RAPPORTO

Clusit

sulla Cybersecurity
in Italia e nel mondo

2025

SECURITY SUMMIT

Indice

ASTREA
Via Copernico, 38 - 20125 Milano

Prefazione

Scrivo per la prima volta la prefazione a questo Rapporto, al quale, da alcuni anni, do qualche modesto contributo come autore: in quel ruolo mi sono concentrata su alcuni aspetti e alcuni contenuti. Oggi ho l'opportunità di considerarlo da un punto di vista più ampio e globale e leggerlo come il frutto di una (felice) collaborazione innanzi tutto con i soci Clusit, ma anche con istituzioni, università, enti di ricerca e altre associazioni

È per me anche l'occasione per ringraziare, a nome di tutto il Clusit, Gabriele Faggioli, che per dieci anni ha condotto l'associazione, promuovendone le attività, la crescita e la visibilità e lasciandomi, quindi, una ricca e impegnativa eredità, che mi impegnerò al massimo nel gestire e far fruttare.

Il lavoro che c'è dietro la raccolta e la presentazione dei dati del Rapporto, benché le serie di dati si ripetano in buona parte di anno in anno, anche per favorire i confronti nelle serie storiche, non è meccanico. È sempre un lavoro critico, soprattutto nello sforzo di dare una corretta interpretazione ai dati, frutto di un confronto tra gli autori. In questi ultimi anni, in particolare, gli scenari nei quali la cybersecurity è coinvolta sono in evoluzione veloce. Le guerre in atto, per esempio, influenzano alcuni tipi di attacchi e bisogna saper leggere dove e in che misura. Analogamente, la cybersecurity stessa è in evoluzione rapida, sia per la diffusione dell'Intelligenza Artificiale, che sta cambiando gli schemi di attacco e di difesa, sia per la sempre maggiore "professionalità" dei cybercriminali, che usano tecniche sempre più sofisticate. Inoltre, il numero dei cybercriminali aumenta, grazie alle modalità "as a service", utilizzata per vendere gli attacchi da parte di cybergang più esperte a criminali con abilità anche medio-basse, aumentando così di molto la probabile platea di potenziali vittime.

Il numero di incidenti è costantemente in aumento, una tendenza che si registra sin dai primi anni della pubblicazione di questo Rapporto, ma negli ultimi anni la crescita è diventata sempre più veloce. Si fa sempre più urgente assumerne totale consapevolezza a livello di persone, di organizzazioni e di istituzioni.

In questo momento sembra che le nuove normative, che sono entrate e stanno entrando in vigore, come per esempio, la NIS2, abbiano effetti positivi. Le sanzioni previste spingono le organizzazioni e le aziende che vi sono soggette, ad adottare contromisure adeguate a prevenire o ridurre i rischi. In qualche settore, come ad esempio quello finanziario, stiamo assistendo a una riduzione del numero di incidenti: probabilmente un effetto dovuto all'obbligo di applicare queste norme e dotarsi

di adeguate difese. L'osservazione del fenomeno nei prossimi anni potrà confermare o meno questa lettura ed eventualmente confermarne l'efficacia nei diversi settori.

Pur auspicando questo effetto "benefico", siamo consapevoli che esso non costituisce e non costituirà da solo la soluzione al problema degli attacchi e degli incidenti. Il progredire della digitalizzazione e la sempre maggiore interconnessione tra ambienti "reali" e digitali (si pensi all'IoT) farà aumentare l'interesse dei cybercriminali verso dati e informazioni disponibili online e, parallelamente, dovranno aumentare gli sforzi per difenderli.

Oltre che dalle evoluzioni tecnologiche, però, le tecniche di difesa passano anche per lo sviluppo di una cultura della cybersecurity, che dovrebbe portare il management di ogni azienda od organizzazione a tenere al centro delle sue priorità la difesa e la prevenzione cibernetica. Altrettanto importante è lo sforzo per rendere consapevole ogni utente: gli adulti, che spesso non hanno familiarità con la tecnologia e, soprattutto, i ragazzi, intervenendo già nei percorsi scolastici (come anche il Clusit sta già facendo). Nel giro di pochi anni i ragazzi di oggi saranno lavoratori, che potranno portare con sé un bagaglio di conoscenze a vantaggio delle realtà nelle quali opereranno.

*** *** ***

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

Oltre 3.000 copie cartacee distribuite durante il 2024, più di 80.000 copie scaricate e più di 1.000 articoli, sono l'evidenza della rilevanza del rapporto CLUSIT, utilizzato come strumento di lavoro e di consultazione per le organizzazioni. Gli autori stessi del Rapporto sono persone di riferimento per i vari aspetti della cybersecurity. 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

Anna Vaccarelli
Presidente CLUSIT

Introduzione al Rapporto

Dall'analisi dei dati emerge che, oltre agli impatti causati dal cybercrime e dalle "normali" attività di intelligence economica che osserviamo da anni, dal 2022, con l'inizio del conflitto in Ucraina, siamo entrati in una nuova fase di "guerra cibernetica diffusa", che si conferma anche nel 2024.

A questa dinamica di fondo nel 2024 si sono aggiunte nuove problematiche, sia derivanti dalla diffusione dell'AI generativa (utilizzata dagli attaccanti come "moltiplicatore di forza"), che dalle aumentate tensioni (a livello socioeconomico e geopolitico), che hanno riportato in auge forme di antagonismo digitale, principalmente realizzate tramite attacchi DDoS.
Oltre alle migliaia di attacchi compiuti da cybercriminali e gruppi state-sponsored, nel 2024 anche una crescente quantità di sigle antagoniste hanno colpito un gran numero di organizzazioni e governi, alimentando un senso di incertezza sempre più diffuso. In alcuni casi, è ragionevole supporre che queste cellule di sedicenti *hacktivist* siano in realtà manovrate da agenzie governative e inquadrate in più ampie attività di guerra psicologica, disinformazione e sabotaggio.

In questo scenario sempre più complesso, il nostro Paese risulta ancora tra i più colpiti, come dimostra il significativo numero di incidenti subiti nel 2024. Fin dal 2022 abbiamo scritto "l'Italia è nel mirino", situazione confermata anche nel 2023, e osservando i dati del 2024 possiamo concludere che il nostro Paese rappresenta un bersaglio preferenziale, con una crescita degli incidenti del 15% rispetto al 2023 (significativa, ma fortunatamente inferiore rispetto alla crescita del 27% a livello globale).

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

Ci siamo avvalsi anche in questa edizione dei dati relativi agli attacchi in Italia rilevati dal **Security Operations Center (SOC) di FASTWEB**.

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 del 2024.

Presentiamo a questo punto l'abituale **capitolo dedicato al settore FINANCE**, con un'analisi sul Cyber-crime nel settore finanziario in Europa, a cura di IBM.

Abbiamo poi inserito un capitoletto dedicato all'**Intelligenza Artificiale**, con due articoli:

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

Segue un approfondimento sulla **Cybersecurity in Sanità: incidenti in crescita e nuove misure di protezione e sanzioni con NIS2**, realizzato dalle Women for Security**.**

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

Pubblichiamo quindi un capitolo realizzato dalla **Community For Security su "CyberFutures, come sarà il nostro lavoro nel 2035?"**

Questi sono infine i temi trattati nella sezione FOCUS ON:

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

Analisi dei principali incidenti cyber noti del 2024 a livello globale

Ancora un record di incidenti cyber in Italia

In questa prima sezione del Rapporto CLUSIT 2025, giunto ormai al suo tredicesimo anno di pubblicazione, analizziamo i più gravi incidenti cyber noti avvenuti nel 2024 a livello globale (Italia inclusa) e li confrontiamo con l'analisi dei 4 anni precedenti.
Dal punto di vista quantitativo, negli ultimi 5 anni il numero degli incidenti rilevati è cresciuto sensibilmente, mostrando una tendenza inequivocabile, tanto che la media mensile a livello globale è passata dai 156 del 2020 ai 295 del 2024.

In percentuale, nel 2024 la crescita anno su anno degli incidenti rilevati da fonti pubbliche è stata del 27,4% (da 2.779 a 3.541). Oltre ad osservare una crescita costante della frequenza degli incidenti, la situazione si è evoluta in senso peggiorativo anche dal punto di vista delle loro conseguenze. Nel periodo di cinque anni considerato, la nostra valutazione della Severity media (indice di gravità) degli incidenti rilevati è cresciuta anno dopo anno, il che rappresenta un ulteriore moltiplicatore dei danni.
Come già nel 2023, nel 2024 gli incidenti classificati come "critici" o "gravi" hanno rappresentato circa l'80% del totale (erano il 50% nel 2020), anche se nel 2024 la percetuale di attacchi "critical" è diminuita, mentre è aumentata quella degli attacchi con severity "high", in particolare per la diminuzione (in media) degli impatti derivanti da attacchi con finalità cybercriminali

Considerato che i dati rilevati riguardano solo attacchi andati a buon fine (cioè effettivamente avvenuti e confermati) e divenuti di dominio pubblico, la loro analisi conferma la nostra convinzione che, rispetto al periodo 2011-2019, negli ultimi 5 anni sia avvenuto un cambiamento drastico nello scenario globale della cyber-insicurezza, al quale, visti gli esiti, non è evidentemente corrisposto un incremento sufficiente della consapevolezza, delle risorse allocate e 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".
A tre anni di distanza, i rischi legati alla crescita delle minacce cibernetiche, oltre ad essere ormai trasversali rispetto a tutti i livelli dell'economia e della società, sono diventati un problema sistemico, e rappresentano una crisi di portata globale, che va ben al di là dei danni crescenti subiti dalle singole vittime.

Riassumendo le nostre considerazioni sullo scenario che emerge dai dati potremmo affermare che, oltre agli impatti causati dal cybercrime e dalle "normali" attività di

intelligence economica che osserviamo già da diversi anni, dal 2022, con l'inizio del conflitto in Ucraina, siamo entrati in una nuova fase di "guerra cibernetica diffusa", dinamica che si conferma anche nel 2024.

A questo scenario di fondo nel 2024 si sono aggiunte nuove problematiche, sia derivanti dalla diffusione dell'AI generativa (utilizzata dagli attaccanti come "moltiplicatore di forza"), che dalle aumentate tensioni (a livello socioeconomico e geopolitico), che hanno riportato in auge forme di antagonismo digitale, principalmente realizzate tramite attacchi DDoS.
Oltre alle migliaia di attacchi compiuti da cybercriminali e gruppi state-sponsored, nel 2024 anche una crescente quantità di sigle antagoniste hanno colpito un gran numero di organizzazioni e governi, contribuendo ad alimentare un senso di incertezza sempre più diffuso. In alcuni casi, è ragionevole supporre che queste cellule di sedicenti hacktivist siano in realtà manovrate da agenzie governative ed inquadrate in più ampie attività di guerra psicologica, disinformazione e sabotaggio.

In questo scenario sempre più complesso, il nostro Paese risulta ancora tra i più colpiti, come dimostra il significativo numero di incidenti subiti nel 2024. Fin dal 2022 abbiamo scritto "l'Italia è nel mirino", situazione poi confermata anche nel 2023, ed osservando i dati del 2024 possiamo concludere che il nostro Paese rappresenta ormai un bersaglio preferenziale, con una crescita degli incidenti del 15% rispetto al 2023 (significativa, ma fortunatamente inferiore rispetto alla crescita del 27% a livello globale). Questo peggioramento del dato deve comunque far riflettere, anche considerando che l'Italia, pur rappresentando solo lo 0,7% della popolazione ed l'1,8% del PIL mondiale, nel 2024 ha subito il 10% degli attacchi registrati a livello globale, tenendo presente, a titolo di confronto, che la Francia è al 4% e la Germania al 3%, così come il Regno Unito. Si tratta di una sproporzione evidente, non giustificabile solo come un bias insito nei nostri dati, che merita certamente attenzione.
Per questa ragione, nel capitolo specifico sull'Italia abbiamo svolto alcune considerazioni puntuali su quanto osservato, nella speranza di contribuire ad un incremento della consapevolezza nazionale e 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 sempre maggiori.

