno	1554	1667	1874	2049	2489	2779	1557	13969
% attacchi MFG su Totale dell'anno	0.1%	0.1%	0.5%	0.6%	1.4%	1.5%	1.4%	0.9%
% Crescita MFG anno su anno	0.0%	0.0%	350.0%	33.3%	191.7%	17.1%		

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 2023, quella del primo semestre 2024 e i trend 2018-1H24.

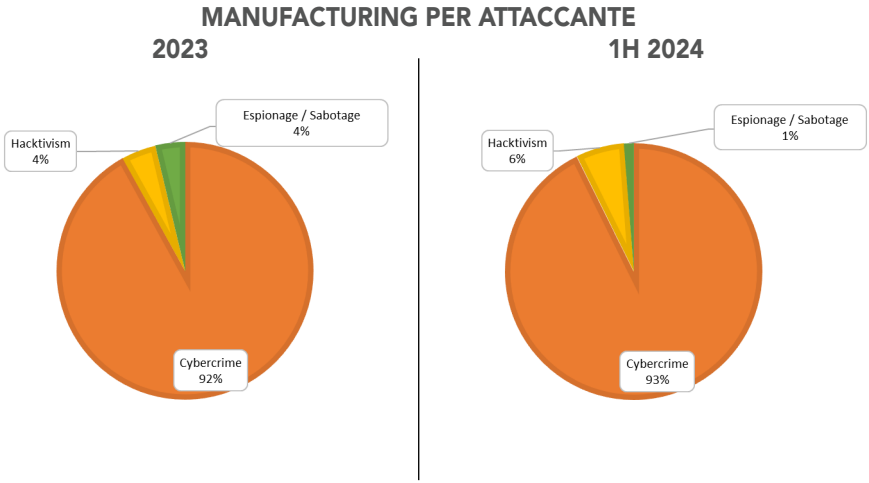
Riassumendo la situazione: gli attacchi verso il settore Manufacturing sono cresciuti, con un raddoppio tra il 2019 e il 2021, fino ad arrivare al loro massimo storico nel 2022 (+79% rispetto al 2021). Come vediamo il 2024 è cresciuto sul 2023, ma non si è registrato l'incremento temuto. Infatti nel primo semestre 2024 gli attacchi MFG hanno sostanzialmente raggiunto la metà del totale registrato nel 2023 e quelli generali sono aumentati di circa il 10%.





© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

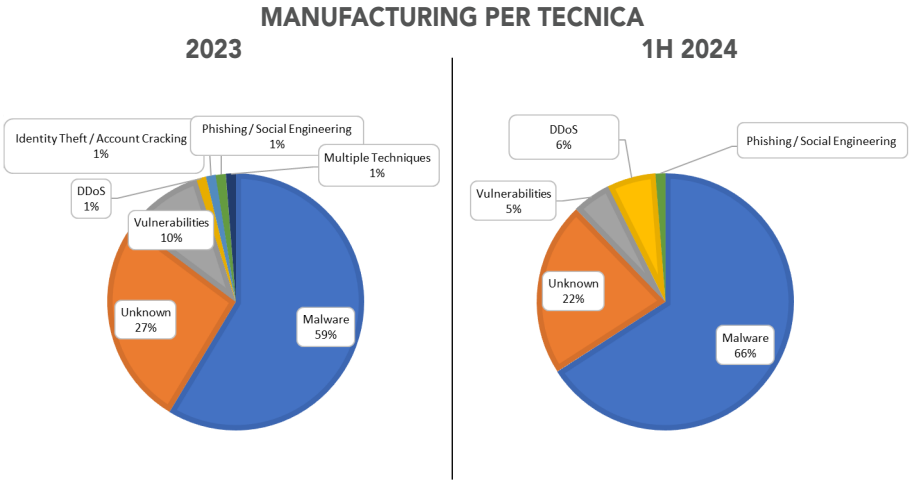
Il Cybercrime si conferma la minaccia principale per questo settore con oltre il 93% dei casi, con minime percentuali di Hacktivism ed attività di intelligence (sempre parecchio problematiche da attribuire).



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

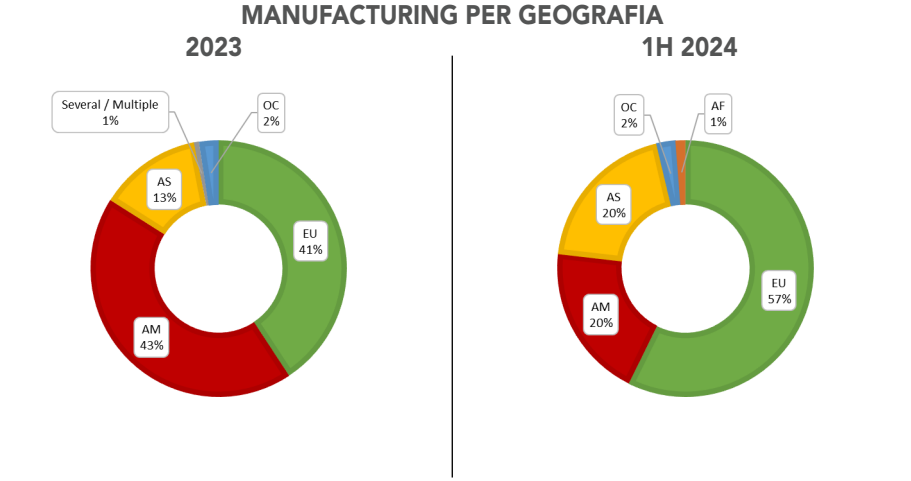
Il Malware (nello specifico ransomware) è salito al 66% nel 2024. Si noti che nel 2024 gli 0-Day rimangono alti (22 %) ma sono in calo così come le vulnerabilità non

patchate mentre crescono sensibilmente i DDoS e si riducono gli attacchi di ingegneria sociale. La "pesca a strascico" è meno onerosa e rende sempre.



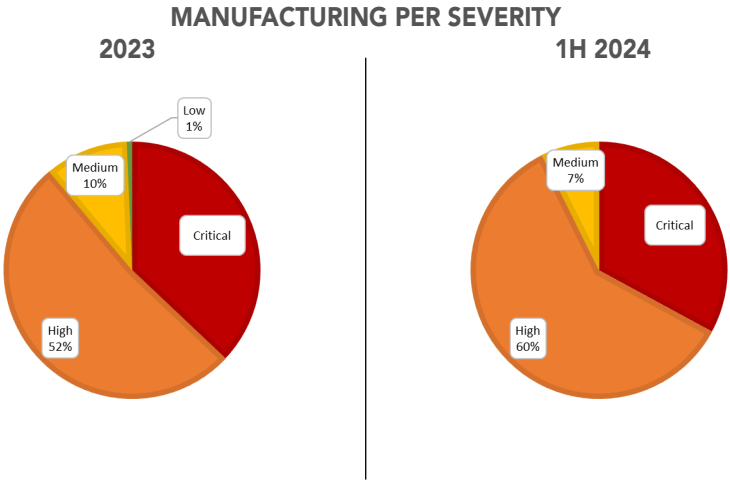
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

L'America risorpassa l'Europa nel 2023, arrivando a coprire il 43% degli attacchi verso il settore, ma nei primi 6 mesi del 2024 L'Europa riprende lo scettro tornando stabilmente sopra al 50%. Seguono a pari merito America ed Asia e pochissimi verso location multiple. (Da valutare meglio la consistenza dei numeri relativi ad attacchi nel "Rest Of the World", ovvero Oceania ed Africa che risultano poco rappresentativi).



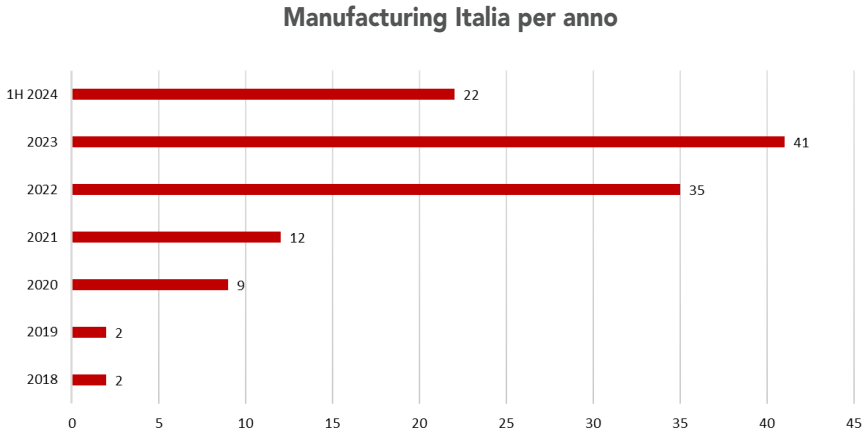
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Gli attacchi con impatti critici erano poco oltre il terzo nel 2023 (37%) e sono ulteriormente scesi al 33% nel 2024 (vedremo poi cosa succede alla fine dell'anno).



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

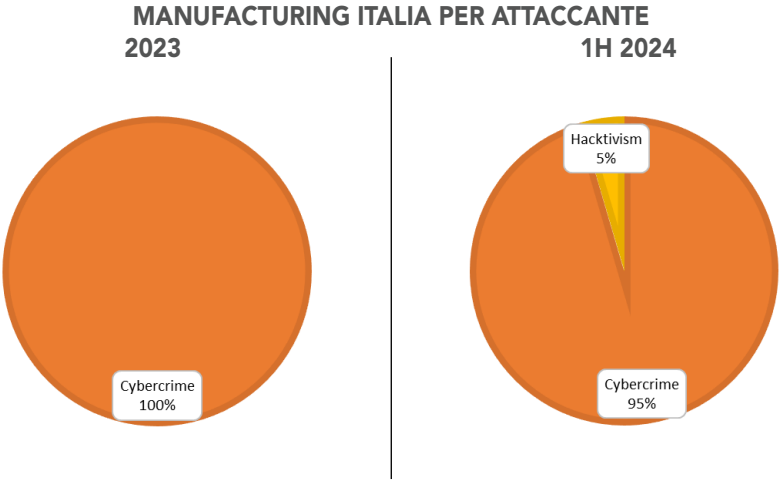
Per quanto riguarda l'Italia invece: nel 2023 gli attacchi verso il settore sono cresciuti in maniera percentualmente quasi conforme al trend mondiale rimanendo inoltre l'1,4% di quelli mondiali



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

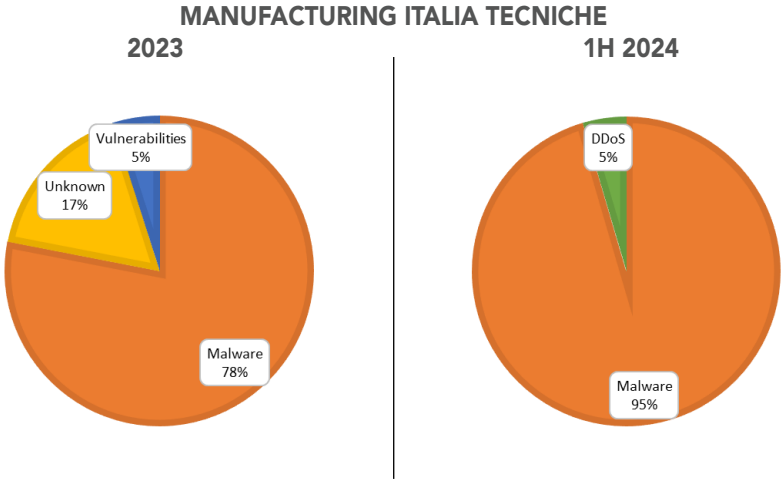
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Il Cybercrime si conferma la minaccia principale per questo settore con oltre il 95% dei casi (in Italia si verifica quasi il 100% ogni anno.)



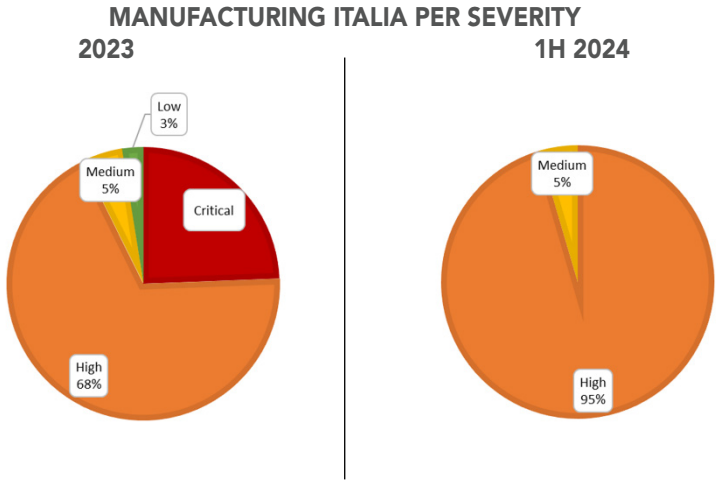
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Il Malware (nello specifico ransomware) e' salito al 95% 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. Il panorama è meno complesso di altre nazioni.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Per i danni creati dagli attacchi quest'anno sembra migliore del precedente che aveva il 24% di Critical severity (i chiodi impattano sulla continuità operativa, non sulla cybersecurity). Comunque un 95% di High non è da sottovalutare.

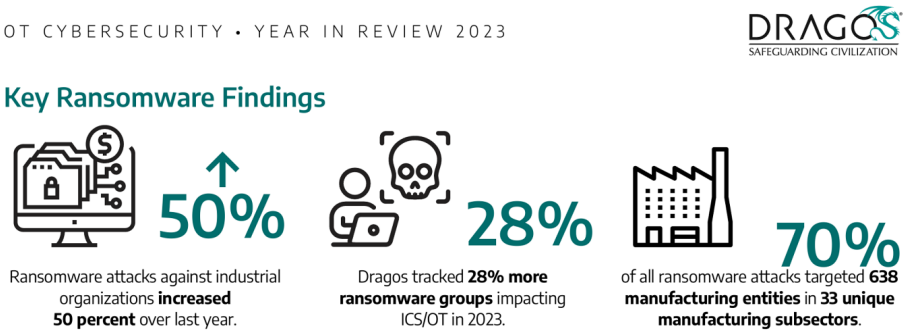


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Alcuni dati dal Report Dragos ICS/OT CyberSecurity Year in Review 2023

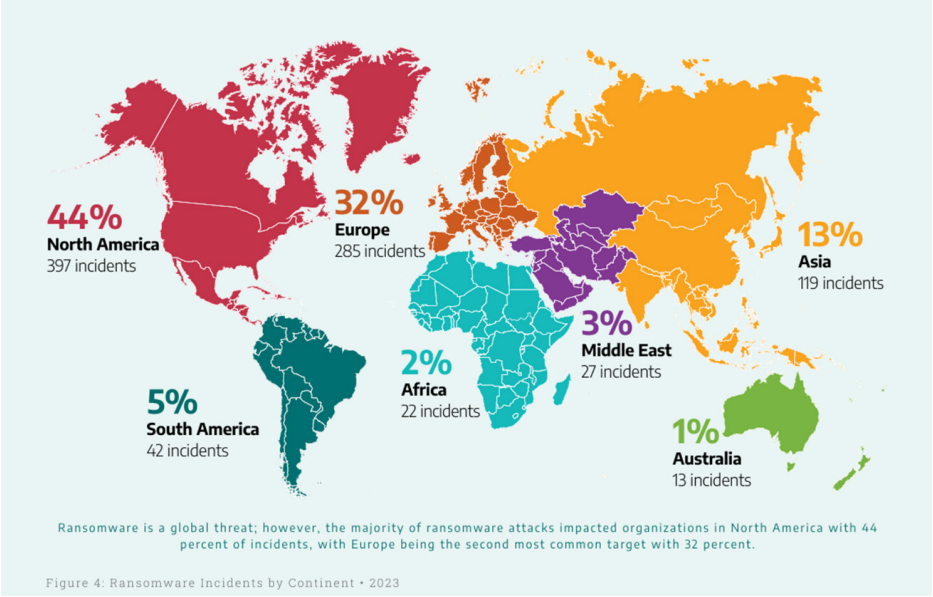
Volendo confrontare i dati del rapporto CLUSIT con altre fonti a livello internazionale, possiamo approfondire l'aspetto del Malware/Ransomware con alcune informazioni contenute nel Report Dragos ICS/OT CyberSecurity Year in Review 2023.

Da questo report possiamo constatare che il Ransomware ha colpito Impianti e sistemi ICS/OT con un aumento del 50% rispetto all'anno precedente, e vediamo anche un aumento del 28% dei gruppi criminali che utilizzano questa tecnica con l'obiettivo di colpire i sistemi di fabbrica.



Inoltre la suddivisione degli attacchi ransomware a livello geografico vede i seguenti numeri:

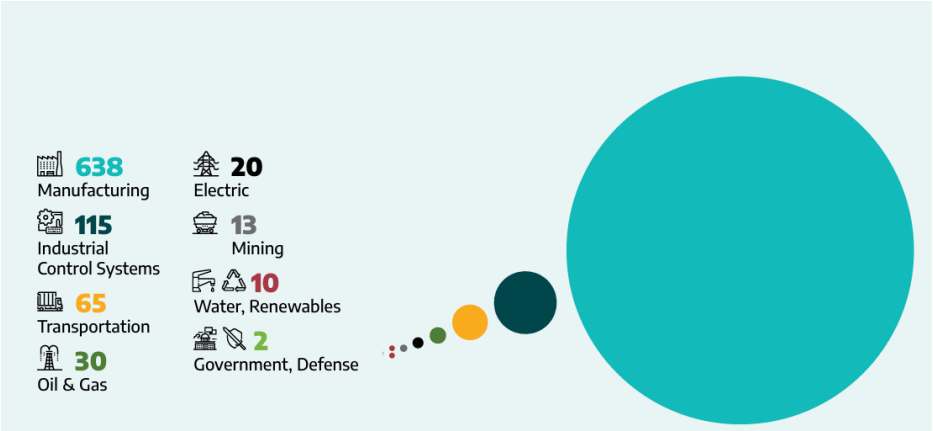
- 44+5 = 49% Americhe (Nord e Sud)
- 32% Europa (stimiamo 3-4% Italia)
- 13+3+2+1 = 19% MEA/Asia/Oceania



Ransomware is a global threat; however, the majority of ransomware attacks impacted organizations in North America with 44 percent of incidents, with Europe being the second most common target with 32 percent.

Figure 4: Ransomware Incidents by Continent • 2023

Si noti che subito dopo il manufatturiero generalista (71%) i secondi più attaccati sono i costruttori di SCADA (13%).



The most common sector impacted in 2023 was manufacturing, with 71 percent of ransomware incidents.
The industrial control systems sector, which is made up of companies that develop OT equipment and applications, was the second most impacted sector with 13 percent.

Figure 5: Ransomware Incidents by Sector • 2023

Per quasi tutti le problematiche di protezione più complesse sono legate alla segmentazione delle reti.

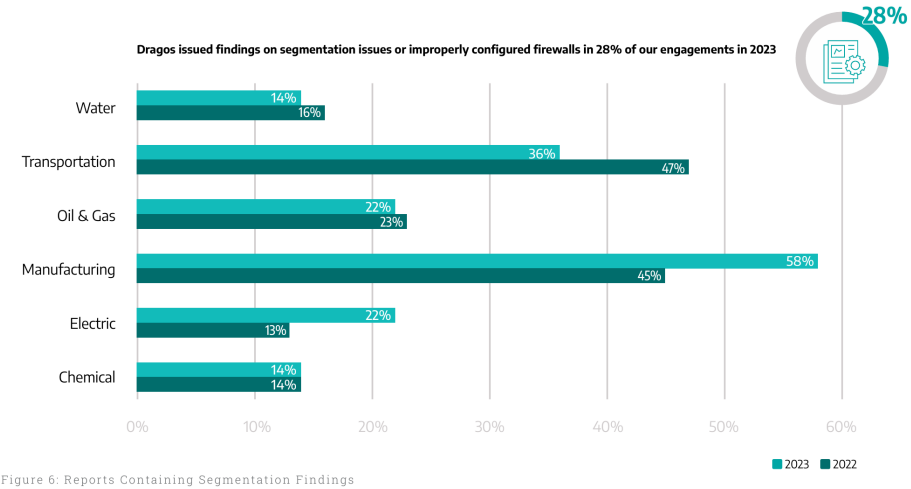


Figure 6: Reports Containing Segmentation Findings

Alcuni dati dal Microsoft Digital Defense Report (Oct. 2023 e Oct.2024)

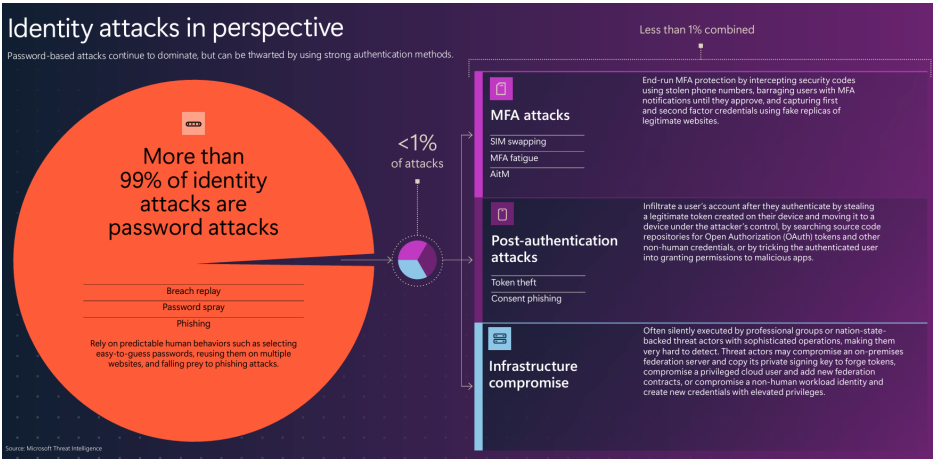
Valutando il livello di esposizione a Vulnerabilità, censite come CVE (Common Vulnerability Exposure) riguardo a sistemi OT/IoT/IIoT, abbiamo alcuni dati che qui riportiamo:

- 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):



Alcuni dati dal SANS ICS/OT CyberSecurity Survey (Oct.2024)

Dal periodico Survey di SANS veniamo a conoscenza che per il 2023-2024 sono stati intervistate oltre 500 persone che gestiscono oltre 1760 Impianti industriali/Utility. 78 Europei (10%) con 190 Impianti (18%).

Sono censite oltre 60 categorie industriali. Possiamo stimare che ci siano circa una decina di Italiani con 20-30 impianti sul nostro territorio (**Figura 1**).

Il dato sulle certificazioni è molto interessante, soprattutto su quanti non riescano a mantenerle per problemi di tempo (**Figura 2**).

Sui vettori di attacco sugli incidenti rilevati (quasi la metà dalla rete non OT - **Figura 3**).

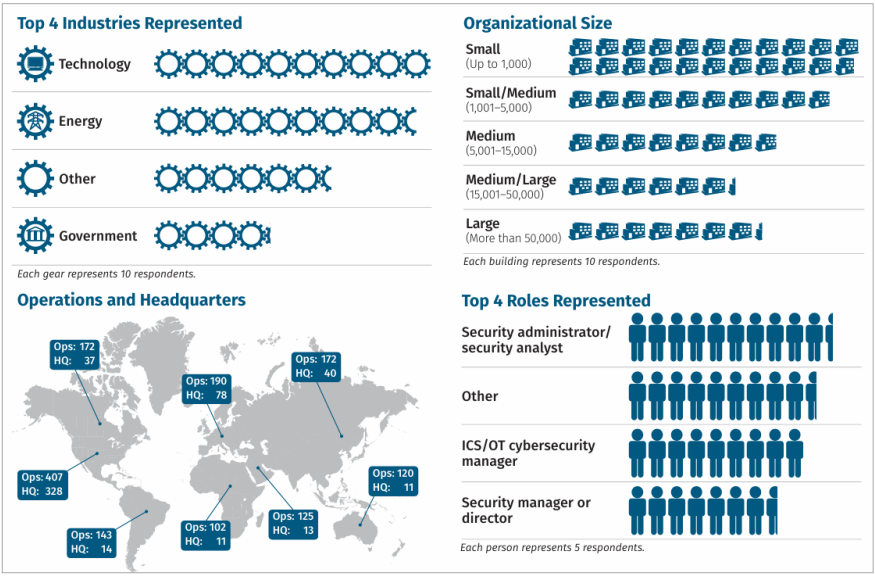


Figura 1

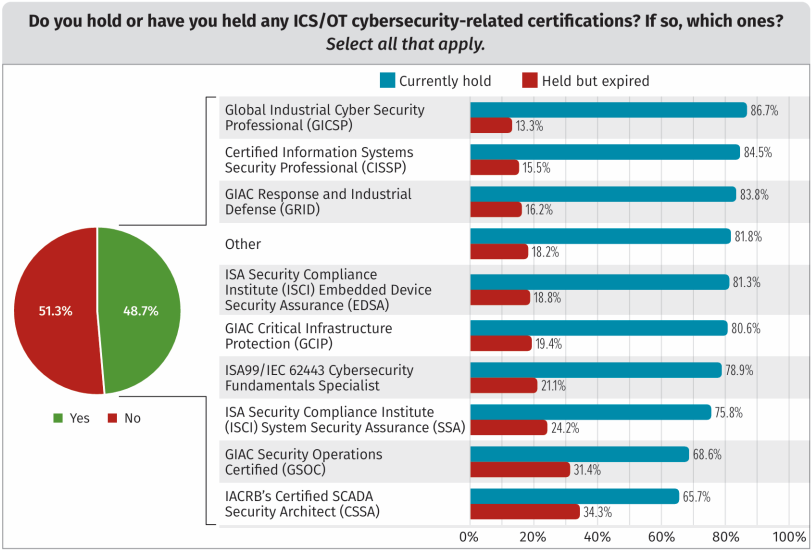


Figura 2

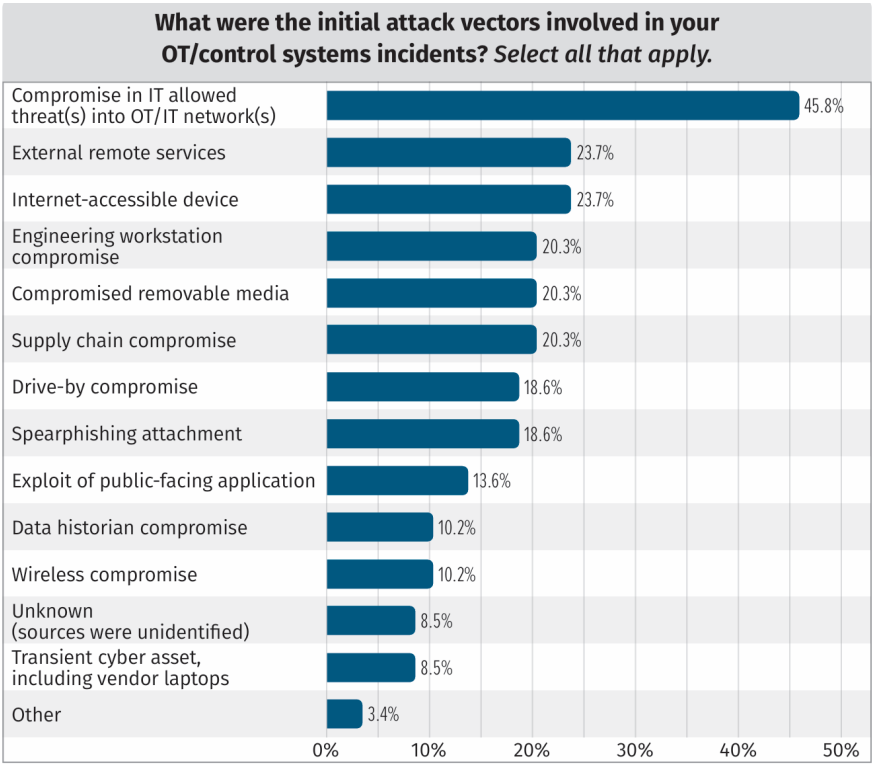
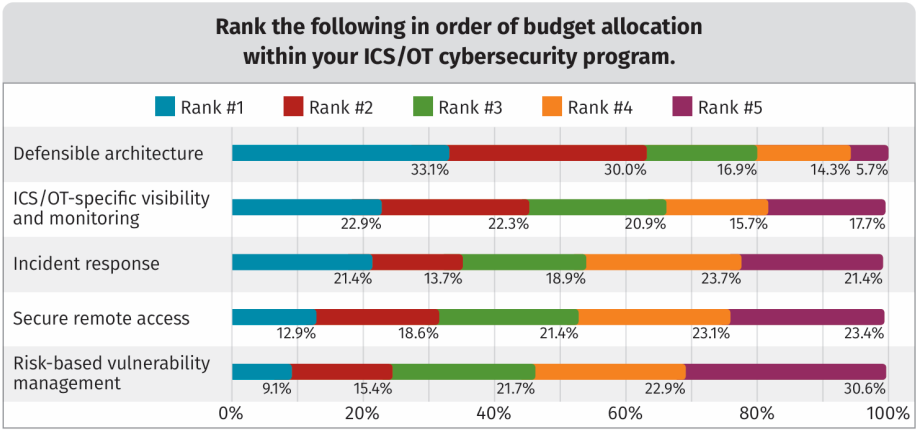


Figura 3

E sulle previsioni di spesa dove le soluzioni infrastrutturali per proteggere gli impianti sono in primissimo piano (**Figura 4**).

Sia per introdurre /estendere l'AI negli impianti (**Figura 5**).

In conclusione, la situazione del 2024 ha fino a ora avuto un trend migliore di quello del 2023, soprattutto in ambito nazionale, ma permangono comunque moltissime cose da affrontare e l'attenzione che le istituzioni stanno rivolgendo al settore manufatturiero, estendendo le regole di cybersecurity a moltissime aziende, dovranno essere recepite per migliorare ancora il panorama, a partire dalla prevenzione del malware a strascico con la mail come vettore di attacco che la fa ancora da padrone e che spesso arriva alle catene produttive a causa di un sezionamento non sufficiente della rete interna e a versioni non patchate dei sistemi. Il tutto aggravato da una superficie d'attacco sempre più ampia in seguito all'IoT e a Industria 4.0.



Priority Level of the SANS Five ICS Cybersecurity Critical Controls, Based on Budget Spend

Figura 4

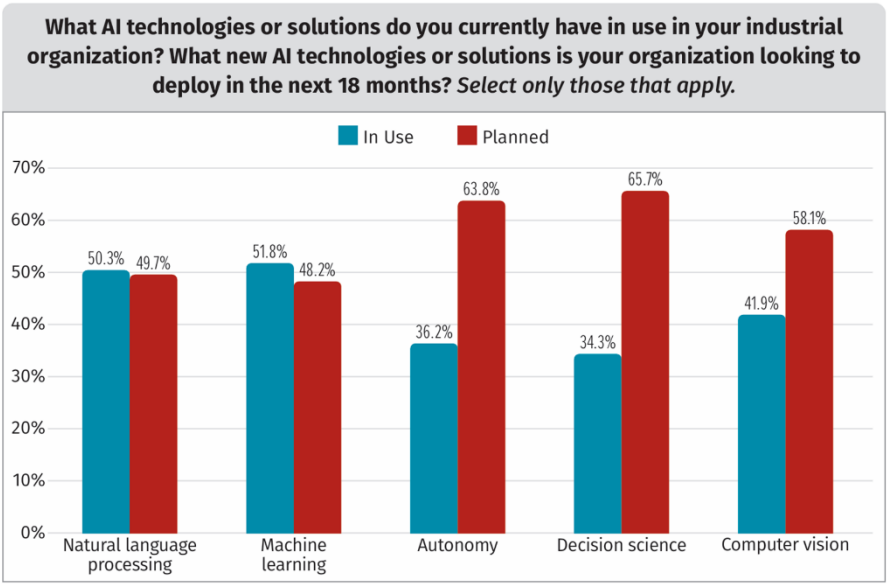


Figura 5

Il Regolamento Macchine e la Cybersecurity nel settore manifatturiero

[A cura di Stefano Castelluccio, CAST]

Dal rapporto Clusit di Novembre 2022: il 17% degli attacchi cybersecurity sono rivolti al manufacturing. L'introduzione del Regolamento Macchine, entrato in vigore il 29 giugno 2023, con data limite 20 gennaio 2027 per la compliance, è una risposta istituzionale alla crescita del rischio cyber per il settore industriale, e un'occasione per le aziende per strutturarsi verso processi più sicuri.

Cybersecurity e interoperabilità, ingredienti fondamentali per IoT e automazione industriale

La tecnologia che possiamo definire di *"automazione avanzata"* è andata, nel corso degli anni, verso una sempre maggiore diffusione all'interno delle strutture produttive delle aziende manufatturiere di tutto il mondo, ed è stata accompagnata da una corrispondente evoluzione tecnologica. Tale processo di innovazione progressiva è stato riassunto, nel gergo comune del business, in un percorso a tappe che va dalla *"Industry 1.0"* (l'industria nata dalla Rivoluzione Industriale) e procede attraverso *"Industry 2.0"* (l'inizio della produzione di massa), *"Industry 3.0"* (l'introduzione delle tecnologie digitali), *"Industry 4.0"* (smart manufacturing e apertura verso Internet) sino al recente paradigma *"Industry 5.0"* (Integrazione tra uomo e intelligenza artificiale, in ottica sostenibile).

La tecnologia IoT (*Internet of Things*), che è al cuore dei moderni processi di automazione industriale (*Operational Technology* – OT), è quindi ormai matura per un uso su larga scala, in sistemi industriali ad alta automazione, in numerosi settori industriali.

A fronte dei consistenti vantaggi introdotti, stante la sua intrinseca apertura verso le reti di comunicazione, la tecnologia IoT è esposta ad attacchi informatici di varia natura, a causa principalmente della presenza di vulnerabilità nel software che gestisce i dispositivi, della mancanza di standardizzazione e della presenza di problemi di interoperabilità. Cybersecurity e interoperabilità dei dispositivi IoT sono quindi requisiti fondamentali per garantire efficacia operativa con livelli adeguati di sicurezza e robustezza.

Il software risulta quindi elemento chiave, sia quello presente nei dispositivi IoT, che ne governa il comportamento locale, sia quello utilizzato centralmente per la gestione degli ecosistemi IoT.

Un sistema IoT efficace, efficiente, robusto, sicuro e interoperabile richiede quindi software esente da vulnerabilità, resiliente, efficiente, robusto e strutturato usando architetture e protocolli consolidati e condivisi.

In questo articolo vedremo come sia opportuno e possibile controllare i rischi software già in fase di sviluppo, definendo automaticamente dei piani di miglioramento basati su obbiettivi di compliance o di contenimento del rischio. Vedremo i vantaggi di esaminare l'architettura software dei sistemi IoT, rilevando pattern sfruttabili per attacchi informatici, o che impattano sull'interoperabilità.

Vedremo infine come, all'interno di questa prospettiva, il nuovo Regolamento Macchine possa costituire per le imprese un'occasione utile per rendere i sistemi di automazione industriale sicuri, controllati e resilienti, all'interno di un corretto processo industriale

IoT e Automazione nella Industry 4.0 e 5.0

L'*Internet of Things* (IoT) è un sistema di interazione remota di oggetti fisici tra loro e/o con l'ambiente esterno, che viene implementato utilizzando tecnologie hardware specializzate e componenti software, che in parte risiedono negli oggetti fisici e in parte implementano sistemi centralizzati di coordinamento. Il sistema è caratterizzato da un continuo scambio di dati in tempo reale e senza intervento umano diretto, che, prevalentemente, utilizza Internet come canale di comunicazione.

Schematicamente, l'IoT si presenta come diversi (decine, migliaia e in futuro anche milioni) componenti (oggetti o dispositivi complessi) connessi principalmente wireless e capaci di scambiarsi informazioni. Questi dispositivi possono essere collegati e controllati da remoto e il loro stato può essere analizzato in qualsiasi momento. Gli oggetti stessi entrano sia passivamente nel sistema, fornendo informazioni su sé stessi, sia lavorando attivamente, raccogliendo dati sul loro ambiente "assegnato" oppure operando direttamente su azionamenti di macchine.

I vantaggi dell'*Internet of Things* sono numerosi:
Maggiore efficienza nei processi produttivi e nella gestione dei dati, grazie all'automazione e alla raccolta di informazioni in tempo reale.
Maggiore sicurezza durante il monitoraggio dei dispositivi, che permette di prevenire guasti e interventi non pianificati.
Migliore qualità di servizio, grazie alla maggiore connettività e facilitando la gestione di dispositivi e servizi.
Aumento della produttività, monitorando le prestazioni dei dispositivi e ottimizzando l'uso delle risorse.
Migliore gestione delle risorse, consentendo il controllo remoto dei dispositivi e l'ottimizzazione del loro utilizzo.

IoT costituisce quindi una tecnologia chiave per lo sviluppo di soluzioni innovative in molti settori, tra i quali possiamo citare i seguenti:

- **Produzione industriale**: le reti estese di sensori e attuatori IoT distribuite lungo le linee di produzione consentono un controllo capillare dei processi produttivi, incrementando l'efficienza, la qualità e prevenendo i guasti e i blocchi con anticipo.
- **Energia elettrica e fornitura di gas e acqua**: l'uso di contatori intelligenti e di sensori di funzionamento delle apparecchiature consentono il monitoraggio remoto, e la corretta pianificazione della distribuzione.
- **Settore sanitario**: l'IoT consente di passare a un nuovo livello di diagnosi delle malattie, tramite dispositivi "intelligenti" che monitorano gli indicatori di salute dei pazienti in background.
- **Agricoltura**: le fattorie e le serre "intelligenti" erogano fertilizzanti e acqua in modo autonomo, e i localizzatori "intelligenti" di animali notificano in tempo reale agli agricoltori posizione e stato di salute degli animali.
- **Trasporti**: le tipiche soluzioni IoT includono la telematica e la gestione avanzata della flotta.
- **Smart-Cities**: le soluzioni IoT aiutano ad automatizzare e ottimizzare l'illuminazione, oppure a gestire in modo efficiente la regolazione del traffico cittadino.

- **Logistica**: l'IoT riduce i costi di trasporto e riduce al minimo l'impatto del fattore umano, oltre a permettere l'ottimizzazione dei magazzini.
- **Vendita al dettaglio**: l'IoT consente a marchi e commercianti di ridurre i costi e migliorare l'esperienza del cliente attraverso la segnaletica digitale, il monitoraggio delle interazioni con i clienti, la gestione dell'inventario e distributori automatici intelligenti.

IoT e Cybersecurity

L'IoT, come descritto, crea molteplici opportunità in un'ottica di automazione evoluta, per l'industria e non solo. Tuttavia, queste opportunità portano con sé una serie di sfide, in particolare in materia di sicurezza informatica.

Si può affermare che la cybersecurity sia un elemento fondamentale per il successo di un sistema di automazione basato su IoT. I motivi principali sono i seguenti:

– la **superficie di attacco è considerevolmente ampia** rispetto agli obbiettivi tradizionali degli attacchi hacker: ogni dispositivo IoT connesso rappresenta infatti un potenziale punto di accesso per i cybercriminali;
- una grande quantità di **dati sensibili** è esposta al **rischio di violazione**: i dispositivi IoT possono raccogliere e trasmettere dati sensibili e strategici, come informazioni personali e finanziarie, oppure dettagli su processi protetti da proprietà intellettuale, che potrebbero essere rubati e utilizzati per scopi illegali;
- eventuali attacchi producono un **impatto significativo**: un attacco informatico di successo su un sistema IoT può avere conseguenze devastanti, causando danni fisici, interruzioni di servizio e perdite finanziarie.

Le comunità hacker si sono accorte già da tempo dell'opportunità offerta dai sistemi automatici di nuova generazione. Giusto per fare qualche esempio:

- tra il 2018 e il 2021 sono avvenuti 45 cyberattacchi su scala globale mirati a sistemi IoT (*fonte: Hackmanac Global Cyber Attacks Report 2018-2021*);
- in questi ultimi mesi il numero di attacchi singoli nel settore manifatturiero, molti dei quali veicolati da vulnerabilità dei sistemi IoT è aumentata del 400% - 6.000 a settimana in valore assoluto (*fonte: ZScaler*).

IoT e Interoperabilità

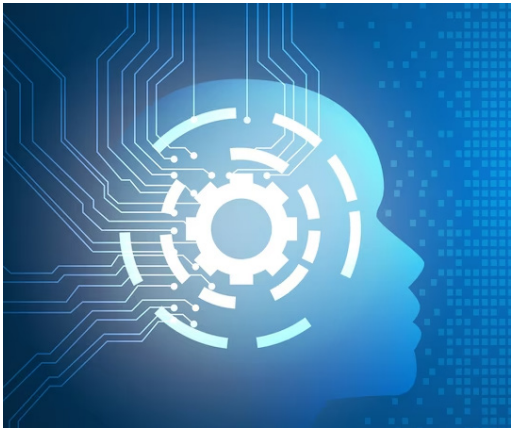
Un altro elemento cruciale da considerare è l'interoperabilità: è fondamentale che i dispositivi IoT siano in grado di comunicare e interoperare tra loro, indipendentemente da chi li ha prodotti o da quale tecnologia utilizzano. Le motivazioni di questa necessità possono essere così schematizzate:

- **efficienza e produttività**: l'interoperabilità è fondamentale affinché tutti i componenti del sistema lavorino insieme in modo efficiente e produttivo, automatizzando compiti complessi e creando nuove applicazioni e servizi;
- **scelta e flessibilità**: l'interoperabilità è basilare per poter scegliere i dispositivi IoT che meglio si adattano alle esigenze, senza essere vincolati a un unico fornitore o ad un unico ecosistema;
- **innovazione e crescita**: l'interoperabilità è una necessità per garantire l'innovazione e la crescita del mercato IoT, aprendo la strada a nuove applicazioni e servizi.