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

Analisi dei principali incidenti cyber noti a livello globale

In questa sezione offriamo una panoramica degli incidenti di sicurezza di pubblico dominio più significativi avvenuti a livello globale nel 2024, confrontandoli con i dati raccolti nei 4 anni precedenti.

+27%
è la crescita degli incidenti dal 2023 al 2024

Lo studio si basa sull'analisi di incidenti cyber attacchi noti, andati a buon fine e di particolare gravità, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle vittime (*vedi Appendice Metodologica*).

Nel periodo in esame, tra gennaio 2020 e dicembre 2024, abbiamo censito un totale di 12.732 incidenti, distribuiti come segue.

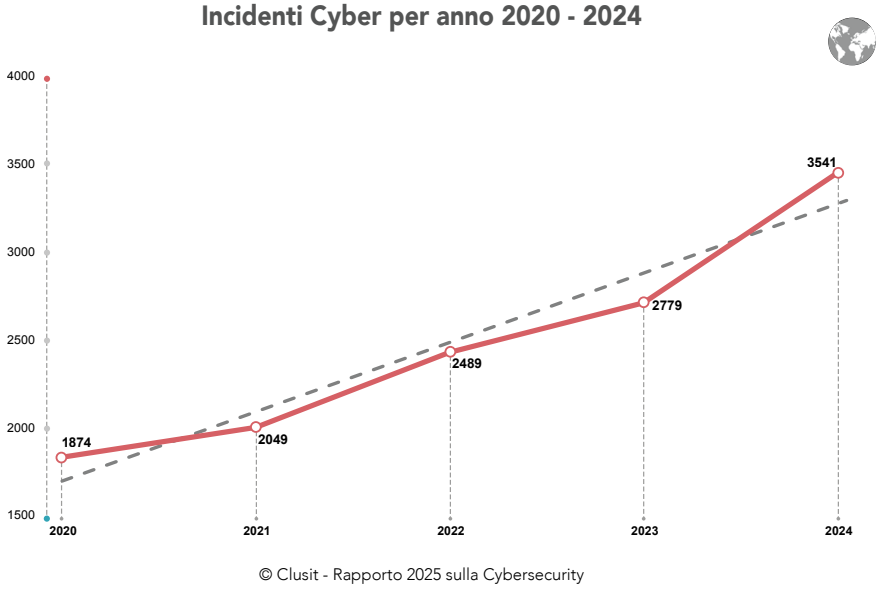


Fig. 1 - Andamento degli incidenti cyber nel periodo 2020-2024

Nell'ultimo anno abbiamo registrato 3.541 incidenti, il numero maggiore di sempre, ed è interessante notare come la realtà stia superando le previsioni indicate in grigio dalla linea di tendenza.

A conferma di una costante recrudescenza dello scenario degli incidenti, gli eventi degli ultimi cinque anni (2020 - 2024) sono più della metà (56%) degli incidenti da noi classificati in totale dal 2011.

56%

56% è il numero degli incidenti degli ultimi 5 anni rispetto al totale registrato dal 2011

Rispetto ai 2.779 incidenti del 2023, nel 2024 si manifesta una crescita del 27%. Rispetto ai 1.667 incidenti censiti nel 2019, ultimo anno pre-pandemico, pre-remote working, antecedente alla forte spinta alla digitalizzazione, in uno scenario ove mancava la presenza pervasiva dell'AI a cui assistiamo oggi, la crescita è addirittura del 112%.

Anche la media mensile è in crescita vertiginosa: dai 139 incidenti/mese del 2019 si passa ai 232 del 2023 e ai 295 del 2024.

A differenza del 2023, il livello di distribuzione mensile è abbastanza uniforme e sostenuto durante tutto l'anno, con un picco in ottobre-novembre, come si evince dal grafico seguente.

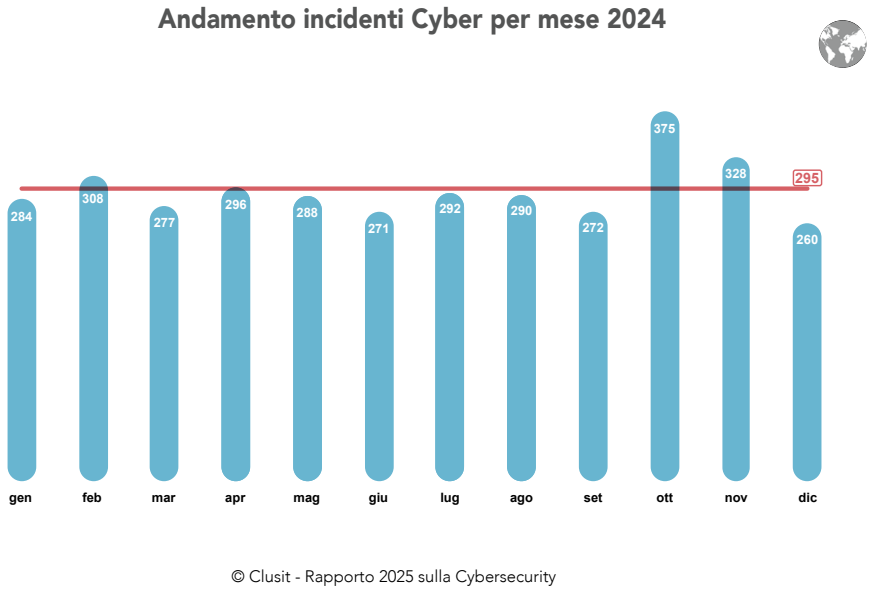


Fig. 2 - Numero di incidenti cyber per mese nel mondo nel 2024

Distribuzione degli attaccanti per tipologia

Il Cybercrime si conferma ancora una volta la motivazione principale degli incidenti, con una crescita che non accenna a diminuire. Nel 2024, infatti, la criminalità cyber è responsabile di quasi 9 attacchi su 10 (86% del totale +3 punti percentuali rispetto al 2023), tornando ai livelli record del 2021. Questa tendenza dimostra quanto anche la criminalità organizzata stia puntando sempre più sul cyberspazio: la resa dei reati informatici ha ormai superato quella di molte attività criminali tradizionali, grazie anche ai modelli "*as-a-Service*" che rendono il cybercrimine accessibile persino a chi non possiede competenze tecniche.

9 su 10
gli incidenti nel mondo di matrice cybercriminale

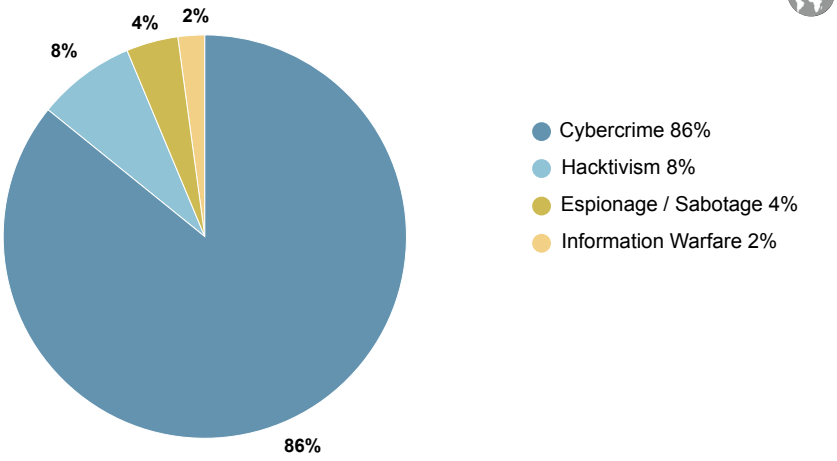


Fig. 3 - Distribuzione percentuale degli attaccanti nel 2024

Il confronto della distribuzione degli attaccanti nel periodo dal 2020 al 2024 (**Fig. 4**) evidenzia in modo chiaro che il *Cybercrime* continua a rimanere la motivazione principale degli incidenti, con un andamento regolarmente in crescita negli anni (+31% nel 2024 rispetto all'anno precedente).

+31%
è la crescita degli incidenti causati dal Cybercrime nel 2024

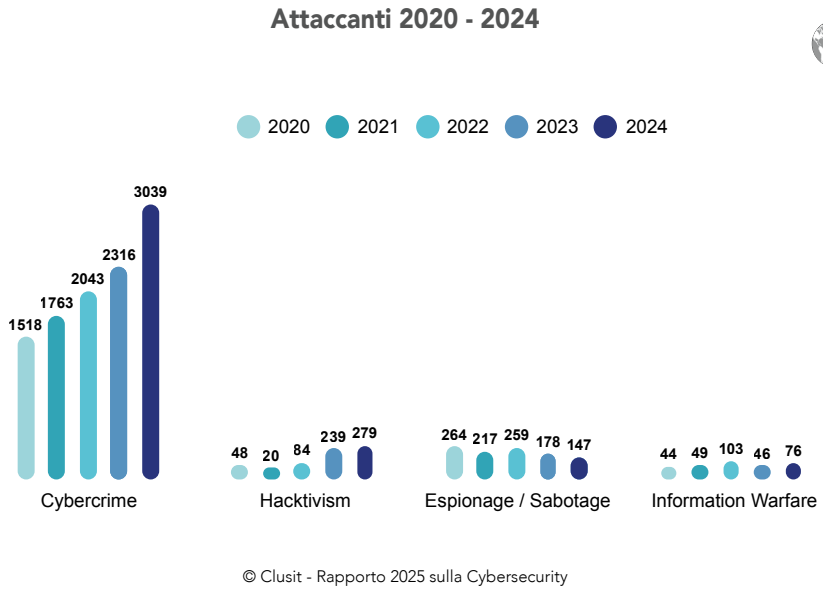


Fig. 4 - Distribuzione degli attaccanti dal 2020 al 2024

Questo andamento conferma quanto già affermato nel Rapporto dello scorso anno: si verifica una commistione, quando non addirittura integrazione, tra criminalità "off-line" e criminalità "on-line" che porta a reinvestire in questo business i proventi delle attività precedenti per aumentare le risorse a disposizione di chi attacca, a fronte di ricavi sempre maggiori.

Non solo: questa crescita mette in ombra il fenomeno comunque crescente dell'Hacktivism (16 punti percentuali in più rispetto all'anno precedente) e delle operazioni note di Information Warfare, che aumentano fino quasi a raddoppiare.

2x

raddoppiano le operazioni note di Information Warfare rispetto al 2023

Solo gli incidenti con finalità di Espionage / Sabotage sono in diminuzione, di quasi 20 punti percentuali.

Distribuzione delle vittime per categoria

L'analisi delle vittime del 2024 (**Fig. 5**) evidenzia che quasi la metà degli incidenti (44%) si concentra sulle prime tre categorie della nostra classifica: *Multiple Targets* (18% del totale), *Gov / Mil / LE* ed *Healthcare* (13% ciascuno). Se gli attacchi indiscriminati di "pesca a strascico" si confermano tra i privilegiati del cybercrime (ed il numero elevato dei successi può essere spiegato da una considerevolmente più elevata intensità di questa tipologia di campagne), gli altri due settori rappresentano obiettivi particolarmente appetibili, per il ruolo strategico che ricoprono e per la rilevanza dei dati trattati.

44%
è la percentuale degli incidenti che colpiscono Multiple targets, Gov / Mil / LE ed Healthcare

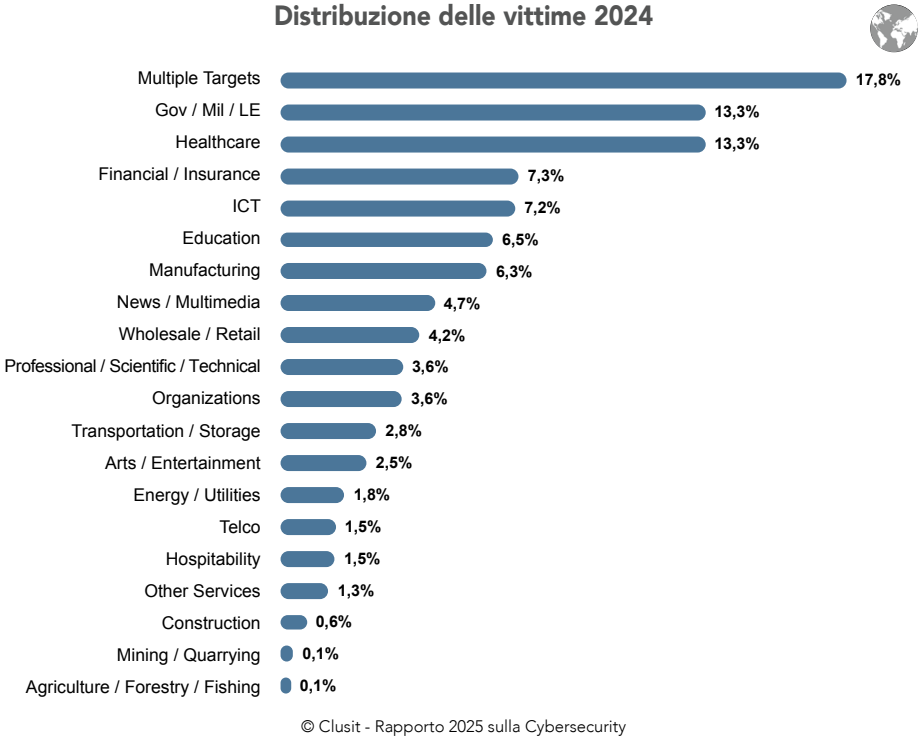


Fig. 5 - Distribuzione della tipologia di vittime nel 2024

45%
è la crescita degli incidenti verso il settore Gov / Mil / LE nel 2024

18,9%
è la crescita degli incidenti verso il settore Healthcare nel 2024

A conferma di ciò, nel confronto con gli anni precedenti (**Fig. 6**) emerge quanto i tre ambiti abbiano subito una costante crescita: il settore Gov / Mil / LE aumenta del 45% rispetto al 2023, Healthcare ha un incremento del 18,9%, mentre Multiple Target cresce di poco più di 17 punti percentuali.

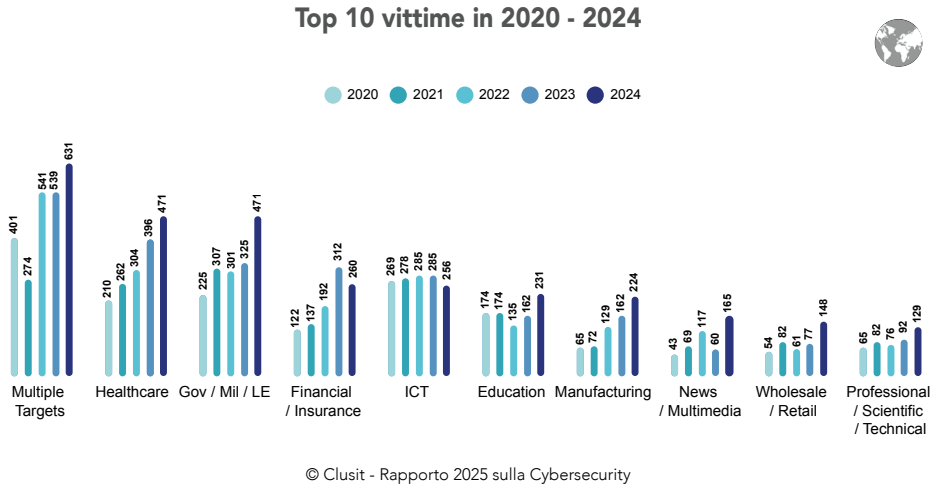


Fig. 6 - Distribuzione delle prime 10 tipologie di vittime dal 2020 al 2024

16 p. p.
è la riduzione degli incidenti verso il settore Financial / Insurance nel 2024

Cala, dopo un tasso di crescita costante dal 2019 al 2023, il settore *Financial/Insurance* (-16 punti percentuali rispetto all'anno scorso): il dato può spiegarsi tanto con un primo effetto di una rinnovata regolamentazione sulla resilienza operativa digitale nel settore (es: almeno per quanto riguarda l'Europa, il Regolamento DORA), quanto ad un maggiore interesse del crimine informatico sul realizzare economie di scala mediante campagne di attacchi trasversali ai settori o verso un numero maggiore di vittime che esprimono una minore capacità di difesa.

Il settore *ICT* è, insieme al precedente, l'altro unico caso in cui il numero di incidenti si riduce (-10 punti percentuali), dopo una fase di stabilità nei due anni precedenti: questo caso pare proprio rappresentare l'effetto concreto di un percorso progressivo

di irrobustimento delle capacità di difesa del settore, con effetti graduali facilmente osservabili.

Focalizzandoci sul resto della "top 10" delle vittime, il dato rilevante è che la crescita si attesta in questi settori praticamente sempre intorno al 40% o oltre: *Education* +43%, *Manufacturing* +38% e *Professional / Scientific / Technical* +40%, con picchi ancora più drammatici nei settori News / Multimedia (+175%, su cui si rimanda all'approfondimento "Il caso News/Multimedia") che dopo un anno di assenza rientra nella parte alta della classifica, e *holesale / Retail*, che con una crescita del 92% sale di una posizione rispetto all'anno precedente.

92%
è la crescita degli incidenti verso il settore Wholesale / Retail nel 2024

Buone notizie, se così si può dire, per il settore *Transportation / Storage*, il quale, dopo la permanenza tra i primi 10 settori colpiti nel 2023, torna a scendere nel 2024 e si attesta al 12° posto.

Distribuzione generale delle vittime per area geografica

La distribuzione geografica delle vittime (**Fig. 7**) evidenzia come nel 2024 oltre i due terzi degli incidenti (65%) abbiano colpito i territori americano ed europeo.

2 su 3
incidenti avvengono nel continente Americano e Europeo

Questo dato non sorprende, considerando che in entrambi i continenti le normative sulla divulgazione degli incidenti informatici sono in vigore da più tempo, garantendo una maggiore trasparenza nella segnalazione. In Europa, in particolare, oltre al GDPR (che ha contribuito sensibilmente a favorire la disclosure dei c.d. Data Breach), nell'ultimo periodo si sono intensificate ed estese normative generali e settoriali che impongono adempimenti sulla notifica degli incidenti, come il Regolamento DORA e "le" Direttive NIS 1 e 2, per non citare il PSNC in Italia e norme equivalenti negli altri paesi UE. L'effetto è evidente: mentre il numero di attacchi noti nel continente americano rimane relativamente stabile da anni, l'Europa, dopo anni di crescita graduale, registra nel 2024 un picco significativo (+67%), come è possibile riscontrare in **Fig. 8**.

+67%
è la crescita degli incidenti rilevanti in Europa

Anche gli attacchi verso località multiple tornano ad aumentare, invertendo la tendenza al ribasso osservata nel 2023. Inoltre, per la prima volta, si registra un'impennata di attacchi verso l'Oceania (+228%), spiegabile sia con un'attenzione crescente

da parte degli threat actors verso questa regione, sia (come in Europa) per recenti aggiornamenti delle normative nei Paesi della regione in materia di cybersecurity.

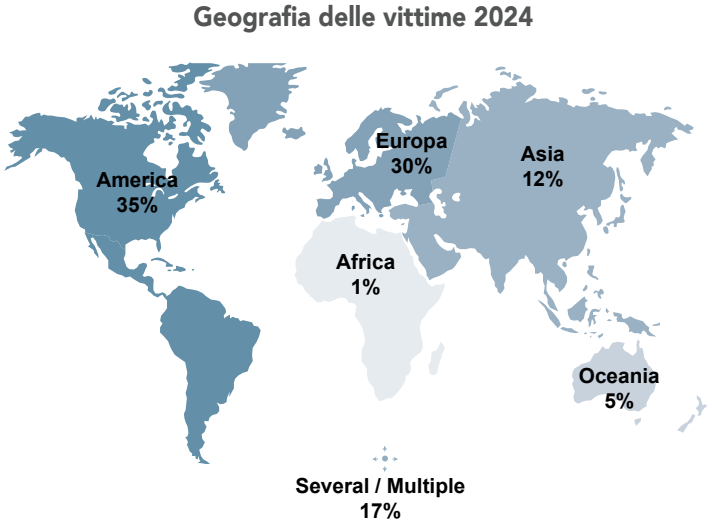


Fig. 7 - Distribuzione geografica delle vittime in percentuale per il 2024

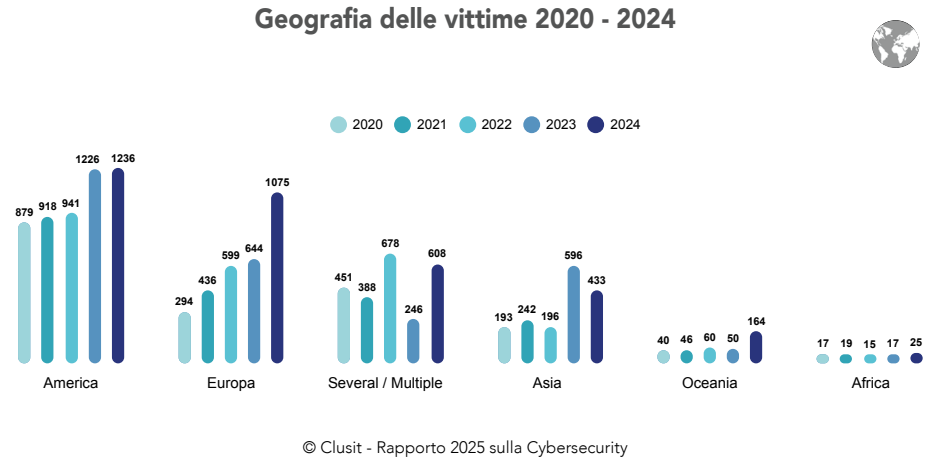


Fig. 8 - Distribuzione geografica della tipologia delle vittime nel periodo 2020-24

È interessante osservare come le aree geografiche dove si collocano i Paesi più sviluppati, che hanno un orientamento molto forte rispetto a politiche di *cyber sovereignty*, presentino ancora oggi un tasso molto basso di incidenti pubblicamente noti, che non possiamo spiegare solo con una minore incidenza di questo fenomeno.
Alcuni di questi Paesi, come noto, applicano forme di censura sulla disclosure pubblica di informazioni pertinenti a vulnerabilità, attacchi e incidenti subiti da soggetti pubblici e privati, la cui effettiva efficacia a limitarne volumi e/o impatti è ancora tutta da dimostrare. D'altro canto, un controllo più rigido sui confini della rete e un monitoraggio stretto all'interno possono oggettivamente rendere più difficili gli attacchi dei cybercriminali e le operazioni con matrice attivista. Seguire l'evoluzione di questi fenomeni nei prossimi anni permetterà anche di comprendere al meglio l'effetto delle scelte strategiche nazionali sullo scenario globale della cybersecurity.

1 su 3
incidente è basato su malware

Distribuzione delle tecniche di attacco

Nel 2024, i cybercriminali continuano a puntare su tecniche consolidate e industrializzabili: i Malware sono infatti responsabili di oltre un terzo degli incidenti, mentre lo sfruttamento delle vulnerabilità, sia note che sconosciute (zero-day), incidono per il 15% sul totale (**Fig. 9**).