Dal punto di vista tecnologico, risulta difficile e sfidante implementare in modo efficace complesse applicazioni IoT, dati appunto i problemi di interoperabilità che possono sorgere quando si tenta di integrare sistemi di più fornitori.

L'interoperabilità, infine, è una caratteristica che copre vari aspetti tecnologici dei sistemi, e che quindi non si limita solo a considerazioni relative agli standard hardware (ad esempio la connettività cablata o wireless) e ai protocolli software di comunicazione, ma che coinvolge aspetti che riguardano la sicurezza, i processi di sviluppo del software e il cloud computing.

Il Software nei sistemi IoT



Dalle considerazioni sin qui fatte, emerge evidente come **il software**, sia quello embedded per i singoli componenti che quello per la gestione dell'intero ecosistema, **sia un elemento cruciale per la tecnologia IoT**.

In sostanza, un sistema IoT efficace, efficiente, robusto, sicuro e interoperabile richiede un software che sia:

- **esente da vulnerabilità**: sia il codice custom che la componente open-source devono garantire livelli di sicurezza adeguati durante tutto il ciclo di sviluppo (SDLC);
- **resiliente**: il comportamento del software deve essere prevedibile anche in condizioni di funzionamento imprevedibili o in presenza di anomalie;
- **efficiente**: il software deve essere progettato per evitare sprechi nell'utilizzo di risorse energetiche e computazionali;
- **strutturato usando architetture e protocolli consolidati e condivisi:** questo garantisce l'integrazione di sistemi e tecnologie di domini e vendor differenti.

La **cybersecurity**, come illustrato, è elemento essenziale per il software dei sistemi IoT, che per natura sono complessi, distribuiti geograficamente, esposti ad attacchi hacker e molto spesso critici per i processi che controllano e per i dati che trattano.

L'approccio tipicamente adottato per la gestione della sicurezza informatica in ambiente OT è quello dell'utilizzo di approcci analitici ex-post, ovvero i VAPT (*Vulnerability Assessment and Penetration Testing*) eseguiti sui sistemi di gestione degli ecosistemi IoT e sui singoli componenti. Tali test sono naturalmente fondamentali, ma non sono sufficienti. Per fornire garanzie sufficientemente adeguate di cybersecurity, il software, sia quello embedded dei dispositivi IoT che quello di gestione, deve essere scritto in modo sicuro fin dall'inizio. Ovvero, deve essere adottato un paradigma di **gestione preventiva del rischio informatico**.

Tipicamente, il software per sistemi IoT risulta composto da una componente custom, scritta in vari linguaggi (C/C++, Python, Java, ecc.) e da una componente Open-Source (ad esempio le librerie per l'interconnessione o i sistemi operativi lightweight). Entrambe le componenti possono essere afflitte da vulnerabilità:

- **codice custom**: i punti deboli (codificati dal MITRE come CWE - *Common Weakness Enumeration*) più critici sono di tipo strutturale, e dipendono dall'architettura a regime del sistema;
- **codice open-source**: viene usato da più del 70% delle applicazioni (*fonte: Gartner*). Risulta più facile da attaccare, in quanto i suoi problemi di sicurezza sono noti (codificati dal MITRE come CVE – *Common Vulnerabilities and Exposures*).

Nel complesso, quindi, una strategia di gestione della cybersecurity adeguata deve comprendere:

- un'analisi strutturale statica del codice custom, integrata con il ciclo di sviluppo del software (SDLC);
- un'analisi della sicurezza delle componenti open-source (SCA).

Altri elementi fondamentali, come illustrato, sono la **robustezza e l'interoperabilità dell'ecosistema IoT**, che naturalmente determinano opportuni requisiti per il software. Per garantire tali caratteristiche, è necessaria una **conoscenza dettagliata e aggiornata dell'architettura complessiva del software dei sistemi IoT**. Occorre quindi avere sempre ben chiaro come ogni componente si connette agli altri, quali sono le possibili operazioni e come vengono implementate, per poter eseguire:

- corrette analisi di impatto nel caso di interventi di manutenzione correttiva ed evolutiva;
- system review efficaci;
- pianificazione delle evoluzioni sostanziali del sistema;
- sviluppo di integrazioni corrette;
- individuazione delle cause dei problemi.

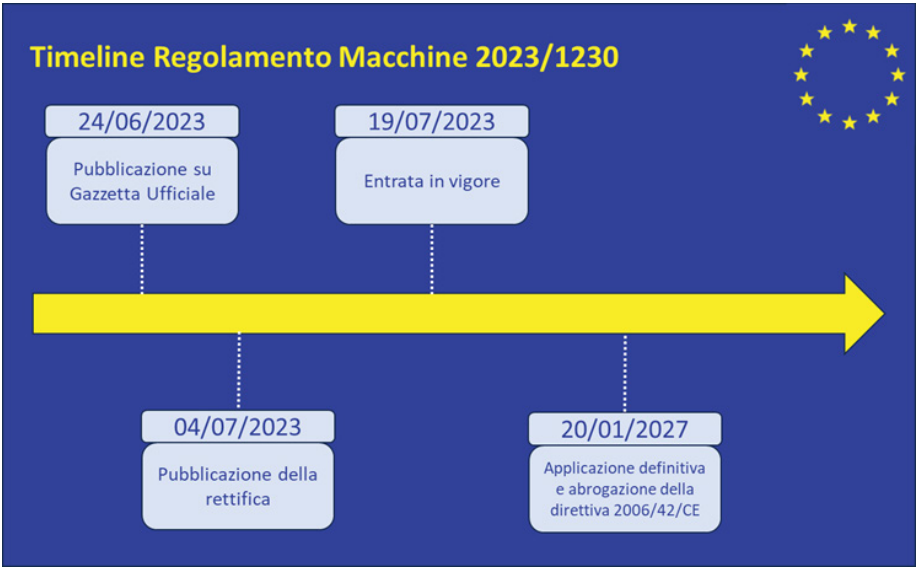
Gli Standard e il nuovo Regolamento Macchine

Da tempo esistono standard consolidati per lo sviluppo di software strutturalmente solido, come ISO-5055 (che copre le aree relative alla sicurezza, all'efficienza, alla robustezza e alla manutenibilità), come peraltro esistono standard specifici per lo sviluppo di sistemi IoT, quali IEEE 2700-2017, IEEE P1451.99, IEEE P2020, IEEE P2520 e IEEE P2846.

Ma fino a poco tempo fa, l'aderenza a tali standard era lasciata all'iniziativa del singolo costruttore o del singolo system integrator. Il **Regolamento Macchine** emerge quindi e soprattutto come esigenza di un riferimento comune per lo sviluppo di macchinari e automazioni nei quali le nuove tecnologie, come IoT, vengano inserite rispettando determinati standard di qualità e sicurezza.

Come illustrato, l'evoluzione tecnologica in ambito OT per il mondo manufacturing sta imponendo ai produttori una rapida revisione del loro modello di gestione dei rischi, con particolare riferimento a quelli provenienti dal mondo cyber, e ha reso obsoleta, da un punto di vista normativo, la precedente direttiva 2006/42/CE (Direttiva Macchine).

Nell'ottica di un comune approccio alla cybersecurity all'interno dei 28 Paesi membri CE, il legislatore europeo ha emanato il Regolamento 2023/1230 (noto come Regolamento Macchine), in vigore da luglio 2023.



Timeline entrata in vigore Regolamento 2023/1230

Il Regolamento introduce il concetto di **software come componente di sicurezza delle macchine stesse**: pertanto, alle componenti software, oltre al marchio CE, dovrà essere associata sia una dichiarazione di conformità UE nei confronti del Regolamento, sia istruzioni operative specifiche.

Questo impone ai costruttori l'applicazione di un modello di gestione del rischio che tenga conto dei rischi connessi al software eseguito a bordo delle macchine e/o delle componenti IoT; inoltre, per quei sistemi che utilizzano tecnologie di intelligenza artificiale, la valutazione dei rischi dovrà considerare anche l'evoluzione del comportamento dei sistemi stessi, in base ai diversi livelli di autonomia previsti.

Tenuto conto del continuo incremento della numerosità degli attacchi e della loro criticità, per macchine e apparati IoT connessi alle reti è quindi necessario considerare le problematiche di sicurezza informatica e i rischi derivati.

A tale scopo, tutte le componenti software vanno verificate e validate secondo un **risk management plan** che comprende un assessment dei rischi stessi, l'implementazione di specifiche misure di mitigazione, oltre alla valutazione del rischio residuo come indicato dal *Considerando* n. 12 del Regolamento.

La nuova impostazione delle normative europee (ad esempio la direttiva NIS2), indica che il produttore della macchina debba autodefinire i rischi e le misure da applicarsi, come indicato anche dal *Considerando* n. 32 e dall'Allegato III parte B del Regolamento che riportiamo testualmente:

> *Il fabbricante dovrebbe stabilire quali requisiti essenziali di sicurezza e di tutela della salute siano applicabili al prodotto che rientra nell'ambito di applicazione del presente regolamento e quali misure debbano essere adottate per affrontare i rischi che il prodotto può presentare. La valutazione del rischio dovrebbe affrontare inoltre gli aggiornamenti o gli sviluppi futuri di un software installato nella macchina o nel prodotto correlato, che sono previsti quando la macchina o il prodotto correlato sono immessi sul mercato o messi in servizio. I rischi individuati durante la valutazione del rischio dovrebbero comprendere i rischi che potrebbero manifestarsi durante il ciclo di vita del prodotto.*

Quanto specificato dal Regolamento Macchine è già stato armonizzato dal legislatore con quanto previsto dalla famiglia di standard ISA/IEC 62443 relativa alla sicurezza dei sistemi di automazione industriale, siano essi IACS o SCADA.

Questi standard definiscono dei *Security Level* che vanno definiti e implementati, sia in termini di controlli da applicarsi per migliorare i livelli di sicurezza informatica, sia, come richiesto dal Regolamento, in termini di valutazione del livello di rischio complessivo e di rischio residuo, come previsto dalle famiglie normative ISO 27000 e ISO 31000. I *Security Level* sono codificati associati al reale livello di sicurezza secondo lo schema:

- **Security Level 0**: Nessuna sicurezza.
- **Security Level 1**: Protezione contro errori accidentali.
- **Security Level 2**: Protezione contro attacchi intenzionali, con mezzi semplici, poche risorse e basso livello di conoscenza.
- **Security Level 3**: Protezione contro attacchi intenzionali, con mezzi sofisticati, risorse moderate e livello di conoscenza medio.
- **Security Level 4**: Protezione contro attacchi intenzionali, con mezzi sofisticati, risorse elevate e livello di conoscenza alto.

La normativa costituisce quindi un framework allineato ai più moderni concetti di sicurezza in generale e cybersecurity in particolare, insistendo sul ruolo centrale del software. Pur rappresentando, da un lato, un ulteriore onere gravante sulle organizzazioni, dall'altro fornisce l'occasione per adeguare i processi produttivi delle imprese a una realtà che sarebbe quantomeno imprudente sottovalutare o ignorare.

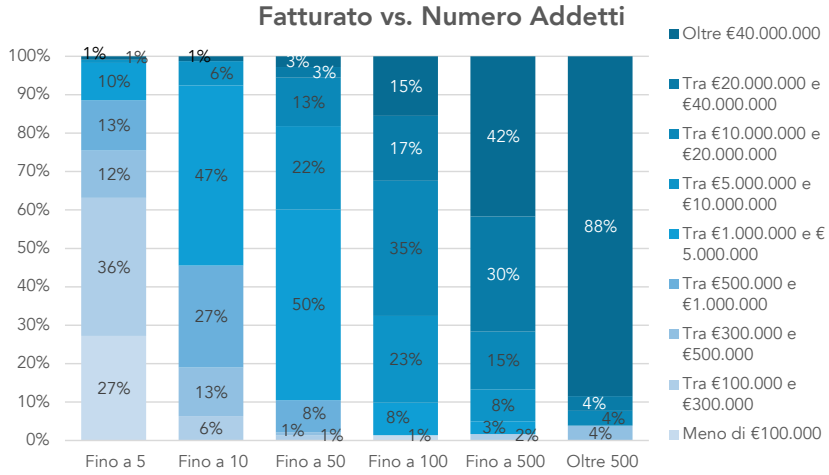
Investire sulla realizzazione di processi SDLC e prodotti sicuri e resilienti porta a un naturale miglioramento della qualità complessiva di tali processi e prodotti, generando, sul medio e lungo termine, innegabili vantaggi in termini di competitività e riduzione dei costi.

Come va la cybersecurity nelle PMI italiane?

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

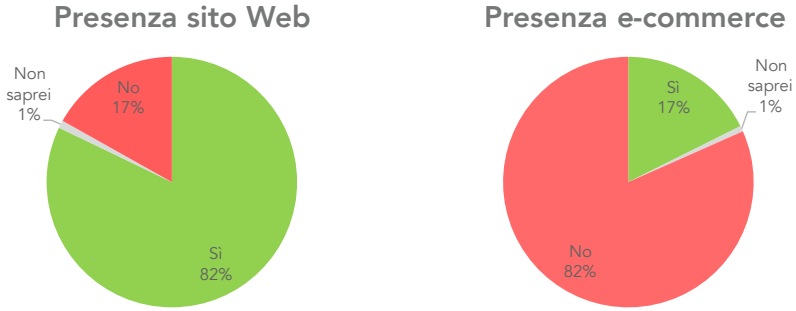
Più di 500 aziende hanno risposto alla survey che è stata realizzata tra maggio e luglio 2024 dalla Camera di Commercio di Modena e dall'Università di Modena e Reggio Emilia, in collaborazione col Clusit. Questa importante risposta ci ha permesso di raccogliere dati preziosi sulla postura di cybersecurity delle aziende italiane di una zona molto interessante. Infatti, la provincia di Modena non è parte di un'area metropolitana – cosa che ci permette di uscire da una potenziale "bolla" nella nostra percezione della realtà – e al contempo è una delle aree economiche più avanzate e industrializzate del paese, nota per i suoi prodotti agricoli e industriali di alta qualità.

La survey aveva come scopo la rilevazione della postura di cybersecurity di queste aziende, che per circa il 70% sono piccole aziende (meno di 10M€ di fatturato), e per il restante 30% sono medie imprese (fatturato fino a 50M€).

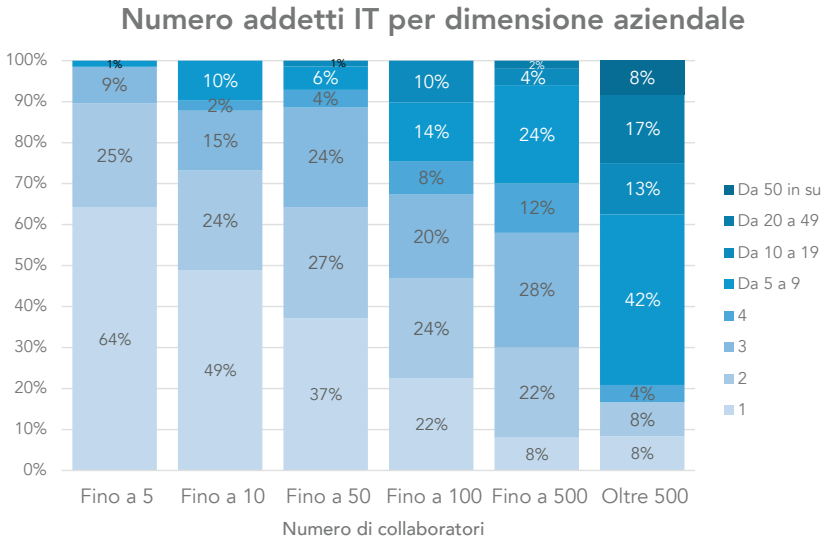


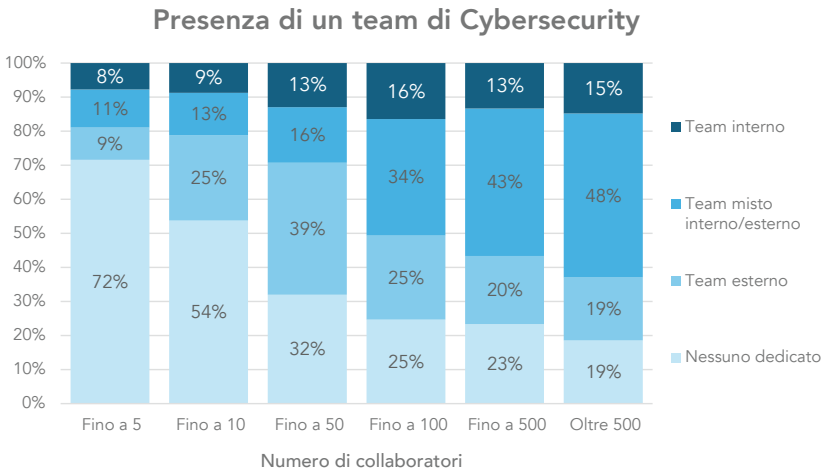
La maggior parte delle aziende presentate nella survey ha un sito Web (l'82%), che ci suggerisce come le aziende abbiano ormai acquisito questo strumento come fondamentale per promuovere le proprie attività commerciali e aumentare la visibilità sul mercato. Tuttavia, tra queste aziende solo il 17% ha anche un sito di e-commerce.

Ciò suggerisce che molte delle piccole e medie imprese presentate nella survey potrebbero beneficiare di strumenti più avanzati per gestire le proprie attività online.

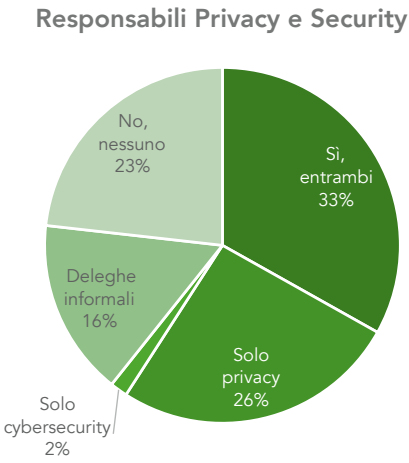


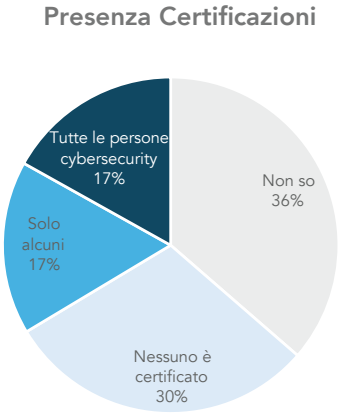
Non è una sorpresa che l'organizzazione e la complessità siano fortemente influenzate dalla dimensione dell'azienda. Il numero di persone dedicato alle funzioni IT, cybersecurity e privacy aumenta con il crescere dell'azienda, dando alle aziende più grandi più risorse specializzate per gestire la sicurezza informatica. Al contrario, nelle aziende piccole e piccolissime (fino a 10 collaboratori) si arriva ad un 80% che non dispone di personale dedicato all'informatica, e si appoggia pesantemente a fornitori esterni. Spesso (nel 64% delle microimprese) si tratta di una persona sola, proveniente da un fornitore, alla quale vengono richiesti anche compiti di cybersecurity.





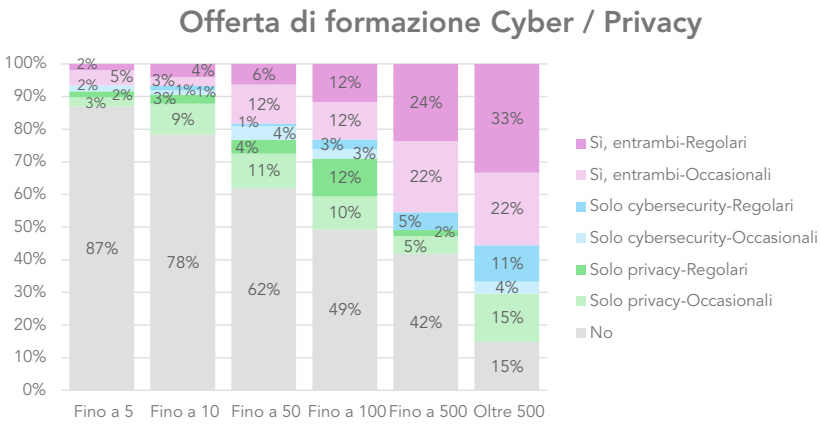
Nelle microimprese, infatti, nel 72% dei casi non c'è alcuna persona dedicata alla cybersecurity; ma anche nelle realtà più grandi in circa 1/3 dei casi non c'è alcuna delega formale (e in 1/4 dei casi la delega è solo per la privacy); e solo in circa il 17% dei casi queste persone hanno ricevuto una formazione certificata sui temi di cui sono incaricate di occuparsi.



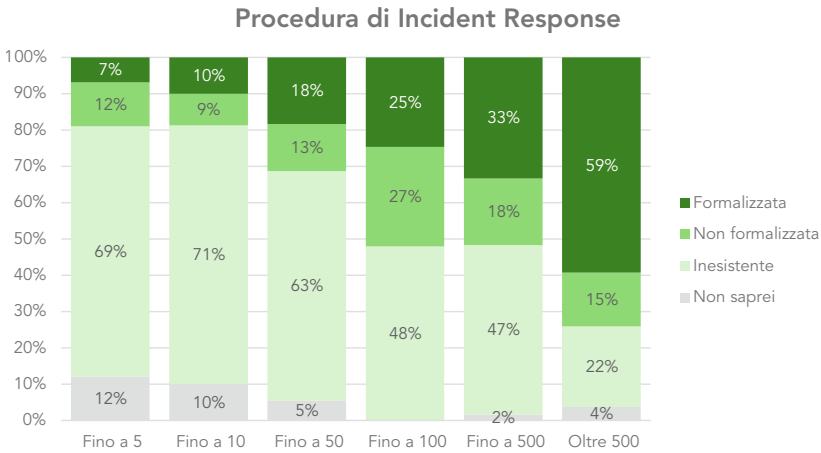


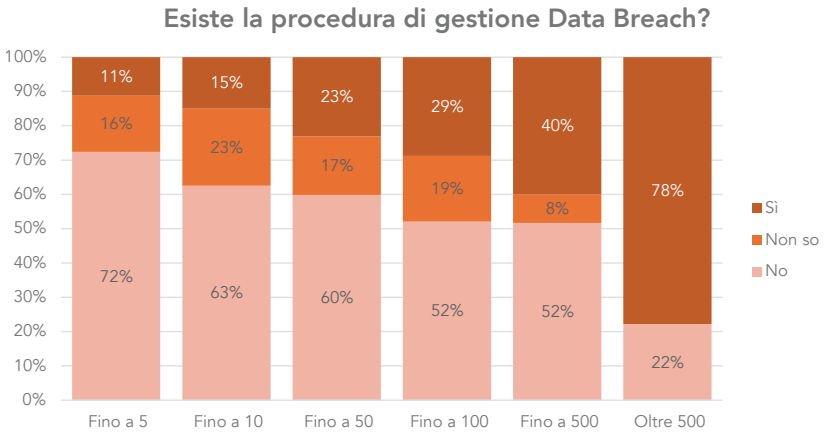
La formazione rimane comunque un ambito con cui le aziende faticano a confrontarsi. Particolarmente significativo sembra il dato che anche nelle aziende più grandi del campione solo poco più di metà offre ai collaboratori una formazione sia in ambito

cybersecurity sia privacy, e solo circa 1/3 lo fa in modo regolare. Per le microimprese, il dato è desolante: per 9 realtà su 10 la formazione è del tutto assente.

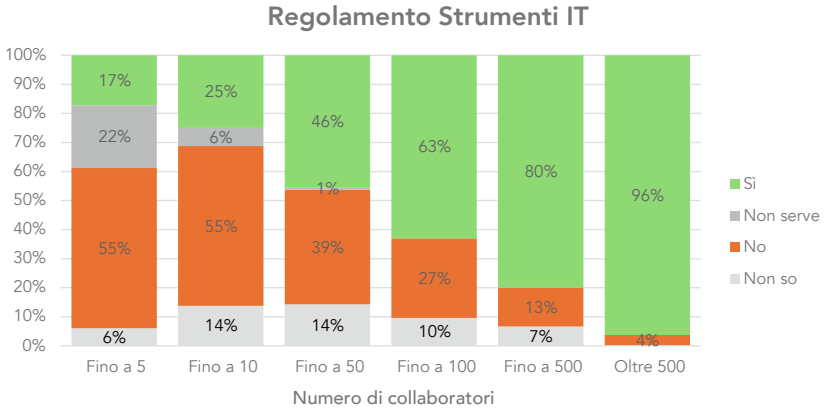


L'adozione di politiche formalizzate, e la loro conoscenza da parte dei collaboratori, sono altresì un punto ancora problematico. Tranne il caso delle ditte individuali, dove naturalmente il problema di divulgare le procedure ai collaboratori non si pone, vediamo che nelle micro e nelle piccole imprese la sensibilità rimane ancora bassa, per quanto questo, purtroppo, non stupisca.

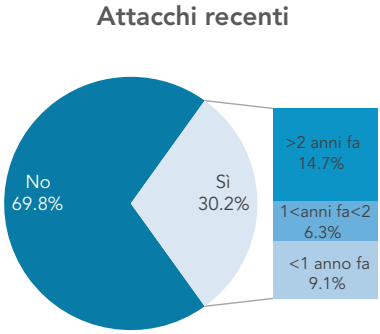




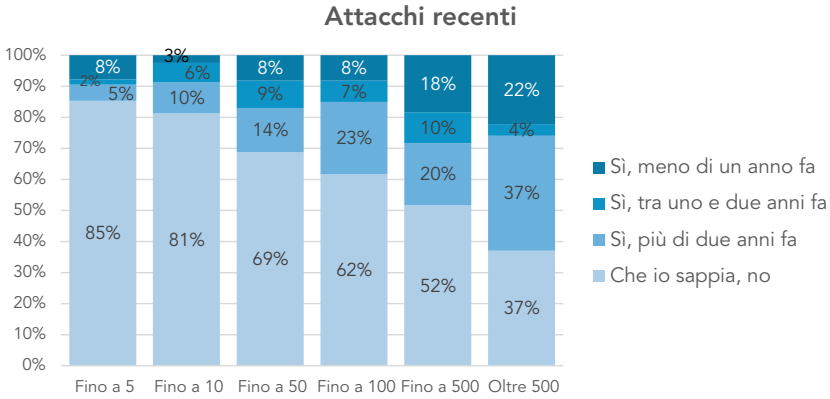
Meno atteso è invece il dato che un terzo delle aziende fino a 100 collaboratori, e il 13% di quelle fino a 500, non adottino un documento di base come un regolamento d'uso degli strumenti IT aziendali.

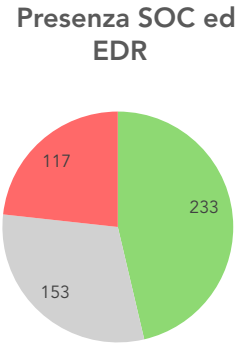


Per un'azienda, essere consapevole di avere subito un attacco cyber è fondamentale perché può compromettere la sua reputazione e le sue operazioni commerciali. Inoltre, gli attacchi di malintenzionati possono comportare costi significativi per l'azienda, come ad esempio multe e sanzioni.

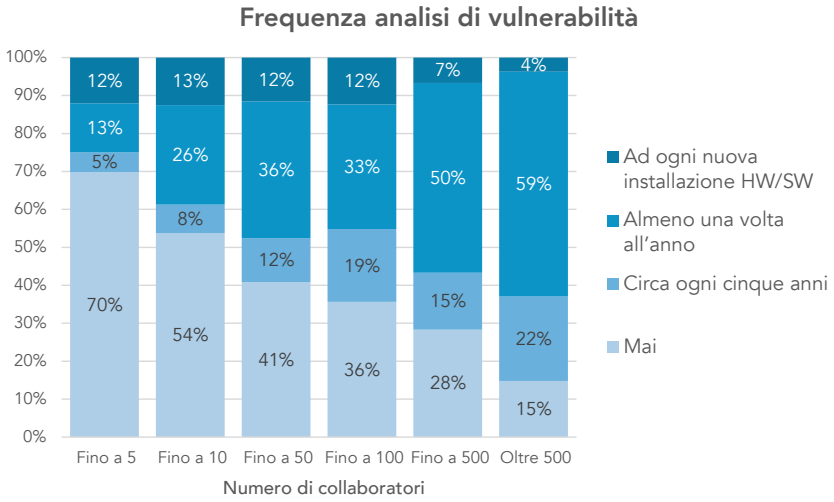


Il dato aggregato mostra che il 30,2% delle aziende del territorio è consapevole di aver subito almeno un attacco informatico in passato. Si evidenzia che più della metà di questi attacchi sono stati subiti negli ultimi due anni, a conferma di un trend in continua crescita, come si può leggere anche nelle altre sezioni di questo rapporto.
I dati dimostrano inoltre che le aziende di grandi dimensioni hanno una maggiore consapevolezza degli attacchi cyber subiti.

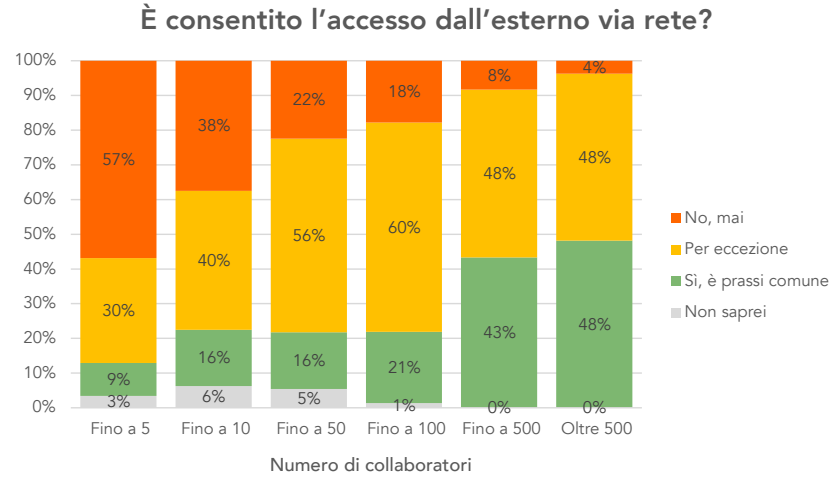


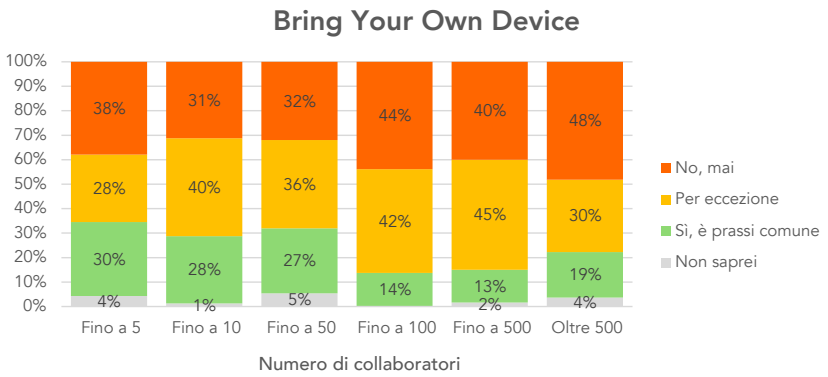


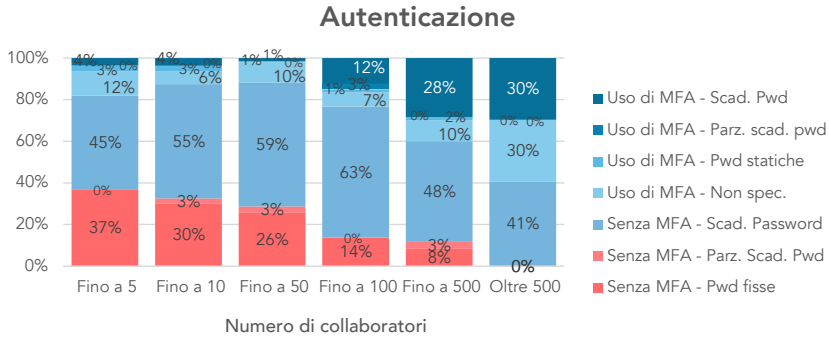
Il fatto che rimanga una percentuale importante di aziende che dicono di non essere mai state attaccate fa sospettare, purtroppo, che manchi consapevolezza, o forse manchino gli strumenti per conoscersi. Quest'ultima ipotesi pare plausibile, alla luce del dato di diffusione dei servizi SOC ed EDR, che risultano utilizzati dalle aziende della survey solo per il 46%.
In questo contesto, anche conoscere le proprie vulnerabilità informatiche è essenziale perché permette di identificare potenziali punti deboli che possono essere sfruttati dagli attaccanti. In questo modo, un'azienda può prevenire ulteriori danni e proteggere i dati sensibili dei clienti.

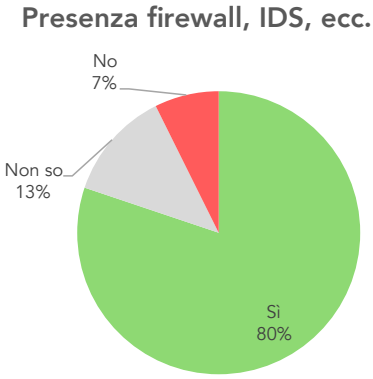


Dai due grafici che seguono si può notare una certa contraddizione: mentre la maggioranza delle aziende afferma di consentire accessi dall'esterno in modo assai controllato (nelle microimprese, solo 1 su 10 consente per prassi l'accesso), più o meno in tutte le realtà – indipendentemente dalla dimensione – è possibile in larga misura l'utilizzo di dispositivi personali per collegarsi alla rete aziendale. Interessante anche che nelle aziende, al crescere della dimensione, diventi più consueto consentire l'accesso dall'esterno.





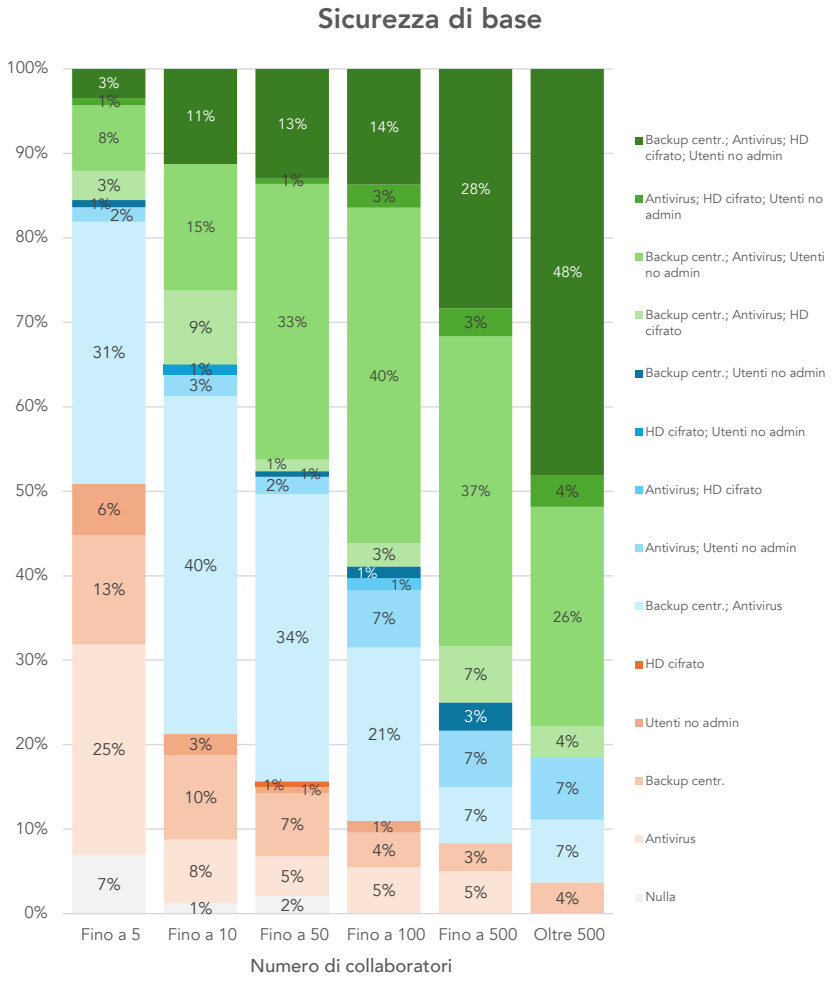




Adozione di strumenti tecnologici, come antivirus, firewall, sistema operativo protetto da malware e altri strumenti, è condizione necessaria per tradurre in pratica le politiche atte a garantire un ambiente di lavoro robusto e sicuro. È confortante riscontrare la presenza dei firewall in una fetta molto grande del campione.

Si riscontra, tuttavia, ancora una insufficiente diffusione di tecnologie di base, che oggi sono disponibili a prezzi molto contenuti, o addirittura incluse nel prezzo di altro software, come ad esempio la crittografia del disco fisso.

Quest'ultima tecnologia è adottata solo in circa il 20% delle aziende, e principalmente in quelle più organizzate.



Conclusioni

In sintesi, questa survey ha rilevato nelle aziende del campione una postura di cybersecurity ancora non del tutto soddisfacente, soprattutto – come spesso si vede anche in altre zone geografiche – per quanto riguarda le realtà più piccole.
Tuttavia, ci sono anche segnali positivi, e la recente spinta normativa derivante dall'adozione della Direttiva NIS2 e del Regolamento DORA dovrebbe essere utile per dare una forte spinta per una evoluzione in senso positivo.

Per migliorare la postura di cybersecurity delle aziende sembra consigliabile investire nella formazione dei collaboratori e nell'adozione di politiche formalizzate. In particolare, è importante creare un ambiente in cui le aziende possano condividere esperienze e conoscenze relative alla gestione della cybersecurity, in modo da poter raggiungere una maggiore consapevolezza dei rischi e delle opportunità di protezione, così come raccomandato dalle migliori pratiche e dalla legislazione in vigore.

Cybersecurity e cyber resilience nell'era del quantum

[A cura di Federica Maria Rita Livelli]

L'avvento del quantum computing rappresenta una svolta importante nella tecnologia, promettendo capacità di calcolo straordinarie che potrebbero risolvere problemi complessi in pochissimo tempo, rispetto ai tempi estremamente lunghi che impiegherebbero i computer tradizionali. Tuttavia, questa rivoluzione comporta nuove sfide di sicurezza informatica, richiedendo una revisione dei protocolli attuali e lo sviluppo di nuove strategie per proteggere le informazioni sensibili.

Il progresso quantico

I computer quantistici sfruttano i principi della meccanica quantistica. Essi utilizzano i qubit che possono esistere in più stati contemporaneamente, a differenza dei bit classici che sono 0 o 1. Tale caratteristica consente ai computer quantistici di eseguire calcoli paralleli su una scala senza precedenti. È doveroso evidenziare che, se da un lato ciò promette soluzioni a problemi complessi in campi come la crittografia, la scienza dei materiali e la scoperta di farmaci, dall'altro lato rappresenta anche una minaccia significativa per gli attuali framework di sicurezza informatica.

Panorama del rischio quantistico

Le organizzazioni non possono permettersi di rimandare la comprensione approfondita dei rischi che le tecnologie quantistiche potrebbero rappresentare per le loro operazioni e la loro sicurezza. Pertanto, devono essere consapevoli che:

- molti dei principali standard di crittografia esistenti sono – o saranno – vulnerabili alla decrittografia; .
- algoritmi quantistici avanzati potrebbero prendere di mira i complessi sistemi di controllo delle reti elettriche, degli impianti di trattamento delle acque o delle reti di trasporto, causando blackout diffusi o addirittura danni fisici;
- le aziende che detengono proprietà intellettuale sensibile, in particolare nei settori dell'energia, della difesa o farmaceutico, potrebbero essere vulnerabili ai furti quantistici;
- l'informatica quantistica potrebbe essere utilizzata per manipolare i mercati finanziari, minare la fiducia nelle valute digitali o attaccare gli algoritmi che attualmente proteggono la tecnologia blockchain;

- attacchi "*harvest now, decrypt later*" da parte dei cyber criminali potrebbero essere già in atto, raccogliendo i dati crittografati per una successiva decrittazione, quando la potenza di calcolo quantistico diventerà più accessibile.