I codici malevoli, soprattutto i ransomware, pur registrando un leggero calo percentuale rispetto al 2023 (-4pp), mostrano una crescita dell'11% in termini assoluti (+114 incidenti), confermando la loro affidabilità nelle strategie cybercriminali (**Fig. 10**).

+33%
è la crescita anno su anno degli attacchi di Phishing e Ingegneria Sociale

Si registra inoltre un aumento significativo di incidenti causati da attacchi DDoS (+36%) portando questa categoria all'8% del totale, Phishing / Social Engineering (+33%, attestandosi all'8% rispetto al totale) e Identity Theft / Account Cracking (al 6% del totale, con una variazione percentuale del +135%) che evidenziano la progressiva diversificazione delle strategie di attacco – e della relativa efficacia nel trasformarsi con successo in incidenti – con una combinazione tra tecniche tradizionali e metodi più sofisticati.

Per un quarto degli incidenti non è stato possibile conoscere la tecnica utilizzata, in quanto non resa nota (*undisclosed*); questi casi, dopo un periodo di flessione, nell'ultimo anno sono tornati a crescere del 56%.

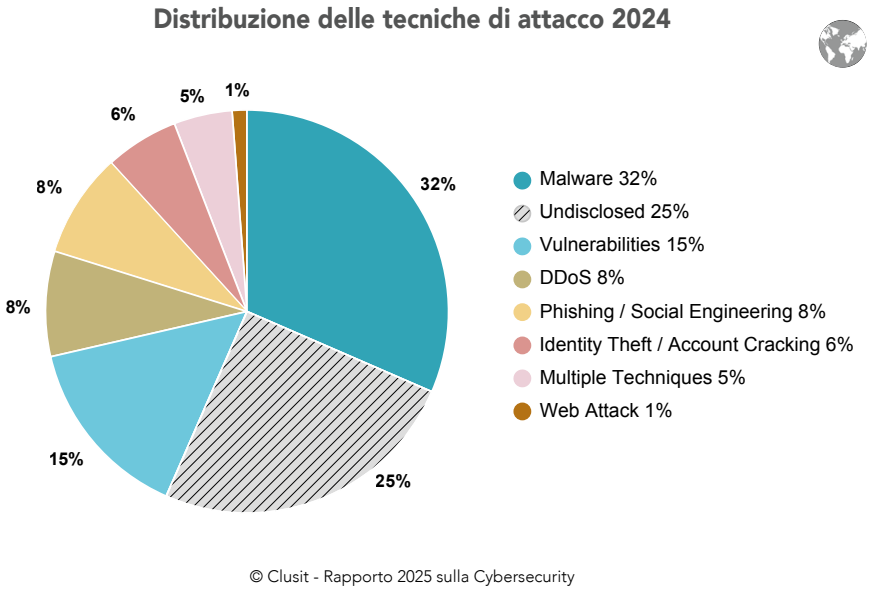


Fig. 9 - Distribuzione delle tecniche di attacco nel 2024

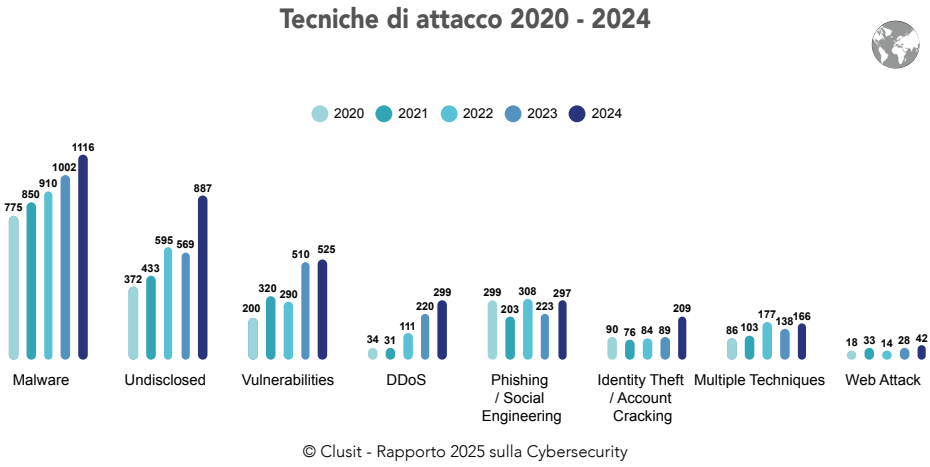


Fig. 10 - Distribuzione delle tecniche di attacco nel periodo 2020-24

Analisi della "Severity" degli incidenti

L'analisi della *severity* si pone l'obiettivo di mettere in evidenza gli impatti degli incidenti, che non sempre sono proporzionali al numero di attacchi né possono essere dedotti esclusivamente dal tipo di vittima o dalla tecnica utilizzata.
Sin dal 2021 (**Fig. 11**), si è consolidata una tendenza preoccupante, con un aumento costante degli incidenti con impatti gravi o gravissimi, che nel 2023 hanno raggiunto circa l'80% del totale, anche in considerazione della natura del campione a cui si riferisce il ns. Rapporto.

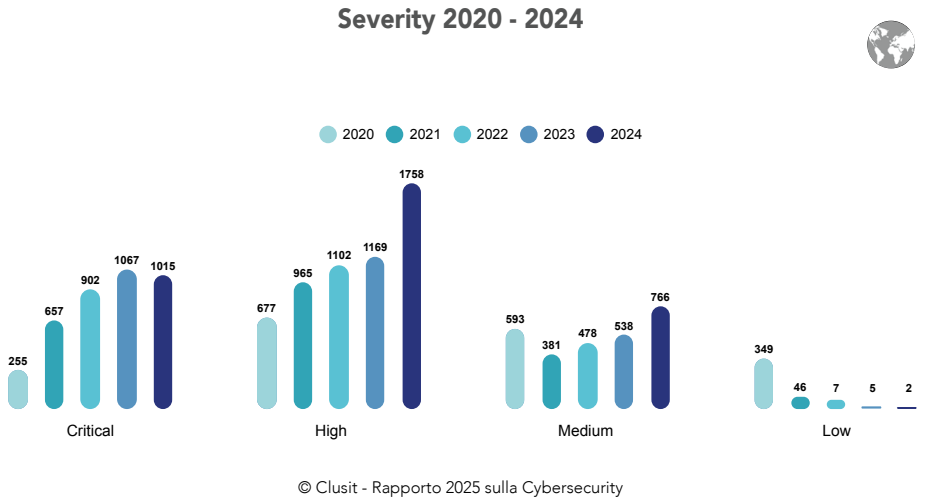


Fig. 11 - Andamento della Severity degli incidenti nel periodo 2020-24

Anche nel 2024, questo trend viene confermato (**Fig. 12**), con un livello di severity importante (impatti Critical e High) che si attesta nuovamente al 79%.

Aumentano anche gli incidenti con severity Media (+42%), mentre gli impatti bassi sono ormai sostanzialmente scomparsi dal campione mondiale.

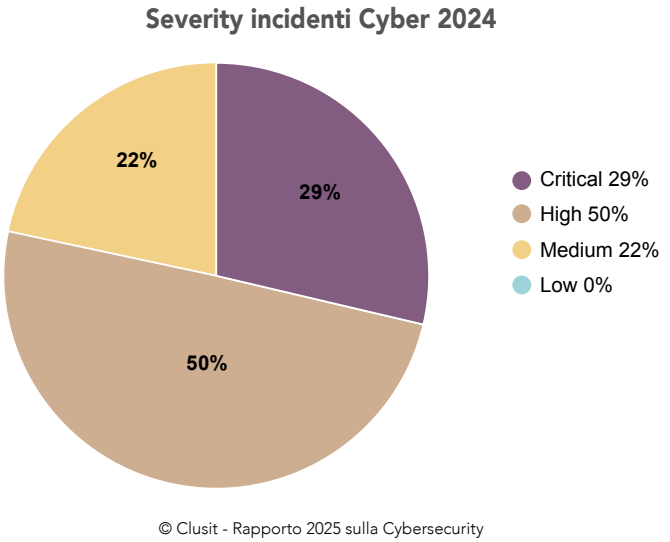


Fig. 12 - Distribuzione della Severity nel 2024

Severity per tipologia di attaccante

La severity per tipologia di attaccante mostra chiaramente quanto, indipendentemente dal numero degli incidenti, gli impatti si differenziano molto in base alla motivazione dell'attacco. Sebbene, infatti, il Cybercrime sia costantemente la categoria di attaccante più prolifica, sono *Espionage / Sabotage* ed *Information Warfare* a guadagnarsi il podio degli impatti, con un andamento pressoché costante negli ultimi due anni.

>6 su 10
attacchi di tipo Espionage/Sabotage e Information Warfare con severity massima (Critical)

Questo è particolarmente evidente dai grafici relativi al 2024 (**Fig. 13**) e 2023 (**Fig. 14**) dove entrambe le categorie mostrano severity critica in quasi il 70% dei casi.

Certamente i numerosi conflitti che hanno caratterizzato il 2024 (Russia – Ucraina, ma anche Israele – Palestina), giustificano il costante ricorso a queste tipologie di attacco.

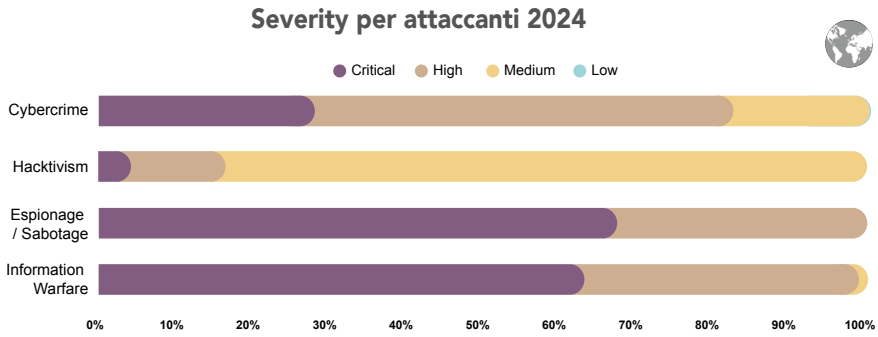


Fig. 13 - Distribuzione della Severity per attaccanti nel 2024

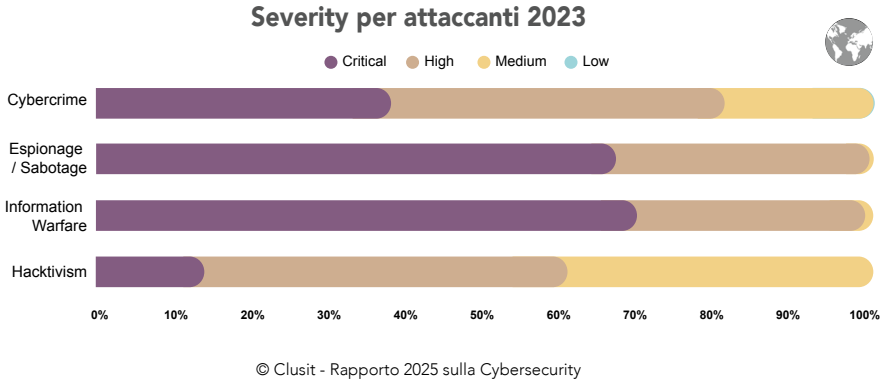


Fig. 14 - Distribuzione della Severity per attaccanti nel 2023

-10%
è la riduzione degli incidenti Cybercrime con severity massima (Critical)

Nel 2024 diminuisce invece l'impatto critico di *Cybercrime* (dal 40% al 30%), indice del fatto che all'aumento dei numeri non è corrisposto, almeno per il momento, anche un incremento di gravità delle conseguenze degli incidenti.