Servizi di sicurezza informatica in trasformazione

I servizi di sicurezza informatica, con l'avanzare del calcolo quantistico, devono adattarsi per affrontare nuove vulnerabilità, adottando nuove strategie, quali:

- **Crittografia post-quantistica -** Per affrontare la minaccia del calcolo quantistico, i ricercatori stanno sviluppando algoritmi crittografici resistenti agli attacchi quantistici. Questi algoritmi post-quantistici mirano a garantire la sicurezza anche contro avversari dotati di capacità quantistiche avanzate. È essenziale che i servizi di sicurezza informatica integrino questi nuovi algoritmi per proteggere i dati dalle future minacce quantistiche. Fondamentale il ruolo, in materia, del National Institute of Standards and Technology (NIST), come riferiamo dettagliatamente più avanti.
- **Protocolli di sicurezza evoluti -** L'avvento del quantum computing impone una revisione dei protocolli di sicurezza attuali. Le organizzazioni devono valutare i loro sistemi crittografici esistenti e identificare le vulnerabilità sfruttabili dai computer quantistici. Aggiornare i metodi di crittografia per renderli resistenti ai quanti e rafforzare i protocolli di sicurezza sarà cruciale per mantenere l'integrità dei dati e difendersi da minacce informatiche sempre più sofisticate.
- **Distribuzione delle chiavi quantistiche (Quantum Key Distribution -QKD) -** La QKD è una tecnologia emergente che utilizza i principi della meccanica quantistica per creare canali di comunicazione estremamente sicuri. Essa permette di condividere chiavi crittografiche con totale sicurezza, poiché qualsiasi tentativo di intercettazione verrebbe immediatamente rilevato. Pertanto, l'integrazione di QKD nei servizi di sicurezza informatica può offrire un livello di protezione aggiuntivo, garantendo la sicurezza delle chiavi crittografiche anche in un contesto quantistico.
- **Rilevamento e risposta alle minacce -** La potenza di calcolo avanzata dei computer quantistici può essere utilizzata per potenziare le capacità di rilevamento e risposta alle minacce. Gli algoritmi quantistici possono analizzare enormi volumi di dati con una rapidità senza precedenti, permettendo un'identificazione più efficiente delle minacce informatiche e delle anomalie. Integrando il calcolo quantistico nei servizi di sicurezza informatica, le organizzazioni possono migliorare la loro capacità di rilevare e contrastare le minacce in tempo reale.

Stato dell'arte delle strategie di sicurezza del quantum computing negli USA

La consapevolezza della minaccia tecnologica quantistica ha messo in moto – già da alcuni anni – il NIST (National Institute of Standards and Technology), la NSA (National Security Agency) e addirittura lo stesso Presidente Biden che a dicembre 2022 ha firmato la legge "*Quantum Computing Cybersecurity Preparedness Act*", imponendo alle agenzie federali di iniziare a controllare i propri sistemi per verificare la presenza di crittografia da sostituire.

Ripetiamo che il NIST svolge un ruolo fondamentale nello sviluppo della crittografia post-quantum. Nel 2016, ha lanciato un concorso internazionale per individuare e standardizzare nuovi algoritmi crittografici in grado di proteggere i dati anche di fronte alla potenza di calcolo dei computer quantistici, selezionando i primi quattro algoritmi post-quantum considerati sicuri e pronti per l'implementazione.

Lo scorso agosto 2024 il NIST ha rilasciato un set finale di strumenti di crittografia progettati per resistere all'attacco di un computer quantistico. Si tratta di tre standard di crittografia post-quantistica in grado di proteggere un'ampia gamma di informazioni elettroniche, ovvero:

FIPS 203 – Standard principale per la crittografia generale, è basato sull'algoritmo CRYSTALS-Kyber, rinominato ML-KEM, i.e. abbreviazione di Module-Lattice-Based Key-Encapsulation Mechanism.

FIPS 204 – Standard principale per la protezione delle firme digitali. Si basa sull'algoritmo CRYSTALS-Dilithium, Ora è chiamato ML-DSA, i.e. Module-Lattice-Based Digital Signature Algorithm.

FIPS 205 – Standard progettato anche per le firme digitali, si basa sull'algoritmo SPHINCS+, ora denominato SLH-DSA, i.e. abbreviazione di Stateless Hash-Based Digital Signature Algorithm. Questo standard è basato su un approccio matematico diverso da FIPS 204/ML-DSA ed è inteso come backup nel caso in cui ML-DSA sia vulnerabile.

E in Europa cosa si sta facendo?

Anche l'UE si sta attivando per gestire il rischio quantico e lo scorso aprile 2024 ha pubblicato il Documento "Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography", incoraggiando gli Stati membri a sviluppare una strategia globale per l'adozione della crittografia post-quan-

tistica, al fine di garantire una transizione coordinata e sincronizzata tra i diversi Stati membri e i loro settori pubblici.

Le raccomandazioni fanno riferimento anche alla direttiva NIS 2, che si concentra sulle infrastrutture critiche, indicando che queste dovranno essere le prime ad essere messe in sicurezza.

Per garantire un'attuazione armonizzata della crittografia post-quantistica nell'Unione Europea, le raccomandazioni ribadiscono la necessità di sviluppare norme comuni e un quadro per selezionare gli algoritmi crittografici appropriati. È altresì incoraggiata la collaborazione tra Stati membri, esperti di cybersicurezza, il gruppo di cooperazione NIS e l'ENISA per la valutazione e l'adozione di tali algoritmi.

Inoltre, l'UE sta già sostenendo lo sviluppo di algoritmi attraverso progetti di ricerca finanziati. Ancora, gli Stati membri e l'UE dovrebbero lavorare con partner internazionali per stabilire norme globali che garantiscano l'interoperabilità delle comunicazioni.

La tabella di marcia per la transizione alla crittografia post-quantistica contenuta nelle raccomandazioni, una volta approvata, servirà come modello per i piani nazionali di transizione o per allinearli a uno standard comune.

È doveroso sottolineare che la mancata conformità alle normative in via di sviluppo potrebbe danneggiare in modo significativo la reputazione di un'azienda e alla fine portare a misure punitive come quelle stabilite nel GDPR, nell'AI Act dell'UE, nella NIS2, ecc. Alle aziende potrebbe essere richiesto, in futuro, di sviluppare piani di continuità aziendale specifici per la quantistica e di valutare regolarmente le vulnerabilità in tutte le loro catene di approvvigionamento.

WEF e Deloitte – Governance e framework per la gestione del rischio quantistico

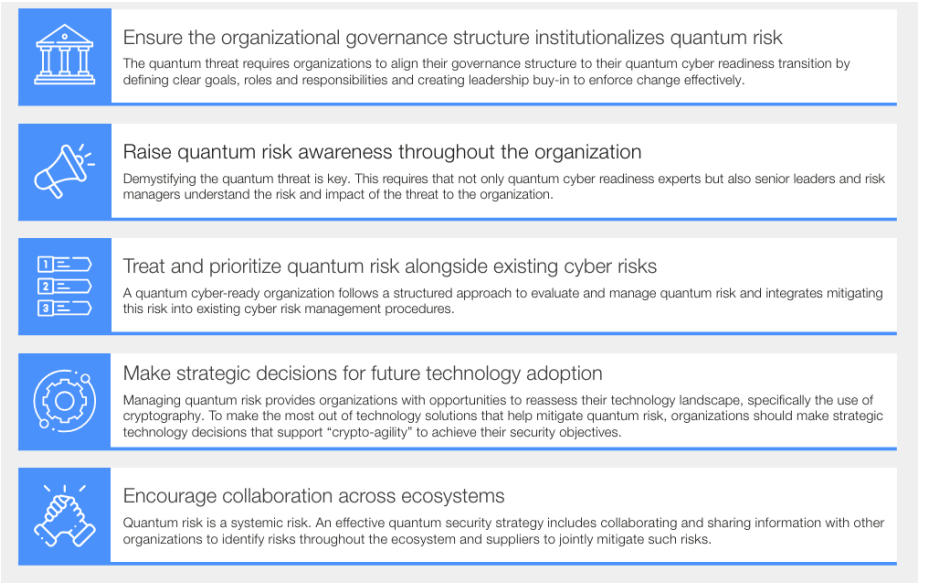
Nel 2022, il WEF e Deloitte hanno sviluppato un framework per aiutare le organizzazioni a prepararsi alla transizione verso un'economia quantistica. Il quadro mette in evidenza l'importanza di adottare un approccio globale, collaborativo e riflessivo, coinvolgendo una rete internazionale di leader aziendali ed esperti di sicurezza informatica.

Il WEF propone principi di governance che promuovono impegni per la sicurezza informatica, la privacy e la responsabilità ed ha sviluppato un toolkit per preparare le organizzazioni alla sicurezza nell'era quantistica, incoraggiando i leader a integrare

protocolli cyber-quantistici nei loro ecosistemi, oltre a collaborare nell'identificazione dei rischi e nell'adozione di misure protettive.

Il WEF Quantum Readiness Toolkit – Si tratta di un 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. Il toolkit funge da leva strategica per gestire il rischio quantistico insieme ad altri rischi esistenti. Di fatto, le organizzazioni devono accrescere la consapevolezza, investire nell'educazione e collaborare con l'ecosistema per comprendere e affrontare i rischi quantistici e possono utilizzare questo toolkit come punto di partenza per la transizione verso la sicurezza quantistica grazie ad indicazioni pratiche e, al contempo, colmare le lacune nelle preparazioni.

Di seguito le principali fasi che le organizzazioni devono contemplare per una transizione sicura al quantum computing.



Fonte immagine WEF - Toolkit per aiutare le organizzazioni a sviluppare protocolli per la sicurezza informatica quantistica.

Integrazione del rischio quantistico nella governance aziendale - Una governance chiara è essenziale per affrontare il rischio quantistico. Le organizzazioni dovrebbero

creare una struttura che istituzionalizzi tale rischio, permettendo un'applicazione efficace dei cambiamenti. Inoltre, le linee guida devono essere prescritte gradualmente, consentendo una transizione ordinata e includendo il rischio quantistico come parte integrante delle attività di cybersecurity. Ancora, è fondamentale considerare le attività di assegnazione di responsabilità specifiche, la nomina di campioni della crittografia e lo sviluppo di una roadmap per allineare la sicurezza quantistica con altri obiettivi strategici.

Consapevolezza del rischio quantistico in tutta l'organizzazione - Poiché il rischio quantistico non è ancora sufficientemente conosciuto, le organizzazioni devono diffondere conoscenze mirate per aiutare gli stakeholder interni ed esterni a comprendere questa minaccia emergente senza generare timore. Ne consegue che è fondamentale sviluppare strategie per formare e riqualificare il personale, garantendo la disponibilità di talenti in sicurezza quantistica, oltre a considerare le seguenti attività: la mappatura dei ruoli impattati dal rischio quantistico, la creazione di partnership per aumentare la formazione e lo sviluppo delle competenze necessarie.

Prioritizzazione del rischio quantistico insieme ai rischi informatici esistenti - Il rischio quantistico deve essere trattato come parte del programma di gestione del rischio informatico dell'organizzazione. Ovvero, le organizzazioni devono documentare la propria tecnologia e i requisiti operativi, creando un "documento crittografico" che elenchi tutti i componenti crittografici impiegati nei servizi e nelle applicazioni. Si consiglia, altresì, di attuare un approccio modulare, separando la crittografia dalle applicazioni e, così facendo, garantire maggiore agilità.
Le attività chiave per affrontare il rischio quantistico includono:

Valutazione del rischio quantistico

- **Minaccia degli attacchi quantistici -** Valutare la pericolosità degli attacchi attraverso rapporti pubblici e analisi delle minacce.
- **Valutazione iniziale del rischio -** Stimare l'impatto del rischio quantistico, considerando la durata di conservazione dei dati sensibili.
- **Prioritizzazione degli asset IT -** Identificare i sistemi critici da proteggere e quelli vulnerabili agli attacchi "harvest-now, decrypt-later" (HNDL).
- **Monitoraggio delle tecnologie ad alto rischio -** Controllare regolarmente sistemi e applicazioni.
- **Gestione del rischio -** Esplorare alternative quali l'assicurazione informatica o accettare i rischi residui per le tecnologie meno esposte.

Integrazione del rischio quantistico nelle procedure di gestione del rischio

- **Registro dei rischi -** Includere il rischio quantistico per monitorarlo e prioritizzarlo.
- **Mappatura dei dati -** Identificare annualmente i sistemi più esposti al rischio quantistico.

Valutazione di fornitori e terze parti

- **Analisi del rischio dei fornitori -** Valutare i piani di prontezza quantistica e il valore dei dati accessibili dai fornitori.
- **Mitigazione del rischio dei fornitori –** Collaborare con i fornitori per ridurre i rischi quantistici proporzionati al loro impatto sull'organizzazione.

Decisioni strategiche per l'adozione futura della tecnologia quantistica – Le organizzazioni, per circoscrivere il rischio quantistico, devono valutare l'infrastruttura tecnica e adottare una cripto-agilità. È importante sperimentare e valutare nuove tecnologie, integrando soluzioni ibride di crittografia e considerando tecnologie emergenti come la distribuzione di chiavi quantistiche. Le organizzazioni devono altresì prepararsi all'adozione della tecnologia quantistica, sviluppando un contesto tecnologico cripto-agile e un ciclo di vita del prodotto che supporti la sicurezza quantistica.

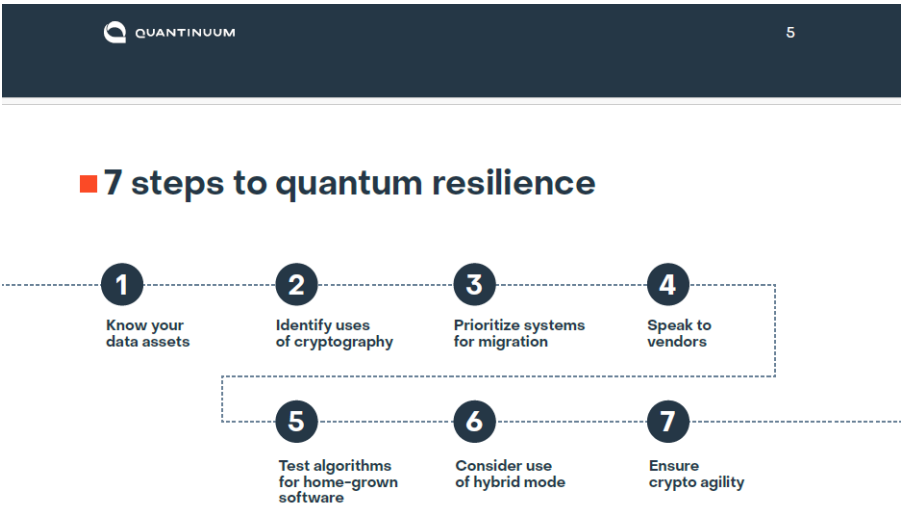
Collaborazione tra ecosistemi - La collaborazione tra ecosistemi è fondamentale per affrontare i rischi sistemici legati alla sicurezza quantistica. Pertanto, le organizzazioni devono stabilire sinergie con i fornitori, i partner della catena di approvvigionamento, le istituzioni ed il mondo accademico per condividere conoscenze e mitigare collettivamente il rischio quantistico. La cooperazione può contribuire, infatti, a definire standard tecnici condivisi, oltre a favorire l'innovazione attraverso collaborazioni con il mondo accademico e industriale.

Come prepararsi al futuro quantistico - Resilienza quantistica in sette passaggi

L'imperativo di agire ora è guidato dalla consapevolezza che, sebbene non si sappia con precisione quando sarà disponibile un computer quantistico sufficientemente potente, il tempo per prepararsi si sta riducendo. Pertanto, le organizzazioni devono avviare immediatamente il processo di adattamento, approfittando del tempo a disposizione per una transizione sicura verso la crittografia quantistica. A tal proposito si segnala una recente guida della società di quantum computing americana Quantinuum - nata dalla fusione di Cambridge Quantum e Honeywell Quantum Solutions – che fornisce indicazioni per costruire la resilienza quantistica in sette fasi.

Quantinuum Report - "7 steps to build quantum resilience"

- **Conoscere i propri asset di dati -** Identificare i dati che rappresentano il maggiore rischio per l'organizzazione in caso di violazione, comprendendo esattamente quali informazioni si possiedono e valutando la loro vulnerabilità agli attacchi.
- **Prioritizzare i sistemi per la migrazione -** Catalogare i punti in cui sono attualmente utilizzati algoritmi vulnerabili al quantum e stabilire le priorità per la migrazione basandosi su una valutazione di gestione del rischio.
- **Identificare gli usi della crittografia -** Creare un catalogo che mostri dove vengono impiegati algoritmi crittografici vulnerabili al quantum.
- **Testare algoritmi per software sviluppati internamente -** Le organizzazioni che sviluppano software proprietario dovrebbero iniziare a testare gli algoritmi indicati dal NIST per la crittografia quantistica. Questi algoritmi hanno caratteristiche diverse da quelli tradizionali e l'unico modo per valutarne l'impatto sui sistemi aziendali è sperimentarli. Un buon punto di partenza è il progetto Open Quantum Safe che fornisce implementazioni di algoritmi per la sperimentazione.
- **Considerare l'uso di modalità ibride -** Le modalità operative ibride combinano algoritmi tradizionali, vulnerabili al quantum, con algoritmi sicuri dal punto di vista quantistico, rafforzando la sicurezza in protocolli come TLS (Transport Layer Security) o SSH (Secure Shell). Questo approccio richiede che un attaccante superi sia l'algoritmo tradizionale che quello quantistico sicuro. Sebbene l'uso delle modalità ibride sia limitato dalla mancanza di standardizzazione, esse rappresentano attualmente un'opportunità per sperimentare algoritmi non ancora standardizzati in ambienti chiusi.
- **Conoscere le strategie dei fornitori -** Le organizzazioni devono verificare le strategie dei loro fornitori per quanto riguarda la sicurezza quantistica, soprattutto in contesti in cui le soluzioni di terze parti sono predominanti. I fornitori dovrebbero essere già impegnati a testare e aggiornare i loro algoritmi per l'era quantistica. Pertanto, se un fornitore non dimostra preparazione o chiarezza su questi temi, è fondamentale rivalutare la partnership e stabilire un piano d'azione.
- **Assicurare l'agilità crittografica -** È fondamentale avere la capacità di adattare rapidamente i sistemi e i processi per passare da un algoritmo crittografico all›altro, in risposta a nuove vulnerabilità o per ottimizzare la sicurezza in ambienti specifici. Pertanto, l'agilità è cruciale nella transizione verso misure crittografiche resistenti ai computer quantistici, consentendo la sostituzione rapida di algoritmi problematici e prevenendo l'uso prolungato di crittografia obsoleta.



Fonte immagine - "7 steps to build quantum resilience" – Quantinuum Report.

Conclusione

Il calcolo quantistico può trasformare vari settori, ma presenta nuove sfide per la sicurezza informatica. La capacità dei computer quantistici di violare i metodi crittografici esistenti richiede un cambiamento radicale nelle strategie di sicurezza. È essenziale integrare la crittografia post-quantistica, aggiornare i protocolli di sicurezza e utilizzare tecnologie come la distribuzione delle chiavi quantistiche (QKD) per proteggere le informazioni sensibili e garantire la sicurezza dei sistemi digitali.

Mentre ci avviciniamo a questa rivoluzione tecnologica, l'adozione proattiva di misure di sicurezza informatica sarà cruciale per affrontare le complessità di un mondo dominato dai quanti. Inoltre, la collaborazione tra governi, leader del settore e istituzioni accademiche è quanto mai fondamentale per sviluppare soluzioni resistenti ai quanti e garantire una transizione sicura all'era quantistica.

I servizi di sicurezza informatica devono rimanere agili, adattarsi continuamente alle nuove minacce e integrare tecnologie innovative per proteggersi dal panorama in continua evoluzione dei rischi informatici. Concludendo, solo con un'azione congiunta e coordinata sarà possibile affrontare le sfide della crittografia nell'era quantistica, assicurando un futuro digitale sicuro e resiliente, fondato sull'integrazione di principi di risk management, di continuità operativa e di sicurezza informatica.

Fonti

- CESP REPORT 2023, *Quantum technologies and cybersecurity – Technology, governance and policy challenges GES*
  https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf
- World Economic Forum (WEF) - *2022, Quantum Computing Governance Principles*, Insight Report, January
  https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf
- WEF-DELOITTE - *Quantum Readiness Toolkit* - 2024
  https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/
- Quantinuum - *Proactive steps to build quantum resilience*
  https://www.quantinuum.com/campaign/cisoguide
- EU digital strategy - *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*
  https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Dall'assessment cyber al trasferimento del rischio residuo nel complesso scenario di minacce e responsabilità: una collaborazione virtuosa

[A cura di Paola Girdinio e Georgia Cesarone (Centro di Competenza START 4.0) e Chiara Gatti (UnipolSai)]

A settembre 2024 ENISA ha rilasciato la pubblicazione "ENISA Threat Landscape 2024".