Anche l'impatto critico di *Hacktivism* si riduce, in maniera più sostenuta, e ciò è connaturato all'obiettivo di queste tipologie di attacco: devono essere *eclatanti* e *visibili*, non necessariamente portare a conseguenze dirette o indirette rilevanti per la specifica vittima.

Severity per tipologia di vittima

L'analisi della severity per tipologia di vittima evidenzia quanto sostanzialmente tutte siano soggette ad impatti variabili, ma quelli critici rappresentano sempre una quota che si aggira tra il 20% e il 40% nel 2024 (**Fig. 15**).

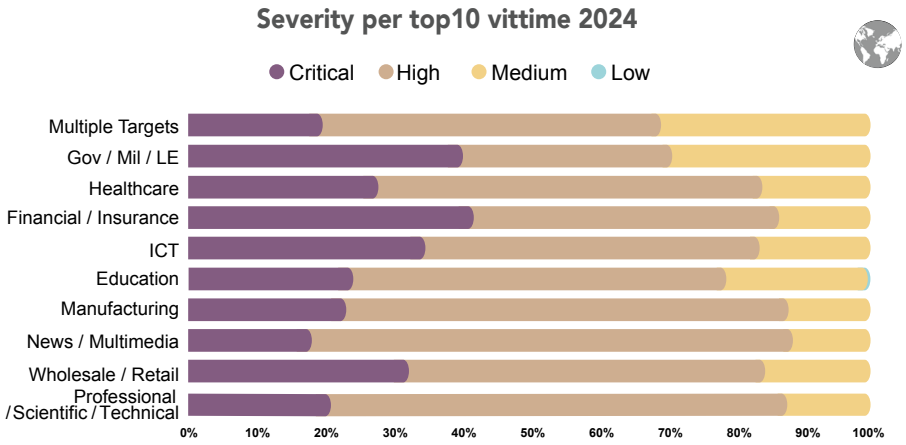


Fig. 15 - Distribuzione della Severity per prime 10 vittime nel 2024

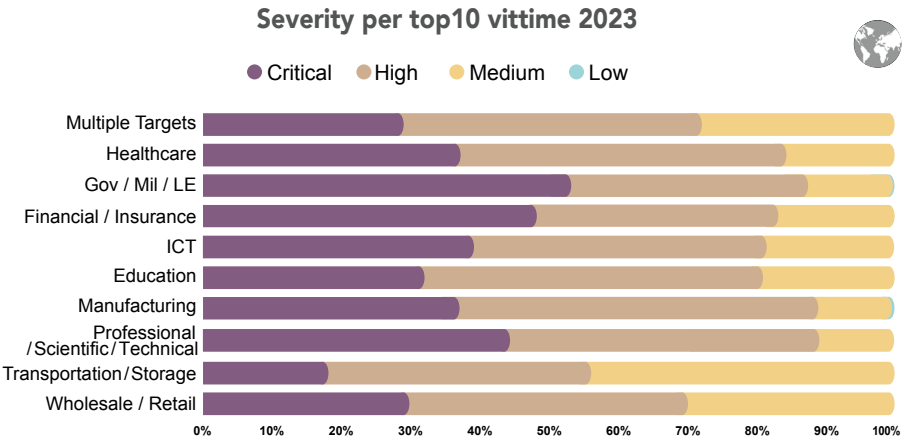


Fig. 16 - Distribuzione della Severity per prime 10 vittime 2023

Dal confronto con l'anno precedente (**Fig. 16**) si evince che sostanzialmente tutte le categorie di vittime subiscono impatti meno critici nel 2024, a fronte di impatti gravi ("high") costanti, quando non addirittura in aumento.

Crescono, anche se di poco, solo gli impatti critici del settore *Wholesale / Retail*, mentre *News / Multimedia* rientra nella Top 10 degli obiettivi, dopo essere stato soppiantato da *Transportation / Storage* nel 2023.

Severity per tecniche di attacco

L'analisi della severity in relazione alle tecniche di attacco mostra al contrario delle maggiori specificità rispetto alla correlazione degli incidenti con le vittime, a maggior ragione confrontando il dato 2024 (**Fig. 17**) con l'anno precedente (**Fig. 18**).

Gli incidenti di tipo *Multiple Techniques* sono al primo posto per severity *Critical*, e ciò è giustificato dal fatto che si tratta tipicamente di eventi causati da attacchi complessi, finalizzati a massimizzare il vantaggio per chi li perpetra (o il danno per il bersaglio).
Gli incidenti basati su *Malware* mantengono anno su anno una distribuzione di *severity* pressoché simile: in più del 35% dei casi l'impatto è di tipo *Critical*, a dimostrazione che questa tecnica resta una risorsa affidabile per i cybercriminali.
Considerando solo la severità *Critical*, la nostra classifica del 2024 per tipologia di incidenti fa seguire a *Malware* le categorie *Vulnerabilities* (in calo rispetto al 2023, quando aveva mostrato un notevole picco a causa dei numerosi e disastrosi zero-day sfruttati dai cybercriminali per operazioni malevole ad altissimo impatto), *Phishing/ Social Engineering* (la cui distribuzione della severity è pressoché costante rispetto all'anno precedente), *Web Attack* e *Identity theft / Account cracking*, che rappresenta forse una delle tecniche di attacco più longeve ed evergreen.

Discorso a parte invece per i *DDoS*, altra tecnica ormai rodata, adottata in larga misura soprattutto dai gruppi attivisti: a dispetto di un aumento del 36% nel numero di incidenti, nel 2024 diminuiscono in maniera decisa gli impatti gravi ("high") e gravissimi ("critical"), divenendo la categoria di tecniche con la maggiore quota di impatti medi.
Anche *Undisclosed* – per ovvi motivi – la consideriamo a parte rispetto alla nostra classifica.

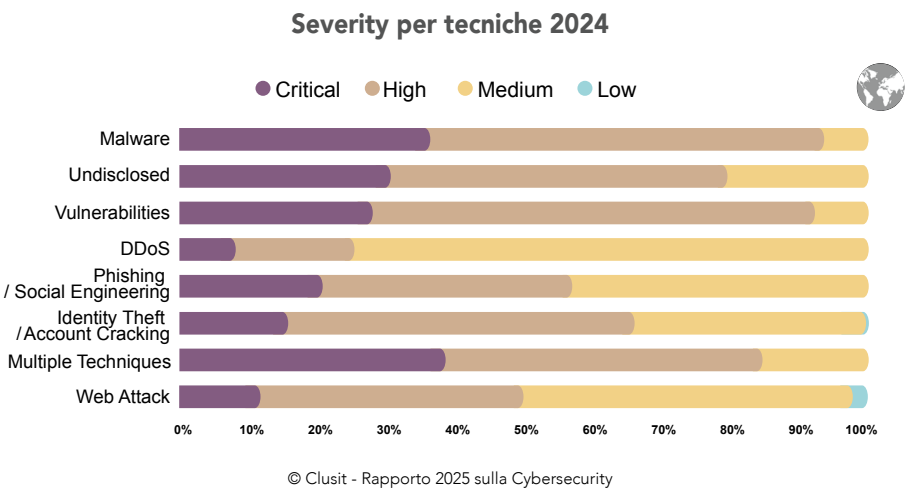


Fig. 17 - Distribuzione della Severity per tecniche di attacco nel 2024

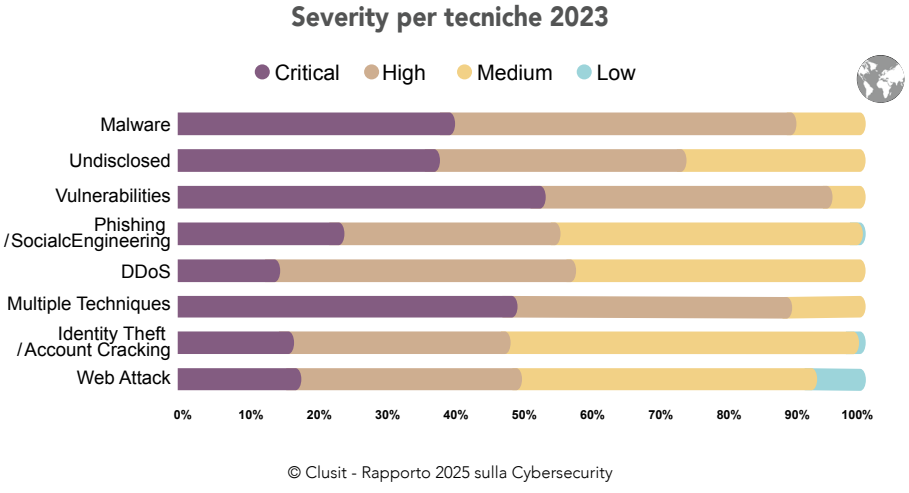


Fig. 18 - Distribuzione della Severity per tecniche di attacco nel 2023

Analisi degli incidenti alle organizzazioni governative e alle pubbliche amministrazioni

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

Tra il 2020 e il 2024 il campione ha incluso **1.393** incidenti noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Globalmente la crescita è più che lineare, ed al forte incremento registrato fra il 2022 e il 2023 è seguito un aumento ancora più significativo fra il 2023 e il 2024. Nell'arco dei cinque anni si è comunque passati dai 208 incidenti del 2020 ai 431 del 2024, con un incremento complessivo di oltre il 100% (**Fig. 19**).

+100%
è la crescita degli incidenti nel settore GOV dal 2020 a oggi

La distribuzione degli attaccanti (**Fig. 20**) mostra chiaramente l'ulteriore aumento del fenomeno Hacktivism, in crescita sin dal 2022: il numero di incidenti generato da questa categoria di attaccanti è cresciuto di oltre il 50% fra il 2023 e il 2024.

+50%
è la crescita degli incidenti di tipo Hacktivism nel settore GOV nell'ultimo anno

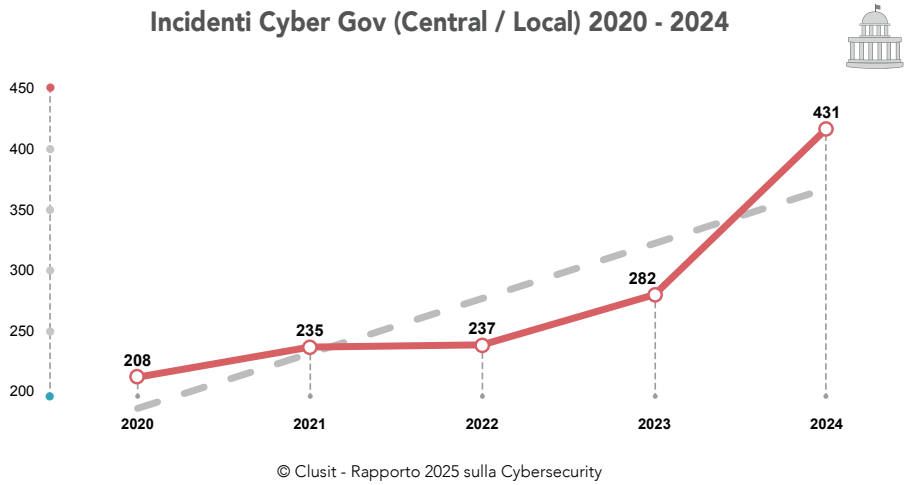


Fig. 19 - Incidenti al settore Gov (Central / Local) nel periodo 2020-2024

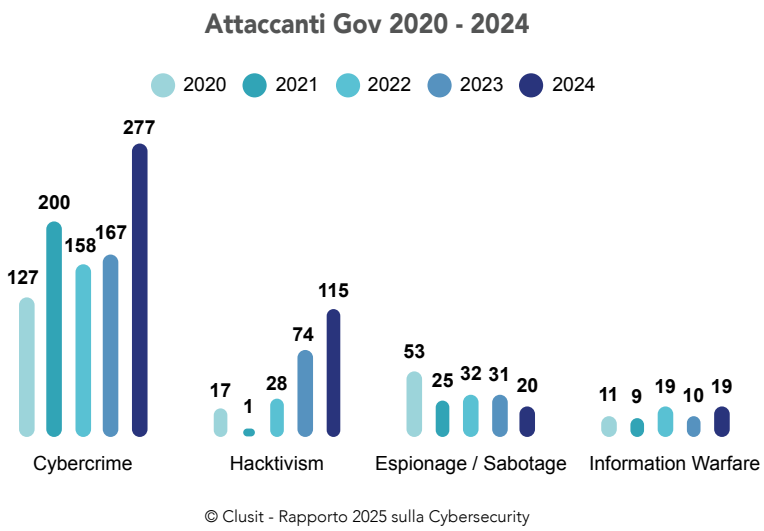


Fig. 20 - Distribuzione degli attaccanti per il settore Gov (Central / Local) nel periodo 2020-24

+90%
è la crescita degli incidenti in Europa nel settore GOV nell'ultimo anno

La distribuzione geografica delle vittime (Fig. 21) mostra che gli incidenti sono cresciuti prepotentemente in Europa, per via della vicinanza geografica e politica rispetto ai territori flagellati dai conflitti. Crescono anche, per il terzo anno di seguito, nel continente americano, soprattutto in Nord-America, e in Asia; inoltre, subiscono un brusco incremento in Oceania dopo anni di relativa calma.

2x
è la crescita degli incidenti DDOS nel settore GOV nell'ultimo anno

Per quanto riguarda le tecniche utilizzate (Fig. 22) notiamo che gli incidenti causati da *DDoS*, tipici dei fenomeni di attivismo, sono più che raddoppiati anche nell'ultimo anno, così come era già successo nell'anno precedente; quelli mediante *Malware* sono cresciuti del 50%, mentre sono rimasti sostanzialmente costanti tutti gli altri. Cresce molto, tuttavia, la quota di incidenti per cui le tecniche impiegate non sono state rese note, oltre il doppio rispetto all'anno precedente.

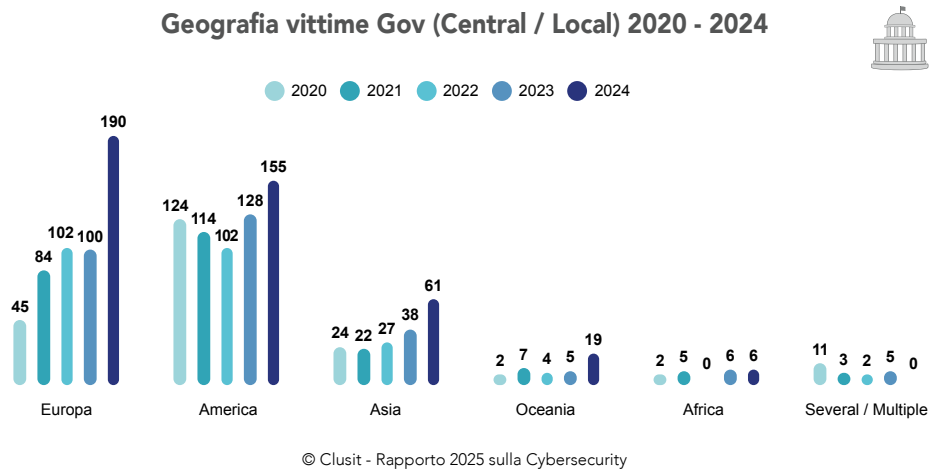


Fig. 21 - Distribuzione geografica delle vittime nel settore Gov (Central / Local) nel periodo 2020-24

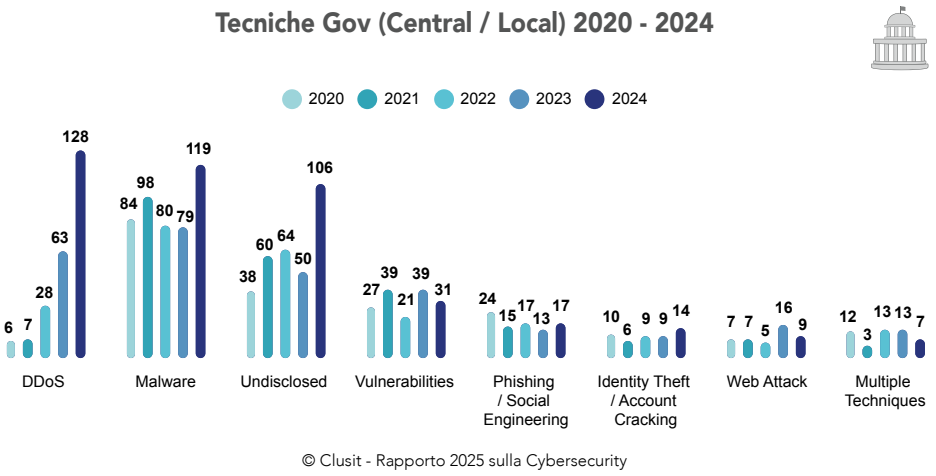


Fig. 22 - Distribuzione delle tecniche di attacco nel settore Gov (Central / Local) nel periodo 2020-24

Analisi degli incidenti in Italia

Tra il 2020 e il 2024 il campione ha incluso **973** incidenti noti di particolare gravità che hanno preso di mira realtà italiane. Di questi, ben 357, ovvero quasi il 39% del totale, sono avvenuti nell'ultimo anno in esame. Come si evince dal grafico (**Fig. 23**), il dato del 2024, sebbene registrando una lieve ulteriore crescita rispetto all'anno precedente, sembra riportarsi nella linea di tendenza degli ultimi anni: gli incidenti sono sì aumentati nel 2024 rispetto al 2023, ma con meno rilevanza di quanto fossero aumentati nei due anni precedenti.

39%
è la percentuale degli incidenti subiti in Italia nel 2024 rispetto al totale dal 2020

Il tasso di crescita degli incidenti in Italia nel 2024 (**Fig. 24**) si assesta al 15,2% rispetto all'anno precedente, inferiore rispetto al dato globale (27,4%), invertendo la tendenza dello scorso anno in cui si registrava invece un aumento degli incidenti in Italia (65%) più significativo di quanto avveniva a livello internazionale (11,7%).

+15%
è la crescita degli incidenti subiti in Italia nel 2024 rispetto al 2023

Sempre in relazione al dato globale, decresce leggermente l'incidenza degli incidenti subiti da organizzazioni italiane rispetto al totale (**Fig. 25**): nel 2024 il dato italiano rappresenta il 10,1% del campione complessivo degli incidenti individuati in tutto il mondo, restando comunque nei pressi del picco negativo registrato lo scorso anno (11,2%).

+10%
è la quota degli incidenti subiti in Italia nel 2024 rispetto al dato globale

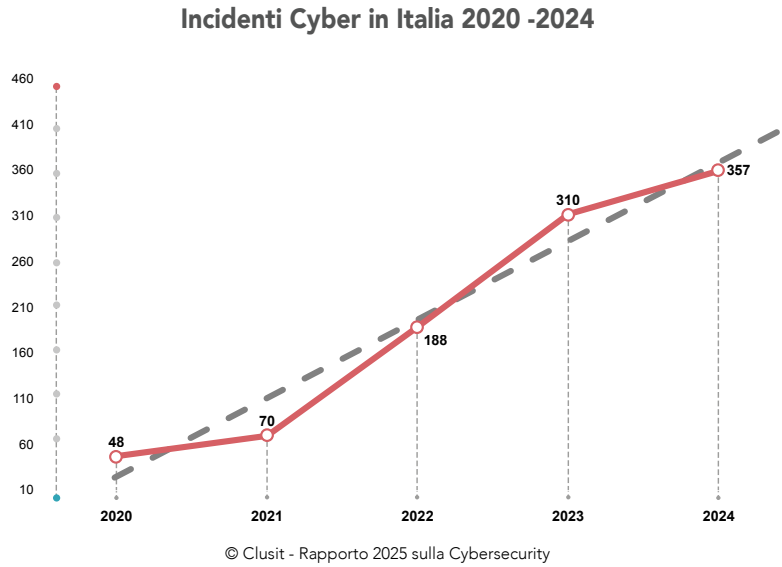


Fig. 23 - Distribuzione degli incidenti cyber in Italia nel periodo 2020-2024

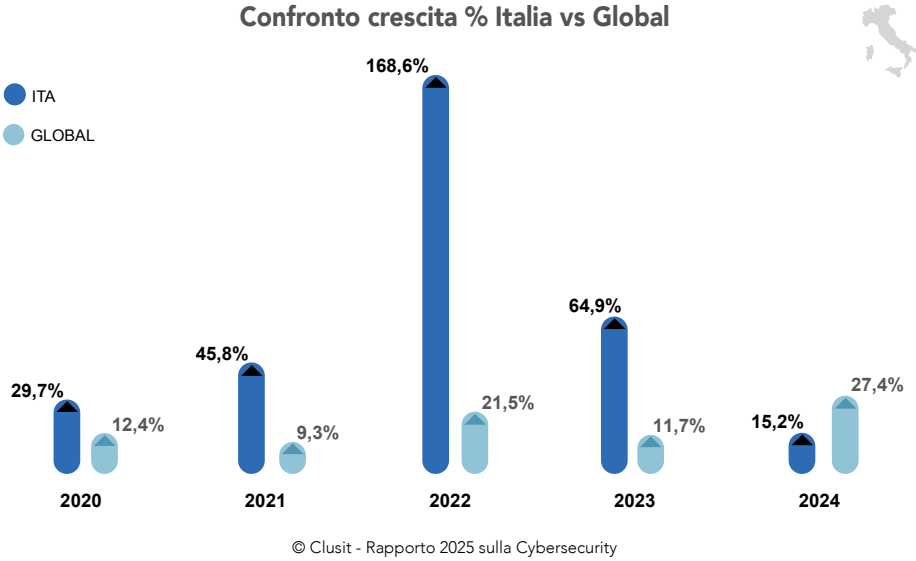


Fig. 24 - Confronto crescita percentuale in Italia vs. Global nel periodo 2020-2024

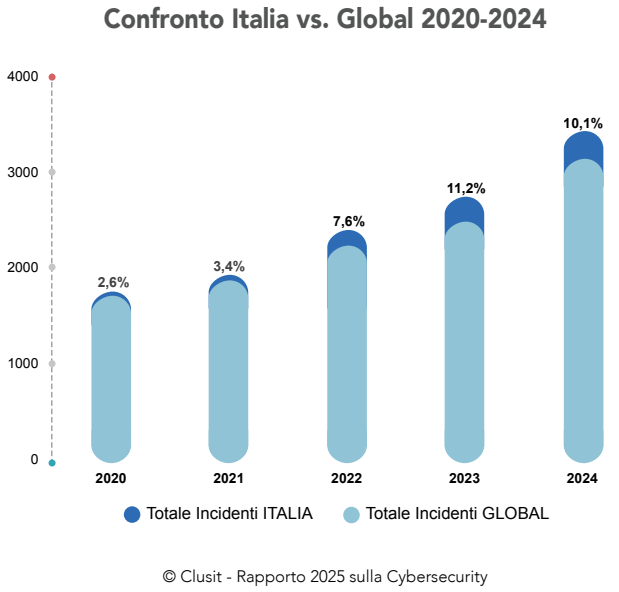


Fig. 25 - Incidenza degli incidenti in Italia rispetto al campione globale - 2020-2024

Distribuzione degli attaccanti per tipologia

Il panorama degli incidenti, valutato attraverso la tipologia degli attaccanti, conferma quanto rilevato negli ultimi anni. In Italia sono principalmente attive due tipologie di attaccanti: i *cybercriminali* e gli *hacktivist*. Nel nostro Paese non rilevano invece in modo significativo gli incidenti nelle categorie *Espionage / Sabotage* o *Information Warfare* (Fig. 26).