Dal report si evincono le tendenze osservate tra luglio 2023 e giugno 2024 relative alle principali minacce informatiche.

La relazione evidenzia un ulteriore aumento significativo negli attacchi informatici, esasperata dalla situazione geopolitica internazionale, che ha avuto un forte impatto sulle infrastrutture critiche dell'Unione Europea. Tra le minacce principali, spiccano nuovamente i ransomware e gli attacchi DDoS che continuano ad essere le più frequenti, insieme alle minacce contro i dati e l'affinarsi delle tecniche di social engineering con l'aumento dell'uso di strumenti di intelligenza artificiale da parte dei criminali informatici, con strumenti come FraudGPT utilizzati per creare e-mail di truffa e script dannosi.

Un punto centrale del report riguarda l'emergente utilizzo di tecniche avanzate da parte degli attaccanti, quali il Living Off Trusted Sites (LOTS), che consente agli

aggressori di mimetizzarsi utilizzando piattaforme legittime per evitare rilevamenti. L'uso di servizi cloud per nascondere le comunicazioni è aumentato notevolmente, insieme al Living Off the Land (LOTL), che permette agli attori di sfruttare strumenti presenti nei sistemi attaccati per eseguire attività malevole senza essere scoperti.

Altri punti significativi da sottolineare sono l'importanza della manipolazione delle informazioni che si impone come una delle principali minacce ibride, in particolare in relazione alla guerra in Ucraina e agli eventi politici, come le elezioni europee e l'aumento degli attacchi di compromissione della supply chain, con esempi di attacchi che mirano a introdurre backdoor nei software open-source.

Le principali raccomandazioni per prevenire e proteggere le organizzazioni includono il rafforzamento delle collaborazioni pubblico-private per migliorare la resilienza informatica e la protezione delle infrastrutture critiche e l'adozione di tecnologie e misure preventive più avanzate per far fronte a queste minacce in continua evoluzione.

Il quadro attuale, unito al framework normativo in continua evoluzione al quale le organizzazioni devono adeguarsi, porta con sé chiare e definite responsabilità e rende l'attivazione di polizze assicurative sulla cybersecurity sempre più rilevante per le aziende e le organizzazioni di ogni settore. ù

È opportuno evidenziare alcuni legami chiave tra la situazione descritta e l'importanza di stipulare le polizze assicurative:

Responsabilità e costi legati all'aumento degli attacchi ransomware e DDoS

Le minacce legate al ransomware e agli attacchi Denial of Service, come abbiamo visto dal report ENISA, sono tra le più comuni e pericolose. Questi attacchi possono interrompere le operazioni aziendali, causare perdite finanziarie e compromettere dati sensibili. Le polizze assicurative per la cybersecurity possono coprire i costi di ripristino, le perdite legate a interruzioni delle attività e le azioni di responsabilità civile dei terzi. Questi costi, senza una copertura assicurativa, hanno portato in passato anche al fallimento di alcune aziende e naturalmente si trovano più esposte soprattutto quelle di piccole e medie dimensioni.

Responsabilità e costi legati alla crescita della manipolazione delle informazioni e delle frodi digitali

Le campagne di manipolazione delle informazioni e le frodi digitali sono in aumento e rendono estremamente pericolosi e ingannevoli gli attacchi basati sul phishing e l'abilitazione di nuove tecniche di social engineering. Le polizze assicurative sulla cybersecurity possono coprire i danni derivanti da questi eventi, inclusi i costi legali e le spese per la gestione della reputazione aziendale, che possono essere gravemente danneggiate da attacchi di questo tipo.

Responsabilità e costi legati all'impatto finanziario degli attacchi alla supply chain

I crescenti attacchi alla supply chain sono di elevata gravità e spesso colpiscono più settori. Per questo è uno dei punti critici sottolineati dalla nuova direttiva europea NIS2 che può provocare danni a cascata lungo tutta la catena di fornitura. Dal punto di vista dell'impatto, un attacco di questo tipo può generare costi di riparazione e interruzione dell'attività che possono essere coperti da polizze assicurative.

Responsabilità e costi legati all'adeguamento normativo in continua evoluzione

Le conseguenze della non conformità alle normative su privacy e cybersecurity includono multe significative legate a chiare responsabilità e possibili azioni legali, oltre a danni reputazionali e operativi.

Le polizze assicurative sulla cybersecurity possono offrire una copertura per i costi associati a tali obblighi normativi, costi per la gestione e mitigazione degli incidenti di sicurezza e spese legali e di consulenza per affrontare i procedimenti giudiziari derivanti da violazioni.

Nel panorama appena descritto, attivare polizze di cybersecurity è diventato non solo un modo per gestire i rischi finanziari, ma una parte integrante della strategia di gestione del rischio di ogni organizzazione.

Ma quante sono le organizzazioni che attivano polizze cyber?

La stima del gap di protezione nel mercato della cyber insurance ammonta a circa 0,9 trilioni di dollari a livello globale[1].

Nonostante le proiezioni indichino una crescente offerta e domanda di polizze assicurative per il cyber, la colmatura del gap di protezione si prevede improbabile nel breve termine.

Poco meno di tre quarti delle polizze cyber risks è sottoscritto da grandi imprese, che spesso operano a livello globale e dispongono di una complessa infrastruttura digitale, risultando esposte a rischi particolarmente elevati di incidenti informatici. Le aziende che gestiscono dati sensibili dei clienti investono sempre più nelle coperture di *cyber liability*, spinte dall'aumento delle normative sulla protezione dei dati che comportano il rischio di cause legali e multe, mentre i fornitori di servizi tecnologici si approcciano con sempre maggior frequenza al mercato della cyber insurance, spinti da obblighi contrattuali imposti dai committenti nell'affidamento degli incarichi.

[1] Global protection gaps and recommendations for bridging them, March 2023, Global Federation of Insurance Associations (GFIA)

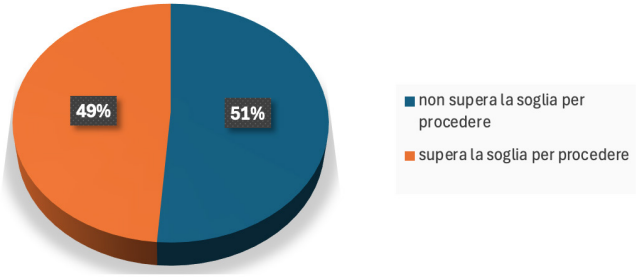
Un'industria che ha fatto da pioniere e ancora oggi rappresenta la quota di mercato maggiore è da sempre quella dei servizi bancari, finanziari e assicurativi.

Queste aziende tendono a investire massicciamente in polizze di assicurazione informatica per mitigare i rischi finanziari e di reputazione associati a incidenti.

Sul piano della distribuzione geografica, nel Nord America si rileva permanentemente il maggior tasso di penetrazione del mercato assicurativo cyber, con una spesa stimata in 4,5 miliardi di dollari e una quota di poco inferiore al 40% del mercato totale. Questa posizione dominante è probabilmente da attribuirsi all'infrastruttura tecnologica avanzata dell'area, alla presenza di grandi aziende multinazionali e alla maggiore consapevolezza delle minacce informatiche.

Per quanto riguarda le PMI italiane, invece, il panorama non è così confortante. Della gran parte delle aziende che manifesta interesse ad una copertura assicurativa, secondo i processi di risk assessment condotti da UnipolSai (compilazione di un questionario tecnico), poco meno del 50% ha una postura di sicurezza informatica che le rende idonee alla stipula di un'assicurazione cyber.
Circa il 3,6% delle stesse sin da un'analisi esterna della superficie di attacco mostra vulnerabilità tali da non poter proseguire nel processo di valutazione dell'idoneità al trasferimento del rischio.

Aziende che hanno completato il questionario tecnico con Unipol-SAI



Complessivamente il 55% delle aziende che ha avviato un processo di cyber risk assessment, tra prima e seconda fase, è risultato avere un profilo di rischio non assicurabile.

Da questi dati nasce il lungimirante rapporto tra UnipolSai e il Centro di Competenza per la sicurezza e l'ottimizzazione delle infrastrutture strategiche START 4.0, partenariato pubblico-privato e soggetto attuatore PNRR per conto del Ministero delle Imprese e del Made in Italy con fondi dedicati alla trasformazione digitale sicura delle imprese, in particolare PMI.

Ricordiamoci infatti di una delle principali raccomandazioni di ENISA: è fondamentale rafforzare le collaborazioni pubblico-private per migliorare la resilienza informatica.

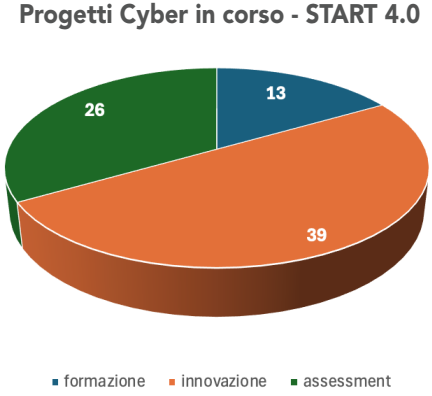
Questo non è una novità: Michael Chertoff, ex Segretario del Dipartimento della Sicurezza Interna degli Stati Uniti sottolineava che "Nella sicurezza informatica, le partnership non sono facoltative, ma essenziali. Sia il settore pubblico che quello privato offrono capacità uniche, e solo lavorando insieme possiamo costruire una difesa veramente resiliente."

D'altronde la Commissione Europea in riferimento alla direttiva NIS2 dichiarava che "NIS2 stabilisce un alto standard per la sicurezza informatica in tutti i settori critici. La cooperazione pubblico-privato è fondamentale per garantire che questi standard siano rispettati e per difendersi da minacce informatiche sempre più sofisticate."

In questo quadro nasce un accordo di collaborazione con cui UnipolSai segnala ai clienti che hanno una bassa postura cyber di richiedere un assessment al Centro di Competenza START 4.0.

Il Centro di Competenza START 4.0 ha infatti contribuito a sviluppare il modello nazionale di cybersecurity assessment utilizzato dalla rete di Confindustria e dei Digital Innovation Hub ed è quindi un soggetto con competenze verticali non solo nella cybersecurity IT, ma anche nella cybersecurity OT e IoT e nella loro convergenza verso l'IT.

Essendo START 4.0 soggetto attuatore PNRR può valutare se il progetto di adeguamento sia in linea con i finanziamenti erogati dal Ministero per contribuire alla messa in sicurezza delle PMI in questa difficile fase di adeguamento. Inoltre, nel progetto START 4.0 verifica sempre che ci siano tutte le componenti essenziali sui 3 pilastri di tecnologia, processi e persone che concretamente contribuiscono al vero raggiungimento degli obiettivi in termini di sicurezza e vantaggio competitivo.



Nei primi 9 mesi del 2024, il Centro di Competenza ha erogato 26 servizi di cybersecurity assessment conclusi con la stesura di un remediation plan atto all'adeguamento aziendale e ne ha in attivazione altri 24 entro la fine dell'anno.

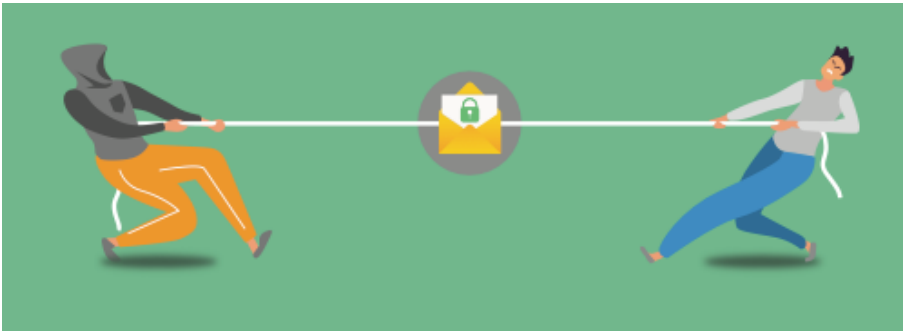
Va sottolineato però che tutti i servizi attivati includono la verifica della sicurezza delle soluzioni progettate in fase di pre-analisi.

Complessivamente il Centro di Competenza ha in corso 78 progetti in ambito cybersecurity: 13 formazione, 39 innovazione, 26 assessment sia con Enti che con aziende di tutte le dimensioni, ma in particolare PMI.

Non è semplice portare questo tipo di consapevolezza nelle imprese, ma come diceva Mark Twain: "*Il segreto per andare avanti è iniziare*".

Il divario di realtà - Focus sulla crescente disparità tra rischio e prevenzione negli attacchi via e-mail

[A cura di Rodolfo Saccani, Libraesva]



Introduzione

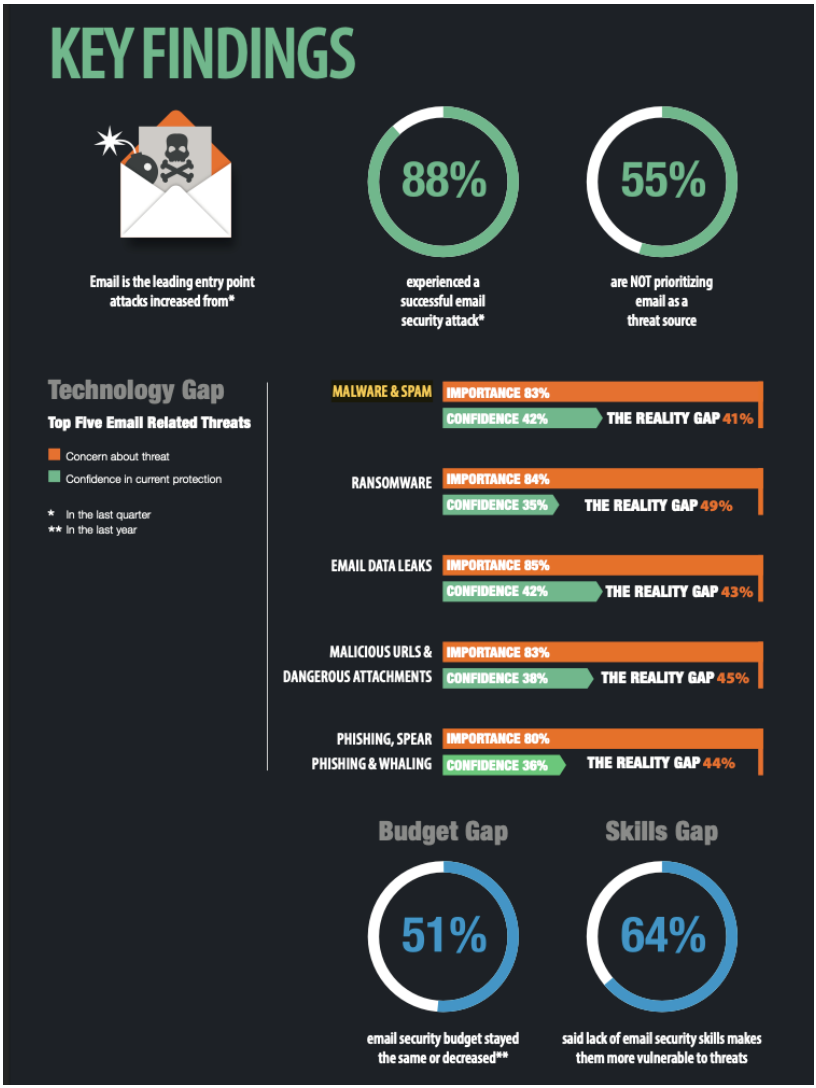
La sicurezza digitale è da sempre un campo di battaglia tecnologico tra criminali informatici e professionisti della sicurezza. Essendo la prima e più diffusa forma di comunicazione digitale, l'e-mail ha rappresentato per decenni un fronte fondamentale per la sicurezza informatica. Oggi i criminali stanno guadagnando terreno, in quanto emerge un divario sempre più ampio tra la loro capacità di lanciare attacchi via e-mail e la capacità delle vittime di prevenirli.

La porta aperta

Partendo da un nostro studio commissionato negli USA, abbiamo scoperto che anche in Italia nonostante l'e-mail sia un vettore di attacco primario per i criminali informatici, la maggior parte delle aziende - di tutte le dimensioni - sta perdendo terreno nei confronti della complessità dell'email security contemporanea. L'aspetto che riteniamo più rilevante è che ciò non è dovuto a mancanza di conoscenza poiché la maggior parte dei CISO, dei professionisti di sicurezza e IT ha un'adeguata comprensione i rischi.

Le minacce alla sicurezza dell'email sono aumentate drasticamente in volume e complessità negli ultimi anni rendendo sempre più obsoleti gli strumenti utilizzati tradizionalmente.
Sebbene sia buona pratica preferire, a parità di efficacia, sistemi e tecniche di difesa semplici, il complesso scenario attuale richiede necessariamente l'adozione di sistemi di difesa di crescente complessità per far fronte ai trend in corso anche nel 2024.

La disconnessione tra sorgente e contenuto, l'aumento degli account compromessi e l'ascesa dell'intelligenza artificiale nel phishing non sono efficacemente contrastati dalle aziende. Secondo la nostra ricerca, quasi 9 su 10 (88%) tra i CISO e i professionisti di sicurezza e IT intervistati ha dichiarato che la propria organizzazione ha subìto un attacco via mail andato a buon fine negli ultimi tre mesi, con una media di nove attacchi a buon fine per ciascuna organizzazione.



Il security gap si ampia mentre gli investimenti stagnano

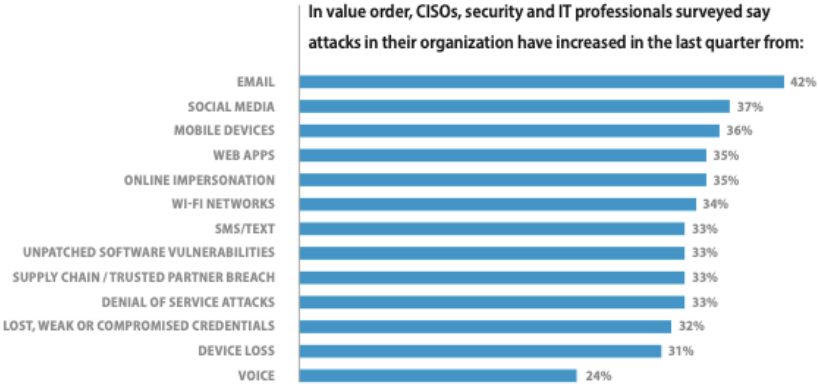
Nel 2024, il costo dei crimini informatici è destinato a raggiungere i 9.22 trilioni di dollari globalmente, con un aumento costante fino a 13.82 trilioni di dollari nel 2028.

Con strumenti sempre più sofisticati, non è sorprendente che quasi tre quarti (74%) dei CISO, professionisti della sicurezza e IT intervistati abbiano dichiarato che le proprie organizzazioni hanno difficoltà a tener testa alle minacce di sicurezza.

Gli attacchi informatici via email stanno aumentando. Secondo i CISO e i professionisti intervistati, l'e-mail è stato il canale più utilizzato per gli attacchi informatici nell'ultimo trimestre.

La mancanza di investimento nell'email security è preoccupante. Solo la metà (47%) dei CISO, professionisti della sicurezza e IT intervistati ha notato un aumento del proprio budget per email security rispetto all'anno precedente.

Mentre gli attaccanti sviluppano tecniche sempre più sofisticate, il gap tra questi attacchi e la capacità di contrasto dei metodi tradizionali di email security è destinato a crescere.



Il gap di talenti sta impattando l'email security

La ricerca di personale con competenze altamente specializzate nel settore IT e sicurezza è risultata problematica negli ultimi anni. Nel 2023, il "gap di talento" ha raggiunto il suo massimo storico in 17 anni.

Questo problema è particolarmente evidente quando si parla della sicurezza dell'e-mail. Secondo la nostra ricerca, più della metà (63%) dei CISO, professionisti della sicurezza e IT ritiene che le risorse per l'email security siano insufficienti nella propria azienda.

La mancanza di risorse e competenze idonee lascia la porta aperta ai malintenzionati. Quasi due terzi (64%) degli intervistati ritiene che la mancanza di talento renda la propria azienda vulnerabile alle minacce via email.

Le aziende che hanno subito un attacco andato a buon fine dichiarano più frequentemente che le risorse per l'email security nella loro azienda sono insufficienti.

Le grandi aziende soffrono di più

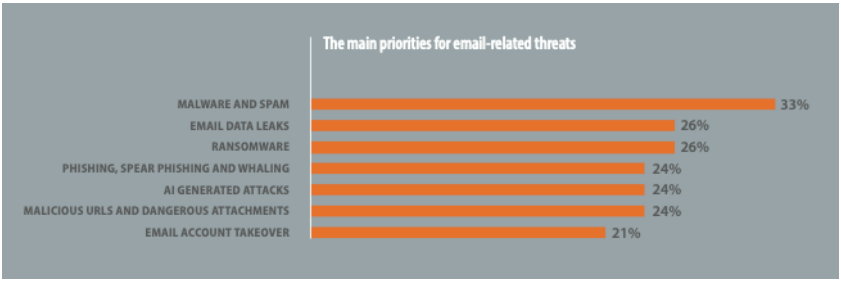
La maggior parte delle grandi aziende sta soffrendo le conseguenze degli attacchi via email. In passato si riteneva che le aziende più grandi fossero meno vulnerabili ai rischi di sicurezza informatica avendo più mezzi per investire in robuste misure preventive.

Tuttavia, la nostra indagine ha scoperto che questo trend si è invertito per quanto riguarda l'email security. La metà (50%) dei CISO, professionisti della sicurezza e IT

intervistati in aziende con 2001-5000 dipendenti ha dichiarato che gli attacchi via email verso le proprie aziende sono aumentati nell'ultimo trimestre, rispetto a meno di un terzo (31%) di quelli in aziende con 1501-2000 dipendenti.

Allo stesso tempo, le aziende più grandi stanno investendo solo marginalmente più risorse nella sicurezza dell'e-mail. La metà (51%) dei CISO, professionisti della sicurezza e IT intervistati in aziende con 2.001-5.000 dipendenti ha dichiarato che la sicurezza dell'e-mail è una priorità, rispetto al 40% di quelli in aziende con 1.501-2.000 dipendenti.

È lecito attendersi che i "bad actors" continueranno a migliorare in sofisticazione e pianificazione degli attacchi rendendo le grandi aziende sempre più i bersagli preferiti dei criminali. Con un migliore "ritorno sull'investimento" per gli attacchi, ci aspettiamo che saranno soprattutto i sistemi di email security delle grandi aziende a doversi confrontare con le più recenti ed efficaci strategie del crimine informatico. C'è uno sbilanciamento tra il livello di rischio attuale e i mezzi dedicati a mitigarlo.



I gap nella difesa dalle minacce emergenti

La nostra indagine ha esposto diversi trend e minacce chiave che stanno alimentando la crescita degli attacchi via email, nonché evidenziato la capacità – o, spesso, la mancanza di essa – delle aziende ad affrontare tali minacce (vedi immagine alla pagina seguente).


ZERO DAY THREATS
(i.e. new or unknown threats)
IMPORTANCE 80%
CONFIDENCE 24%
THE REALITY GAP 56%
UNUSUAL OR SUSPICIOUS
)MMUNICATION PATTERNS & BEHAVIOR
IMPORTANCE 82%
CONFIDENCE 32%
THE REALITY GAP 50%
SUPPLY CHAIN ATTACKS /
VENDOR EMAIL COMPROMISE
IMPORTANCE 79%
CONFIDENCE 32%
THE REALITY GAP 47%
SPOOFED SENDER DOMAIN
IMPORTANCE 81%
CONFIDENCE 38%
THE REALITY GAP 43%
SOCIAL ENGINEERING
IMPORTANCE 79%
CONFIDENCE 30%
THE REALITY GAP 49%
RANSOMWARE
IMPORTANCE 84%
CONFIDENCE 35%
THE REALITY GAP 49%
PHISHING, SPEAR PHISHING
& WHALING
IMPORTANCE 80%
CONFIDENCE 36%
THE REALITY GAP 44%
MALWARE & SPAM
IMPORTANCE 83%
CONFIDENCE 42%
THE REALITY GAP 41%
MALICIOUS URLs &
DANGEROUS ATTACHMENTS
IMPORTANCE 83%
CONFIDENCE 38%
THE REALITY GAP 45%
EMAIL DATA LEAKS
IMPORTANCE 85%
CONFIDENCE 43%
THE REALITY GAP 42%
EMAIL ACCOUNT TAKEOVER
IMPORTANCE 82%
CONFIDENCE 38%
THE REALITY GAP 44%
BUSINESS EMAIL COMPROMISE
IMPORTANCE 83%
CONFIDENCE 34%
THE REALITY GAP 49%
AI GENERATED ATTACKS
IMPORTANCE 80%
CONFIDENCE 29%
THE REALITY GAP 51%
Important to protect against threat
Confidence in current protection

Intelligenza artificiale

Molti settori sono stati scossi dalla rapida proliferazione dell'intelligenza artificiale e la sicurezza dell'email è uno di essi. In molti modi, l'AI è al cuore stesso della futura sicurezza dell'email - sia in senso positivo che negativo.

- I criminali possono usare l'AI per creare strumenti potenti e illeciti e per migliorare l'efficienza delle loro azioni. Le principali minacce sono due:

- L'utilizzo della AI generativa per creare email malevole sempre più convincenti a un ritmo e su una scala maggiori, amplificando la capacità di attacco oltre il testo, con l'inclusione di attacchi multimediali (spoofing di immagini, voci, video ecc.)

- I modelli di apprendimento automatico addestrati sulle informazioni rubate e sui comportamenti degli utenti possono essere utilizzati per rivelare informazioni e sfruttare le vulnerabilità in preparazione di un attacco futuro.

Quattro persone su cinque (80%) dei CISO, professionisti di sicurezza e IT intervistati ritiene importante che il sistema email security sia in grado di affrontare gli attacchi potenziati dall'AI, ma questa è solo la loro quarta preoccupazione in ordine di priorità, nonostante l'attenzione mediatica recente su AI.

Solo 29% può dire con fiducia che l'attuale sistema di email security protegge dagli attacchi generati da AI.

Phishing

Nell'anno successivo all'uscita pubblica di ChatGPT, le aziende hanno visto un aumento del 1.265% dell'email phishing.

Tuttavia, questi strumenti non hanno solo aumentato i volumi di phishing, spear phishing e whaling; gli attacchi sono divenuti anche più sofisticati attraverso l'imitazione dello stile di comunicazione o anche della voce di contatti fidati; non solo negli attacchi mirati ma su scala sempre più ampia, portando il social engineering a nuove altezze.

Il phishing è in bassa posizione nella lista delle priorità dei CISO, professionisti della sicurezza e IT coinvolti nello studio, con il solo 24% di loro che lo considera una priorità. Quattro su cinque (80%) partecipanti hanno dichiarato che gli attacchi phishing sono importanti da contrastare, ma solo il 36% di loro è fiducioso nel fatto che i propri sistemi di sicurezza email possano far fronte a questi attacchi.

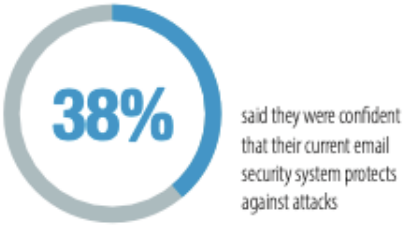
Spoofing dei domini

Con l'evolversi delle strategie di attacco da parte degli attori malevoli, non è possibile giudicare se un'email è sospetta solo dal suo indirizzo di provenienza.

All'inizio del 2023, Google e Yahoo hanno aggiunto nuovi requisiti con l'obiettivo di ridurre lo spam e promuovere l'adozione di DMARC per contrastare lo spoofing dei domini. Tuttavia, l'adeguamento delle aziende al DMARC è stato lento.

Sebbene sia una priorità bassa per gli specialisti di IT e della sicurezza, l'81% degli intervistati concorda sul fatto che i propri sistemi di sicurezza email debbano essere in grado di gestire attacchi di spoofing.

Ecco riemergere lo stesso divario tra minaccia e azione: solo il 38% dei partecipanti può dire con certezza che i propri sistemi di sicurezza email attuali proteggono contro tali attacchi.



Ransomware

La complessità dei moderni ransomware è resa evidente dalla scala delle organizzazioni attaccate.
Questi software malevoli, spesso venduti con un modello 'as-a-service', rendono il ransomware accessibile anche a criminali con un'insufficiente conoscenza tecnica.

A causa della natura pubblica di questi attacchi, non è sorprendente che il ransomware sia la terza priorità più grande per i CISO e gli specialisti di sicurezza e IT. L'84% di loro considera importante proteggersi. Tuttavia, c'è un divario tra la coscienza della minaccia e la risposta effettiva: solo il 35% dei partecipanti può dire con certezza che i propri sistemi di sicurezza email attuali proteggono contro il ransomware.

L'AI può chiudere il security gap nell'email?

L'obsolescenza delle tecniche di email security e le crescenti ambizioni dei criminali, sia nella scala che nella complessità delle loro operazioni, richiedono continui adattamenti. La capacità dei sistemi di email security di identificare discrepanze tra un'email e i pattern di comunicazione legittimi tra quel mittente, quel destinatario e l'organizzazione nel suo complesso, diventa importante. Fare spoofing di pattern di comunicazione (inclusa la propria storia di relazioni con la vittima e la sua organizzazione) è assai più difficile del fare spoofing di elementi tutti contenuti all'interno di una singola email.

Questo è un compito che richiede una comprensione della tipologia di relazione, dei suoi pattern e degli stili di comunicazione, oltre ad un continuo aggiornamento di queste conoscenze. Un compito per il quale gli algoritmi per l'apprendimento automatico e i grandi modelli linguistici possono fornire un contributo, classificando i comportamenti tipici e modellando un contesto di sfondo contro il quale giudicare le anomalie.

Con l'integrazione di questa nuova tipologia di intelligenza artificiale, le soluzioni di email security diventano adattive e proattive, migliorando costantemente per rimanere un passo avanti rispetto alle minacce emergenti. In un momento in cui i team di sicurezza sono sottodimensionati e sovraccarichi, l'occhio attento dell'intelligenza artificiale ha la potenzialità di divenire essenziale per chiudere il gap di sicurezza della posta elettronica che attualmente sta lasciando le aziende in una situazione di crescente esposizione.

Conclusioni

Siamo partiti da un report, unico nel suo genere, da noi commissionato negli USA per scoprire l'impatto degli attacchi via email nel 2024 e l'efficacia delle risposte delle organizzazioni. Essendo la nostra una azienda nata, cresciuta e fortemente radicata in Italia, tanto che a tutt'oggi l'intera attività di ricerca e sviluppo e di sviluppo dei prodotti è interamente basata in Italia, abbiamo voluto confrontarne i risultati con la realtà italiana, trovando una sostanziale omogeneità nei principali indicatori.
I risultati di questa ricerca rappresentano un avvertimento.

La maggior parte delle aziende mostra seri elementi di inadempienza nella difesa corrente, nella preparazione contro le minacce emergenti e nelle competenze necessarie per stare al passo.

È ormai una questione di urgenza per le aziende il colmare il divario tra la crescente esposizione agli attacchi via email e le azioni intraprese per prevenirli. Le innovazioni tecnologiche nella sicurezza degli email possono aiutare, ma le risorse e gli staff di cybersecurity sono estremamente sottodimensionati e questo significa che le soluzioni tecniche devono essere sia economiche che minimizzare l'effort della loro gestione diretta.
L'intelligenza artificiale si è rivelata una vera novità. L'apprendimento automatico e i modelli linguistici ben si adattano al mondo ad alta densità di dati della sicurezza delle email, dove la rilevazione delle minacce rappresenta un problema di ricerca dell'"ago nel pagliaio" nella migliore delle ipotesi.
È iniziato un nuovo round nel confronto tra i criminali e gli specialisti nella sicurezza. Questa volta entrambi sono armati con l'intelligenza artificiale.

Come utilizzare la AI per accelerare detection, investigation e response

[A cura di Luca Nilo Livrieri e Alberto Greco, CrowdStrike]

Nell'ultimo anno si è affermata la consapevolezza che, mentre la AI non sostituirà necessariamente gli esseri umani, gli esseri umani che utilizzano la AI avranno un grande vantaggio su quelli che non la utilizzano.

Questa considerazione si applica anche alla prossima era della cybersecurity, il cui sviluppo ha subito una accelerazione significativa nell'ultimo anno. Le recenti scoperte nel campo della AI generativa sono molto promettenti per chi si occupa di defensive security. Tra la duplice pressione dell'accelerazione degli attacchi - che in alcuni casi si riducono a poco più di due minuti - e la persistente carenza di competenze, la AI generativa ha il potenziale per essere non solo un acceleratore, ma un vero e proprio moltiplicatore di forze per i team di ogni dimensione e livello di maturità. Abbiamo potuto constatare di persona questi impressionanti vantaggi con utenti che hanno segnalato incrementi di velocità fino al 75% nei flussi di lavoro supportati.

Per rendere gli operatori più efficaci ed efficienti possibile è necessario fornire loro gli strumenti migliori per svolgere i loro compiti. L'attuale panorama della AI include un gran numero di modelli, numero peraltro in continua crescita; tali modelli sono stati sviluppati da comunità open source, da startup o da grandi aziende e avere una idea chiara di quali siano i modelli più adatti alle diverse esigenze può essere complesso. Ogni modello è unico nei suoi punti di forza e nelle sue applicazioni, variando in termini di velocità, accuratezza, dati di addestramento, intensità di calcolo e rischi sottostanti per gli utenti finali. Inevitabilmente, la scelta di un solo modello, o di una sola famiglia di modelli, può costringere gli utenti ad accettare compromessi su una qualsiasi di queste variabili.

I team di sicurezza non dovrebbero essere costretti a scendere a compromessi sugli strumenti che utilizzano per proteggere le loro aziende. In un mondo ideale, i loro strumenti dovrebbero supportare i requisiti di velocità e precisione richiesti dalla enorme mole di flussi di lavoro che devono essere supervisionati, senza compromessi in termini di prestazioni e rischi e senza imporre a chi si occupa di difendere l'ecosistema aziendale l'onere di prendere in considerazione la complessità computazionale.
Per questo, fra le varie possibilità, spiccano i sistemi Multi-AI che suddividono i flussi di lavoro in singole funzioni distinte e consentono ai data scientist di isolare, testare

e confrontare l'efficacia dei diversi modelli nelle varie attività. Questo approccio consente di scambiare dinamicamente i modelli fondamentali applicati ai flussi di lavoro, assicurando agli utenti finali di interagire con un assistente AI in costante miglioramento, alimentato dalle più recenti tecnologie di AI generativa del settore.

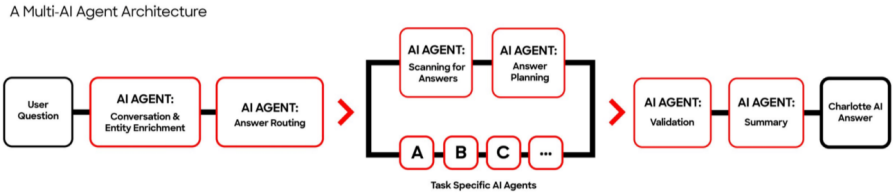
Dietro le quinte: dalla domanda alla risposta con gli agenti AI

L'assistente conversazionale AI consente agli operatori di liberare la potenza di trasformazione dell'AI generativa nei flussi di lavoro della sicurezza. Con una semplice domanda, gli utenti possono attivare l'intelligenza artificiale per rispondere a domande sui loro ambienti, generare script o analizzare le informazioni emergenti sulle minacce. Le capacità di elaborazione naturale riducono il livello di competenza e di esperienza necessario per prendere decisioni rapide ed accurate in materia di sicurezza, consentendo anche agli analisti più esperti di ottenere incrementi di velocità in ogni fase dei loro processi operativi, dalla individuazione delle segnalazioni in cui il fattore tempo è critico, all'analisi degli incidenti, fino agli interventi operativi che aiutano nella risposta.

I sistemi "Multi-AI" orchestrano molteplici "agenti AI" orientati alle attività per interpretare la domanda di un utente, pianificare i passaggi necessari per assemblare una risposta completa e strutturare il risultato finale. Ogni agente AI è un sottosistema costituito da un modello e dal suo codice di riferimento che gli consente di svolgere compiti specifici e di interagire con altri agenti. Si può pensare che l'LLM (o un'altra classe di modelli sottostanti) di ogni agente AI sia il suo "cervello" e che le funzionalità uniche di ogni agente (abilitate dal codice di riferimento) siano le abilità che gli permettono di eseguire compiti specifici.

Possiamo pensare a questi agenti di intelligenza artificiale come ad un'équipe di medici che lavorano di concerto in una sala operatoria, ognuno dei quali supervisiona compiti specializzati, dalla somministrazione dell'anestesia all'intervento su specifiche aree di interesse. Allo stesso modo, ogni agente di intelligenza artificiale ha una responsabilità specifica ed una specifica area di competenza. Proprio come un'operazione che richiede la collaborazione di un team di specialisti, la task force dinamica di agenti AI lavora insieme per supportare un numero crescente di processi operativi: dalla sintesi delle informazioni sulle minacce, alla scrittura di query, alla assistenza nelle indagini sugli incidenti.
Ad alto livello, l'AI ricorre agli agenti AI per strutturare le risposte nella seguente sequenza:

- **Fase 1 -** Comprensione della domanda: inizialmente l'AI attiva gli agenti AI con il compito di comprendere il contesto della conversazione dell'utente e di estrarre le entità a cui si fa riferimento nella domanda, come gli attori delle diverse minacce, le vulnerabilità o le caratteristiche dell'host.
- **Fase 2 -** Instradamento dei singoli compiti agli agenti AI: l'intelligenza artificiale attiva un router che determina quale agente o quali agenti AI assegnare alla richiesta dell'utente.
- **Fase 3a -** Analisi delle risposte: se un utente pone una domanda che richiede dati da una o più chiamate API, la richiesta viene passata ad un agente dedicato all'interno che assicura che le informazioni vengano recuperate e rese disponibili per un'ulteriore elaborazione.
- **Fase 3b -** Pianificare le risposte alle domande: se la domanda dell'utente non corrisponde a una o più chiamate API (ad esempio, quando si chiede all'intelligenza artificiale di generare una query), l'agente AI può attivare una serie di altri agenti di intelligenza artificiale, appositamente studiati per svolgere compiti specifici.
- **Fase 4 -** Convalida del piano e dei dati ottenuti: l'agente runtime esegue le chiamate API definite dall'agente AI precedente. Il risultato di questo processo viene esaminato da un agente di validazione che determina se le informazioni ottenute sono complete o se richiedono ulteriori informazioni. L'agente AI può anche inviare un avviso all'utente finale se la risposta è incompleta.
- **Fase 5 -** Generazione della risposta: un agente AI finale struttura la risposta alla domanda dell'utente, tenendo conto dei modi intuitivi di presentare le informazioni all'utente finale e generando una sintesi delle informazioni presentate.



Guardrail contro la sovraesposizione degli LLM

I sistemi che forniscono agli utenti visibilità diretta all'output degli LLM (spesso definiti "naked LLM") rischiano di esporre agli utenti informazioni imprecise quando gli LLM si comportano in modo imprevisto, situazione che avviene quando gli LLM forniscono informazioni che non sono supportate dai dati originali o addirittura li contraddicono. Le informazioni imprecise possono avere implicazioni molto gravi per la

sicurezza, implicazioni che vanno dalla riduzione della produttività all'indebolimento della postura di sicurezza, sino ad una grave violazione.

È consigliabile utilizzare architetture Multi-AI che svolgono un ruolo fondamentale nel consentire un'esperienza utente sicura, fornendo meccanismi che isolano gli utenti finali dall'output diretto degli LLM. In primo luogo, grazie alla flessibilità di applicare diversi modelli nei flussi di lavoro, è possibile limitare gli effetti a catena delle variazioni inattese delle prestazioni derivanti da un singolo modello e inoltre l'utilizzo di un agente appositamente incaricato di validare le risposte prima che vengano presentate agli utenti finali, consente che le risposte siano coerenti con il tipo di risultato che l'utente si aspetta.

Potenziare i flussi di lavoro della sicurezza: dalla risposta all'azione

Mentre i modelli linguistici di grandi dimensioni raggiungono nuovi livelli di maturità, i team di sicurezza si trovano di fronte ad un panorama crescente di assistenti AI conversazionali. L'architettura Multi-AI consente agli utenti di sfruttare la potenza dei migliori modelli fondamentali e delle innovazioni più avanzate in tutti i loro flussi di lavoro, riducendo al minimo i compromessi derivanti dalla limitazione della selezione di un unico modello o di una famiglia di modelli. Questa adattabilità architetturale consente di migliorare l'efficacia di ogni analista, dotandolo delle conoscenze necessarie per prendere decisioni più rapide ed accurate ed avere un vantaggio di velocità nei confronti degli avversari moderni.