8 su 10
incidenti subiti in Italia nel 2024 sono di matrice Cybercrime

In particolare, la maggioranza degli incidenti italiani si riferisce alla categoria *Cybercrime*, che rappresenta il 78% del totale. Rispetto al 2023, in cui gli eventi di questa tipologia si fermavano al 64%, la distribuzione italiana si riavvicina a quella del campione globale, dove il Cybercrime si attesta all'86% (*vedere Fig. 3*).

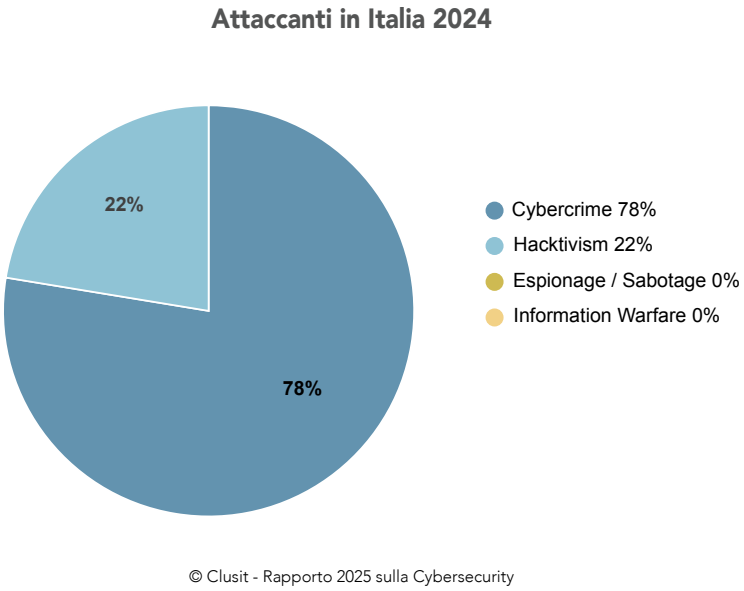


Fig. 26 - Attaccanti in Italia nel 2024

Gli incidenti classificati come *Hacktivism* costituiscono il restante 22%. Come già visto per lo scenario globale, anche in questo caso il tema dell'*attribution* di tali tipologie di attacco è un aspetto rilevante: gli eventi riferiti all'attivismo in questo periodo sono prevalentemente di matrice geopolitica e correlati ai conflitti in essere durante l'anno. D'altro canto, il protrarsi del conflitto in Ucraina nel 2024 ha causato una fase di lieve rallentamento degli attacchi e quindi degli incidenti di questa categoria, che rispetto al 2023 (**Fig. 27**), si riduce del 28% circa. In ogni caso, l'incidenza degli attacchi *hacktivism* rivolti a vittime italiane continua a essere considerevole: dei 279 incidenti rilevati complessivamente, 80 (circa il 29%) sono avvenuti nel nostro Paese.

29%
è la percentuale degli incidenti di hacktivism subiti in Italia nel 2024 rispetto al campione global

+40%
è la crescita degli incidenti di matrice cybercrime in Italia nel 2024 rispetto al 2023

Guardando i numeri in valore assoluto, colpisce come il cybercrime non solo mantiene la quota più consistente di incidenti, ma con 277 eventi nel 2024 contro i 197 del 2023 cresce percentualmente del 40,6%.

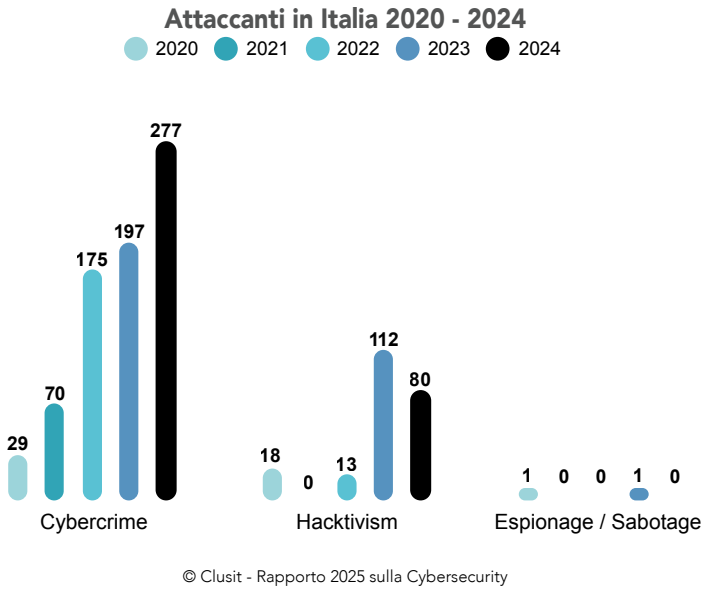


Fig. 27 - Attaccanti in Italia nel periodo 2020-2024

Il consistente aumento del cybercrime rende concreto ed evidente una tendenza diffusa di maggiore facilità di accesso agli strumenti necessari per mettere in atto questi reati anche da parte di cybercriminali meno esperti. Come evidenziato anche nell'analisi dei dati globali, la modalità di distribuzione degli attacchi in modalità "*as-a-Service*", che si realizza nel dark web su vere e proprie piattaforme di e-commerce, ha reso il la struttura tecnica del cybercrimine accessibile in modo vasto alle diverse organizzazioni criminali "tradizionali", aumentando così la frequenza degli attacchi su larga scala.

Distribuzione delle vittime per categoria

L'importanza di questo Rapporto risiede anche nella capacità di intercettare i cambiamenti significativi, che anno su anno possono fornire indicazioni utili per le organizzazioni pubbliche e private, per ridefinire la propria postura di sicurezza.

Uno di questi è rappresentato dalla distribuzione delle vittime italiane, che quest'anno contiene una novità che potrebbe rappresentare più un evento eccezionale che un'effettiva tendenza (Fig. 28): la categoria merceologica per cui si rileva un maggior numero di attacchi, infatti, è *News / Multimedia* che raggiunge il 18% del totale degli

incidenti (per maggiori dettagli, vedere più avanti l'approfondimento "*Il caso News / Multimedia*"). I settori che storicamente guidavano questa triste classifica si trovano nelle posizioni immediatamente successive: *Manufacturing* è al secondo posto, con il 16% degli attacchi, seguito da *Government* (10% del totale), che nel 2023 occupava il vertice della graduatoria. Da notare che anche quest'anno gli incidenti causati da attacchi *Multiple Target*, che per anni hanno guidato le classifiche nazionale e globale, sono meno di 1 su 5, in seconda posizione assieme al settore *Manufacturing*.

Proseguendo, si trovano le categorie *Transportation / Storage* (7%), *Professional / Scientific / Technical* (6%) e *Organizations* (5%).

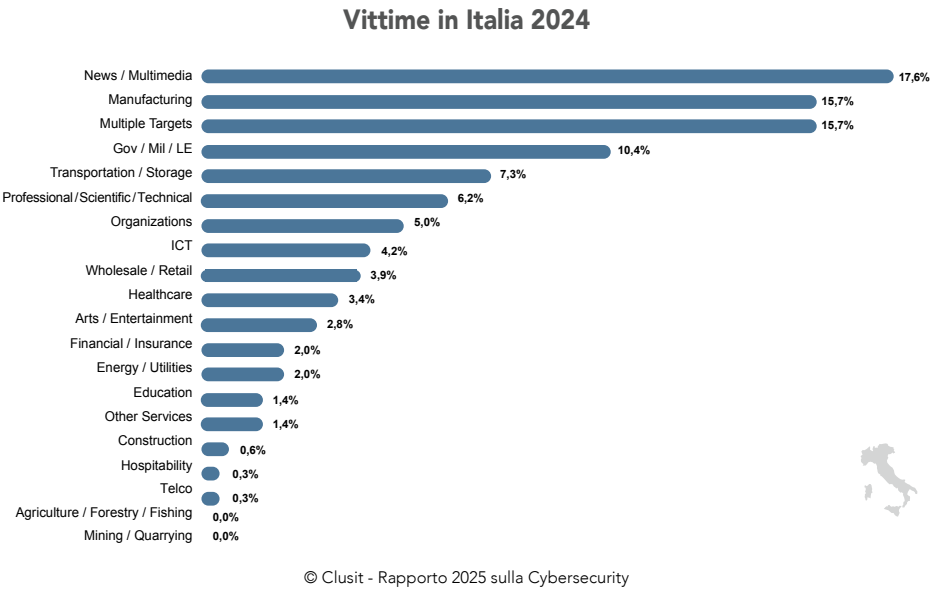


Fig. 28 - Distribuzione delle vittime in Italia nel 2024

Lo scenario italiano presenta quindi delle peculiarità, non solo derivanti dall'elevata incidenza degli incidenti rispetto al dato globale, anche in termini di distribuzione delle vittime. Nel campione mondiale, infatti, *News / Multimedia* è solo all'ottavo posto, subito dopo *Manufacturing*.

1/4

degli incidenti al settore Manifacturing nel mondo avvengono contro realtà italiane nel 2024

E proprio il manifatturiero è, come ormai triste consuetudine, un altro settore in cui l'Italia si distingue per numerosità delle vittime rispetto al mondo. Anche quest'anno un quarto del totale degli incidenti rivolti al *Manufacturing* complessivamente riguarda realtà italiane, settore che a livello globale rappresenta solo il 6%.

+1/4

degli incidenti settore Transportation / Storage nel mondo sono contro realtà italiane nel 2024

Risulta poi particolarmente colpito anche il comparto *Transportation / Storage*, con il dato italiano che rappresenta il 26% del dato globale.

Guardando alle dinamiche, si rileva ancora una volta un aumento del numero degli incidenti rispetto all'anno precedente per quasi tutte le aree merceologiche prese in esame.

Questi dati delineano un quadro allarmante rispetto alla capacità di protezione delle organizzazioni. Le tecniche di difesa adottate si rivelano infatti spesso inefficienti e la presenza di vulnerabilità rende questi bersagli particolarmente appetibili per gli attaccanti. È una tendenza da monitorare con attenzione, poiché rischia di aggravarsi nel prossimo futuro: se, da una parte, infatti, i livelli di protezione delle organizzazioni appaiono insufficienti, dall'altra gli attacchi diventano sempre più sofisticati, anche grazie all'uso dell'Intelligenza Artificiale, e facili da mettere in atto, con la già citata diffusione di modelli di minacce *as-a-Service*. Senza un'adeguata evoluzione delle contromisure introdotte, si rischia quindi che il divario tra attaccanti e vittime sia sempre più ampio e sempre più difficile da ricucire.

Il "salto" più evidente tra 2023 e 2024 (**Fig. 29**) è ovviamente quello della categoria *News / Multimedia*. Si verifica un aumento significativo degli incidenti anche nei settori *Multiple Target*, che con 21 incidenti in più cresce di 5 punti percentuali nella ripartizione complessiva, *Manufacturing* (56 incidenti nel 2024 vs 35 nel 2023, +3 punti percentuali) e *Professional / Scientific / Technical*. Sull'*Healthcare* la situazione è pressoché stabile, mentre diminuiscono gli incidenti indirizzati a *Government* che, seppur con 37 incidenti subiti, quest'anno risulta meno colpito dagli eventi con matrice hacktivism che avevano segnato una peculiarità nel 2023 (-8 punti percentuali), e *Transportation / Storage* (-5 punti percentuali rispetto al picco del 2023).