Innovazioni in ambito di triage ed analisi grazie all'intelligenza artificiale

La sicurezza informatica è un gioco basato sulla velocità. Con attacchi che possono avvenire anche in pochi minuti, l'agilità con cui i team di sicurezza possono rilevare e sconfiggere gli avversari può fare la differenza tra essere il cacciatore o la preda.
Tuttavia, avere un vantaggio di velocità nei confronti degli avversari può essere un compito complesso per i team di sicurezza. I difensori devono oggi fare i conti con ruoli di sicurezza non coperti, una complessità che ostacola l'agilità ed un volume di avvisi estremamente elevato. Tutti questi sono fattori che aggravano i tempi di risposta e fanno perdere minuti ed ore ai team in attività non urgenti. Nel frattempo gli avversari stanno raggiungendo nuovi livelli di complessità e capacità di muoversi in modo furtivo, con metodi sempre più di frequente coadiuvati dall'intelligenza artificiale e dalle tecnologie automatizzate.
Per garantire che i team siano in grado di bloccare le violazioni in modo più rapido ed

efficace che mai, è possibile utilizzare l'intelligenza artificiale per migliorare e accelerare ogni fase dell'esperienza degli analisti in molteplici parti del loro lavoro. Vediamone alcuni esempi: una capacità di ingestion dei data sources differenti facilitata, una ridefinizione della priorità delle detection, la visualizzazione di potenziali percorsi di attacco e l'accelerazione del triage di rilevamento ed analisi.

Use case 1 - Ingestion dei dati facilitato con i parser generati dall'intelligenza artificiale

Una delle maggiori sfide che i team di sicurezza devono affrontare si presenta prima ancora di iniziare ad analizzare le detection e parte dall'onboarding dei dati. I team di sicurezza sono sommersi da dati provenienti da innumerevoli nuove data sources, ognuna con un formato di log unico. Lo sviluppo di parser personalizzati per questi registri può essere un processo che richiede tempo e risorse, soprattutto perché i formati dei differenti log si evolvono costantemente. Tenere il passo con questi cambiamenti e garantire che i dati rimangano accurati e accessibili è una lotta continua e che spesso porta a ritardi nell'implementazione, ad un aumento dei costi e a team sovraccarichi.

L'intelligenza artificiale più evoluta, sta cambiando le regole del gioco grazie ai parser generati dall'AI che consentono ai team SOC di effettuare ingestion ed elaborare rapidamente i dati da qualsiasi fonte. Invece di scrivere i parser in modo manuale e di doverli aggiornarli ogni volta che cambiano i formati dei log, i team possono sfruttare la potenza della AI generativa per creare parser istantaneamente sulla base di log rappresentativi.

Per generare i parser, gli utenti devono semplicemente fornire dei log campion che siano rappresentativi per quella specifica piattaforma. A partire da questi dati, l'AI analizza i campioni con più modelli linguistici di grandi dimensioni (LLM) per imparare la struttura ed il contenuto. I parser generati dall'intelligenza artificiale aderiscono allo standard assicurando una correlazione perfetta e un migliore rilevamento delle minacce.

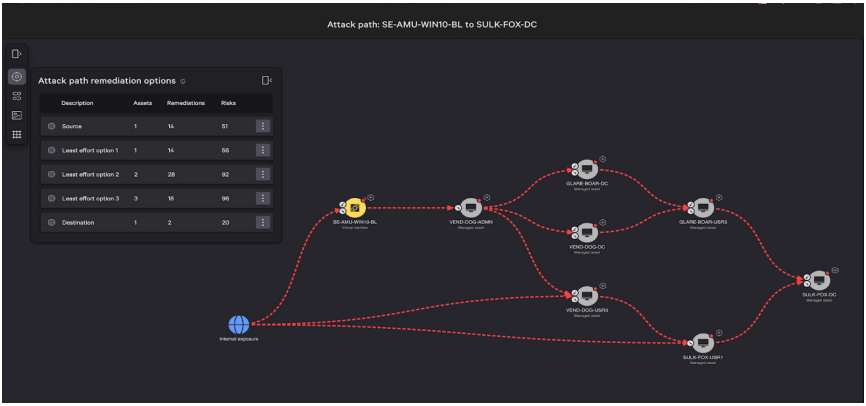
Grazie alla creazione dinamica di parser, i team di sicurezza possono eliminare ore di lavoro ed essere più veloci nella detection.

Use case 2 - Gestione proattiva dell'exposure con l'analisi degli "attack path" basata sull'intelligenza artificiale

Un altro problema che i team di sicurezza devono costantemente affrontare riguarda i processi per la gestione proattiva delle esposizioni ai rischi. Di fronte a migliaia di vulnerabilità e a risorse limitate, la definizione delle priorità è un compito impegnativo ma fondamentale per i team di sicurezza.

Gli strumenti tradizionali di gestione delle vulnerabilità spesso assegnano le priorità

alle vulnerabilità in base ai singoli punteggi di gravità, che non forniscono un contesto sufficiente per stabilire le priorità in modo efficace: oltre il 50% di tutte le CVE sono classificate come di gravità elevata o critica in base ai punteggi CVSS, offrendo informazioni limitate su cui lavorare. Questi punteggi ignorano anche il contesto del panorama in cui operano le aziende.
L'applicazione dell'AI predittiva e la tecnologia di apprendimento automatico consentono di migliorare la valutazione della gravità delle vulnerabilità. L'AI valuta in modo predittivo e dinamico la possibilità di sfruttamento di una vulnerabilità per restringere la percentuale di criticità su cui i team devono concentrarsi. Gli algoritmi di apprendimento automatico aiutano a rilevare i ruoli delle differenti risorse per informare sulla criticità aziendale dei diversi componenti, siano essi, ad esempio, un host utilizzato come punto di accesso, una e-mail o un server web, fornendo un importante contesto relativo all'ecosistema.
Grazie a queste informazioni l'AI crea un vero e proprio "percorso" di attacco ed evidenzia il modo in cui gli attaccanti potrebbero intromettersi e muoversi lateralmente nell'ambiente del cliente per compromettere i sistemi critici. I percorsi di attacco reali vengono distinti da quelli teorici e vengono identificati i punti di arresto o i vicoli ciechi, in modo che i team possano aumentare le loro difese per sigillare proattivamente i percorsi.
Inoltre l'Attack Path Analysis è in grado di mappare le connessioni tra asset cloud e on-premise, adattandosi alla tipologia dell'infrastruttura ibrida in cui vive la maggior parte delle aziende e di evidenziare le previsioni di attacco basati su CVE tradizionali e misconfigurazioni cloud-native. Vengono inoltre fornite raccomandazioni di remediation basate sulla prioritizzazione, ad alto impatto e a basso costo, in modo che i team possano agire rapidamente, facilitando una risposta mirata.



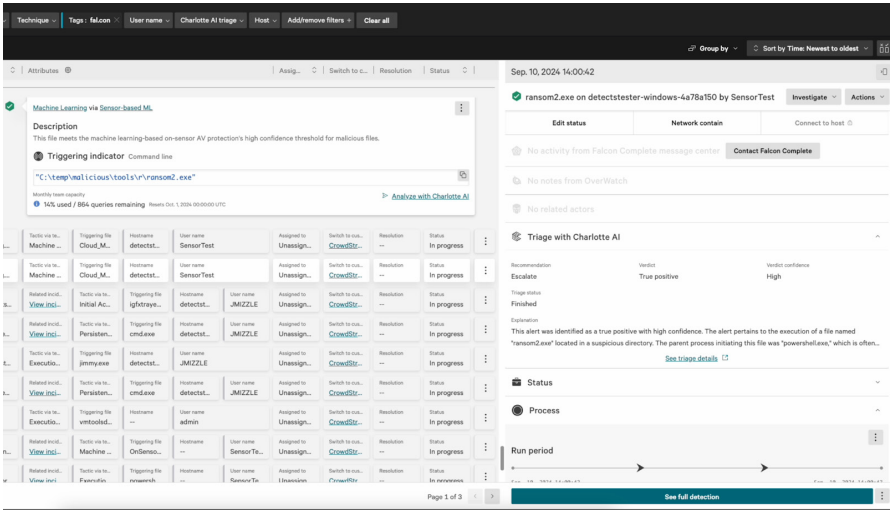
Use case 3 - Ridefinizione della priorità delle detection

Un'altra sfida legata alla capacità di prioritizzazione si presenta quando i team di sicurezza devono trovare "l'ago nel pagliaio", nello specifico far emergere le detection che meritano l'attenzione degli analisti con maggiore urgenza.
I sistemi di rilevamento tradizionali spesso faticano ad identificare minacce complesse e possono sommergere gli analisti con numerosi avvisi non prioritari; questo tipo di approccio tradizionale applica spesso regole e soglie generiche che non tengono conto delle caratteristiche specifiche di ogni ambiente. Senza l'assistenza dell'intelligenza artificiale, gli analisti devono eseguire manualmente il triage e mettere insieme informazioni disparate, con conseguente perdita di focus per gli avvisi più critici e la perdita di detection delle minacce reali.
L'intelligenza artificiale affronta queste sfide generando e dando priorità in modo contestualizzato alle segnalazioni automatiche. Raggruppando gli eventi correlati in analisi utilizzabili e fornendo un punto di partenza chiaro per le indagini, l'AI riduce il rumore di fondo, accelera il rilevamento e la risposta e garantisce che gli analisti della sicurezza di tutti i livelli di competenza possano identificare e neutralizzare rapidamente le minacce.
L'AI migliora il rilevamento precoce delle minacce analizzando un'ampia gamma di dati, compresi gli indicatori più lievi e sin dalle fasi iniziali, consentendo ai team di sicurezza di identificare e rispondere alle potenziali minacce prima che queste possano causare danni. Grazie all'approccio AI, la detection si adatta alle caratteristiche specifiche di ogni ambiente. Ciò garantisce che solo le minacce più rilevanti e critiche vengano visualizzate per la validazione da parte degli analisti, consentendo una prioritizzazione ed una risposta più accurate. Adattandosi alla singola azienda e fornendo una misura immediata della sua postura di sicurezza attuale, l'AI riduce la probabilità di minacce non identificate e migliora la sicurezza generale.

Use case 4 - Risposta più rapida grazie al triage di rilevamento guidato da GenAI

Un'ulteriore sfida che i team di sicurezza devono affrontare è quella di incrementare la velocità e la capacità di triage e di risposta. Per ridurre ulteriormente i tempi di indagine e risposta (MTTR), i team di sicurezza possono utilizzare l'AI per accelerare il triage dei rilevamenti, velocizzando le fasi più lunghe e maggiormente soggette ad errori del triage iniziale: riconoscere veri da falsi positivi e segnalare le differenti valutazioni. Questa funzionalità permette di utilizzare l'aiuto al triage dei rilevamenti fornito dall'AI per aumentare velocità, precisione e scalabilità della risposta. Come per tutte le azioni abilitate dall'AI, gli utenti possono configurare in anticipo le tipologie di rilevamenti a cui questa funzione può essere applicata ed utilizzare un sistema

di orchestrazione SOAR per decidere quali azioni possono essere intraprese in base ai risultati dell'analisi fatta dalla AI.
Quando si riceve un nuovo rilevamento, l'intelligenza artificiale analizza la segnalazione per determinare se si tratta di un vero o di un falso positivo e fornisce un livello di confidenza per la sua valutazione, fornendo indicazioni relative al fatto che il rilevamento debba essere chiuso o affidato ad un analista umano. Le valutazioni dell'AI possono essere utilizzate come parametro all'interno dei processi decisionali del sistema di orchestration per notificare automaticamente agli analisti quando iniziare un'analisi o un'indagine. Infine, l'intelligenza artificiale genera una spiegazione che riassume i rilevamenti e relative raccomandazioni.



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/).*
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.
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.
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***)
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.
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 e internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; • facilitare la risposta a 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.
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 azioni 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)*
CSIRT (Computer Security Incident Response Team)	Struttura sostanzialmente simile ad un *CERT.*
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 crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.

Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
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.
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…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.

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.

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).
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.
FIDO2	Meccanismo di autenticazione avanzata che standardizza l'uso dei dispositivi di autenticazione per l'accesso ai servizi online, sia in ambiente mobile che desktop.
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 e 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 e operatore telefonico.
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.
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 ed 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.

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)	vedi ***Hit & Run***
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.
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.

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.
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.

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.
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 2024 – 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.

Luca Bechelli, Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali e internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione e al project management per attività di system integration. 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 collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Membro del Consiglio Direttivo del Clusit dal 2007 al 2018, è membro del Comitato Scientifico Clusit, con delega su Tecnologie e Compliance. Svolge attività di divulgazione su tematiche di sicurezza IT, mediante la partecipazione a convegni, la pubblicazione di articoli su testate generaliste o di settore e la partecipazione a gruppi di lavoro.

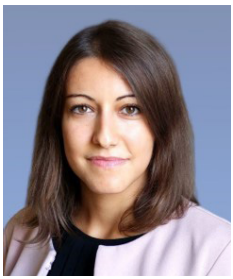
Giancarlo Butti, ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente ESG(*) e Inclusion del Comitato Scientifico del CLUSIT. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. 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, Universita 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 28 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 30 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di ACFE, di DFA e del BCI, 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 IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, CBCI, AMBCI.
(*) Già ricercatore nell'ambito delle energie rinnovabili (UNESCO - International directory of new and renewable energy information sources and research centers, 1986).

Stefano Castelluccio, nel 1994 ha conseguito la laurea specialistica in Ingegneria, Magna Cum laude, presso l'Università degli Studi di Parma. Dal 1995 è iscritto all'Albo degli Ingegneri di Parma. Nel 1997 ha pubblicato l'articolo "A real-time oriented system for vehicle detection" (Journal of Systems Architecture, vol. 43, n. 1-5, marzo 1997, Elsevier Science). Dal 1995 al 2001 ha lavorato prima come system engineering, poi come product manager, per SKG Group S.p.A. (Automotive Electronics, Ultra-high Vacuum measurement devices). Dal 2001 è entrato nel mondo ICT, iniziando come Senior Project Manager presso Oracle Corp. (Business Intelligence e Data Warehousing). Dal 2005 al 2008 ha lavorato come Business Unit Manager (Infrastructure and Security Solutions Division) per Kelyan S.p.A. – Franco Bernabè Group. Nel 2005 ha conseguito un Master in Sicurezza Informatica presso l'Università degli Studi di Bologna. Nel 2002 ha iniziato un'attività parallela come consulente professionista e temporary manager, e dal 2009 al 2014 è diventata un lavoro a tempo pieno, con contratti di 2 o 3 anni come Project/Program Manager, Temporary CIO/CTO, ICT Governance Consultant e Board Consultant. Nel 2019 ha ottenuto le certificazioni ITIL 4 Foundation, ISO/IEC 27001 Foundation e PRINCE 2 Foundation. Da novembre 2019 è registrato come Innovation Manager ufficiale presso il Ministero dello Sviluppo Economico. Nel 2014 è entrato in CAST Software come Senior Solution Delivery Consultant, iniziando a occuparsi di Software Intelligence e SDLC Management. Dal 2022 ha assunto il ruolo di Solution Design Manager.

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 a 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 e 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.



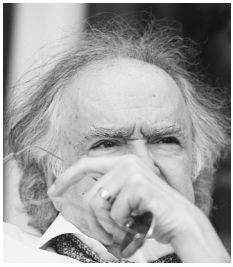
Giorgia Dragoni, si è laureata nel 2014 in Ingegneria Gestionale al Politecnico di Milano e nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection e dei Big Data Analytics e Direttore dell'Osservatorio Digital Identity. Nel 2022 ha conseguito l'Executive Master in Management presso la Polimi GSoM. È membro del Comitato Scientifico del Clusit e delle Women for Security.

Gabriele Faggioli, legale, è amministratore delegato di Digital360 e di Partners4Innovation, Presidente del Clusit e Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano. Gabriele è inoltre Adjunct Professor del MIP – Politecnico di Milano ed è stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amministrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui: "I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti con i cloud" (Franco Angeli), "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre a innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

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 Specialità Polizia Postale e delle Comunicazioni dal 2006. Dopo 3 anni in forza al Compartimento Polizia Postale e delle Comunicazioni di Genova, dal 2009 è al Servizio Polizia Postale del Dipartimento della PS. Dal maggio 2012 ha ricoperto l'incarico di Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Dal luglio 2017 è nominato Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, a cui fanno riferimento il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC, la Sezione Cyber Terrorismo e la Sezione per il contrasto al Financial Cyber Crime. Dal gennaio 2022 è Direttore del Servizio Polizia Postale e delle Comunicazioni.

Chiara Gatti, giurista attiva nel mercato assicurativo dal 2012, riveste per UnipolSai Assicurazioni s.p.a. il ruolo di Responsabile della linea di sottoscrizione cyber risks. In possesso della certificazione Risk Management FERMA Rimap ® e membro della Clusit Community for Security con la quale ha collaborato per la stesura della 13esima pubblicazione "Rischio Digitale Innovazione e Resilienza" (Marzo 2022) e della 14esima edizione dal titolo "Supply chain security".

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 Direttivo 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 e 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.

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 a 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 scientifico 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 Scientifico di CLUSIT, del BCI Cyber Resilience Group e del Comitato Direttivo e Scientifico di ANRA, 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 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.

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.

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 e internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali e internazionali. 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. È inoltre membro del Comitato Scientifico di Clusit.

Pier Luigi Rotondo, è specialista tecnico per le soluzioni IBM Security di Threat Management. Ha contribuito a molti progetti 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. Per conto di IBM Italia scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia sul cybercrime nel settore finanziario, presentando i risultati IBM e le tendenze del mercato della cyber security. È membro del Comitato Scientifico del CLUSIT dal 2021.

Rodolfo Saccani, CTO in Libraesva, vive l'IT dal 1994. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della security, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicu-

rezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, siede nel board della European Hang-gliding and Paragliding Union, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero.

Sofia Scozzari, appassionata di tecnologia da sempre, ha oltre 30 anni di esperienza nell'IT e 16 nella Cyber Security. Ha maturato esperienze come System Administrator, ICT Consultant, Project Manager, Pre-sale, Cyber Security Consultant e Manager per principali realtà Italiane e multinazionali. Da 5 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 membro del Comitato Direttivo Clusit e di Women For Security. 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 delle pubblicazioni «Cybersecurity e IoT: come affrontare le sfide di un mondo connesso» (2022, Women For Security), «Blockchain & Distributed Ledger: aspetti di governance, security e compliance» (2019, CLUSIT) e «La Sicurezza dei Social Media» (2014, Oracle Community for Security). È infine speaker a eventi e convegni di Cyber Security, sia in Italia che in UAE, e trainer in materia di Cyber Security Awareness.

Claudio Telmon, consulente sui temi di rischio e sicurezza ICT. Membro del Comitato Direttivo di Clusit. Senior Partner di Partners4Innovation.

Anna Vaccarelli, è Dirigente Tecnologo del Consiglio Nazionale delle Ricerche; responsabile delle Relazioni esterne, media, comunicazione e marketing del Registro .it, gestito dall›Istituto di Informatica e Telematica del Cnr. Dal 2010 coordina e promuove un›azione di diffusione della cultura di internet nelle scuole, con laboratori dalle primarie alle secondarie di secondo grado attraverso la Ludoteca del Registro .it. È tra gli ideatori di Internet Festival e coordinatore del Comitato Esecutivo del Festival. Fa parte del Comitato Direttivo di Women for Security dal 2020 e del Comitato direttivo del Clusit. È stata docente in corsi di Cybersecurity, responsabile scientifico di progetti nazionali e internazionali, coautore di oltre 100 pubblicazioni scientifiche e tecniche.

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 e 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 e 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, e 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.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

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 19a edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (a Milano, Napoli, Roma, Cagliari, Catania e Verona), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing).
- I Gruppi di Lavoro della Clusit Community for Security.
- Il Rapporto Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012.
- 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 2023 i Security Summit sono stati oggetto di oltre **800 articoli e servizi su web, cartaceo, Radio e TV.**

L'edizione 2025

Il 2025 inizierà con una edizione tutta in presenza, dal **11 al 13 marzo, a Milano**.
Saremo in seguito: in **maggio** a **Napoli**, in **giugno** a **Roma**, in **settembre** a **Cagliari** e/o a **Catania**, in **ottobre** a **Verona** e in **novembre** chiuderemo l'anno con un **Security Summit Streaming Edition.** Continueranno inoltre gli **eventi Vertical**i, programmati il 28 maggio (**Energy & Utilities**), il 18 giugno (**Health Care**) e il 12 novembre (due eventi: **Manufacturing** e **Finance**).

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/

In collaborazione con

CROWDSTRIKE

Microsoft

SECURITY SUMMIT

www.securitysummit.it