Il caso News / Multimedia

Il posizionamento strordinario di *News / Multimedia* in testa alla classifica delle vittime in Italia merita un approfondimento: tra gli incidenti pubblicamente noti c'è stato infatti uno specifico attacco che ha colpito ripetutamente un ampio insieme di testate giornalistiche, ad opera dello stesso gruppo cybercriminale, che ha sfruttato una vulnerabilità zero-Day per colpire il CMS diffusamente utilizzato dalle organizzazioni operanti nell'ambito dell'informazione. Le fonti riferiscono di 77 vittime colpite (di cui 62 sono le vittime note in Italia, 59 delle quali appartenenti appunto al settore *News / Multimedia*) e del furto dei dati personali di **5 milioni di utenti** (contenenti email, password, date di nascita e altre informazioni).

Perché è importante parlare di questo attacco? Sebbene si tratti chiaramente di un avvenimento anomalo e probabilmente isolato, presenta delle *lesson learnt* utili non solo per il settore specifico, che si è dimostrato particolarmente vulnerabile in Italia (l'incidenza delle vittime italiane sul totale degli incidenti subiti della categoria dell'informazione a livello globale è del 38%), ma per tutti gli ambiti in cui una tecnologia informatica – tipicamente un'applicazione o un servizio su cui si basa il funzionamento di applicazioni a supporto del business – è utilizzata in modo prevalente e presenta delle criticità di sicurezza. In tali casi, infatti, soprattutto quando tale tecnologia è nota per le caratteristiche sopra esposte, può diventare un bersaglio estremamente interessante e appetibile per gli attaccanti. Pur riducendo e/o concentrando l'investimento su poche tecnologie dominanti in uno specifico settore, i criminali informatici hanno però la certezza di generare, con una sola campagna di attacchi, un numero ingente di danni, fino a poter mettere in crisi un intero settore e causare verso la società conseguenze dirette, indirette o semplicemente generare caos e problemi verso comunità locali e nazionali. Si pensi ad esempio se ad essere bersagliata fosse una tecnologia utilizzata nell'ambito della distribuzione alimentare, o della logistica di beni e servizi ai cittadini. Non è un caso che tali scenari sono e devono essere esattamente quelli da considerare nell'ambito dell'applicazione della NIS2, particolarmente in quei settori che sono stati introdotti in perimetro nel passaggio dalla versione precedente a quella attualmente in vigore.

-7%

è la diminuzione degli incidenti subiti in Italia nel 2024 dal settore Finance / Insurance

Un'altra situazione eccezionale rilevata lo scorso anno era rappresentata dal picco degli incidenti subiti dai settori *Financial / Insurance*, che quest'anno tornano allo stesso numero del 2022 (7 eventi) e scompaiono dalla Top 10, con un'incidenza di solo il 2% sul totale e una diminuzione di 7 punti percentuali. La crescente pressione normativa su questo settore, già fortemente regolato, impone alle istituzioni finanziarie di conformarsi a requisiti stringenti per garantire la protezione delle informazioni e la resilienza operativa, stimolando gli investimenti in sicurezza e l'introduzione di contromisure all'avanguardia.

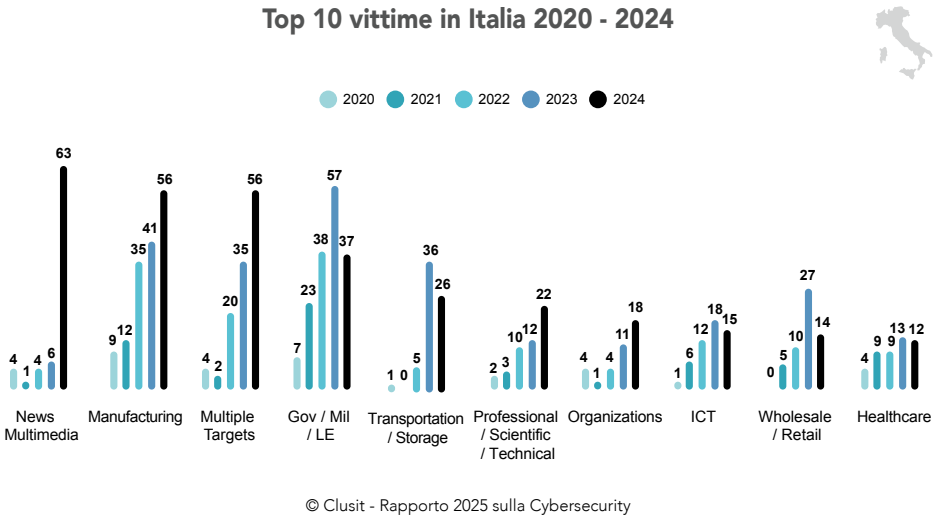


Fig. 29 - Le prime 10 categorie di vittime n Italia nel periodo 2020-2024

Distribuzione delle tecniche di attacco

Anche l'analisi delle tecniche di attacco aiuta a comprendere le cause sottostanti al numero significativo di incidenti di cui sono state vittime le nostre imprese e istituzioni.

Nel 2024 il *Malware* torna ad occupare la prima posizione, con il 38% degli incidenti (**Fig. 30**). I cyber incidenti causati da *DDoS* si attestano quest'anno al 21%, cedendo il primo posto occupato nel 2023 con il 36% del totale.

+1/3
degli incidenti in Italia nel 2024 sono causati da Malware

Ma c'è un'altra novità significativa: al terzo posto, infatti, si trovano gli incidenti basati su *vulnerabilità*, al 19%, una quota storica per l'Italia. Questo incremento è certamente giustificato dall'influenza degli incidenti che hanno colpito il settore *News / Multimedia*, di cui abbiamo parlato nei paragrafi precedenti.

Segue il *Phishing / Social Engineering* all'11%, confermando che resta una tecnica "prediletta" dagli attaccanti per accedere ai sistemi delle vittime: il fattore umano resta sempre il varco di accesso più facile!

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

Nel grafico di Fig. 30 si nota anche la "comparsa" in Italia delle *Multiple Techniques* (2%), indice di una quota di attacchi particolarmente sofisticati, e la persistenza dei *Web Attacks* (2%).

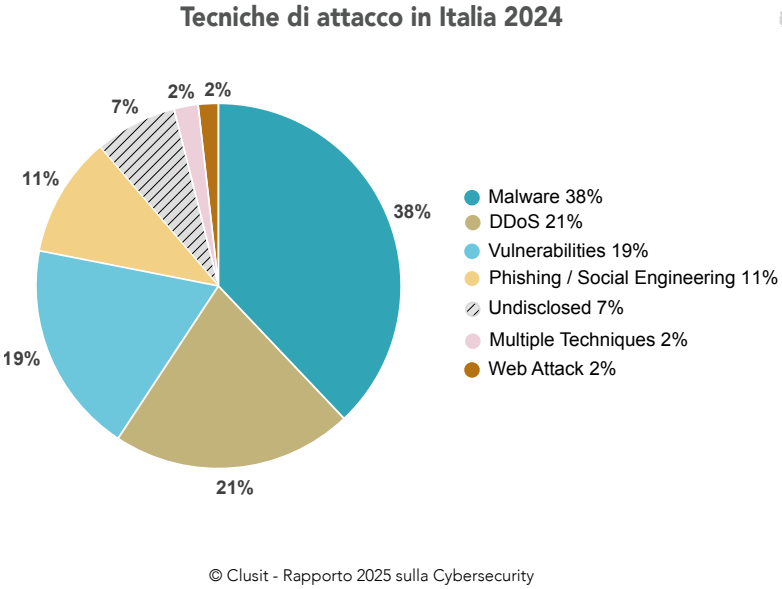


Fig. 30 - Tecniche di attacco in Italia nel 2024

Se proviamo a esaminare i dati storici sulle tecniche di attacco (**Fig. 31**) notiamo una diffusa crescita per quasi tutte, eccezion fatta per le già citate "*Undisclosed*" e per i *DDoS*, che diminuiscono anche in termini assoluti del 36% (76 incidenti contro i 111 del 2023, quando si è verificato il picco della costante crescita degli anni precedenti); questo dato è in controtendenza con il dato globale che vede invece un aumento di incidenti che sfruttano questa tecnica.

-36%
è la riduzione dal 2023 al 2024 degli attacchi DDOS in Italia

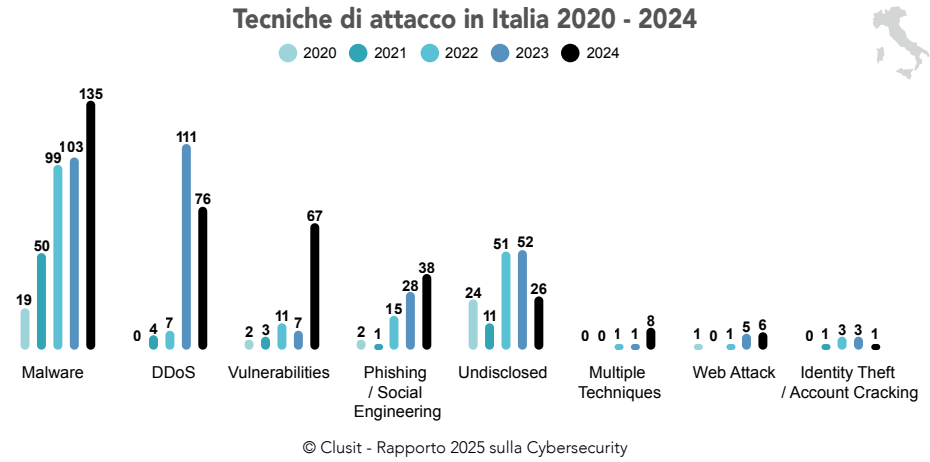


Fig. 31 - Tecniche di attacco in Italia nel periodo 2020-2024

Questo risultato si può spiegare in due modi: l'interesse degli attivisti potrebbe essersi spostato su altri Paesi più coinvolti del nostro negli attuali scenari di guerra, oppure gli attacchi non generano in Italia, come è avvenuto in passato, un numero così elevato di incidenti significativi per una migliorata postura delle vittime. D'altro canto, il calo del *DDoS* è coerente con il calo di *Hacktivism* che abbiamo sottolineato nei paragrafi precedenti: i *DDoS* sono prevalentemente attacchi dimostrativi, perpetrati dagli attivisti, che nel 2024 impattano molto meno sulle organizzazioni italiane.

+90%

è la crescita degli incidenti in Italia basati su Vulnerabilities, dal 2023 al 2024

Il *Malware* vede invece un considerevole aumento di incidenti (135 rispetto a 103 del 2023, con un tasso di crescita di oltre il 30%) con un andamento analogo al resto del mondo; gli incidenti basati su *vulnerabilità* crescono quasi del 90% (da 7 a 67 incidenti), per le ragioni spiegate sopra relative al settore *News / Multimedia*, e, per le stesse ragioni, restano invece stabili come media mondiale.

+35%

è la crescita degli incidenti in Italia basati su phishing e ingegneria sociale, dal 2023 al 2024

I *Web attack* restano pressoché stabili, mentre a livello globale registrano in incremento di circa il 50%, e le *Multiple Techniques* vedono un preoccupante aumento del 90% (da 1 a 8 incidenti). In aumento anche il numero di incidenti dovuti al *Phishing* (da 28 a 38, con un tasso del +35%).

La percentuale di incidenti che sfruttano il furto di identità in Italia rimane trascurabile, ma è bene ribadire ciò che già affermavamo lo scorso anno: nel nostro Paese, le cosiddette "truffe informatiche", rivolte sia a persone sia a piccole imprese, sono in realtà in costante aumento[1], tuttavia con un impatto e una gravità che non consentono a questo tipo di avvenimenti di rientrare nella statistica del nostro Rapporto.

Analisi della "Severity" degli incidenti

Dal punto di vista della Severity degli incidenti, il dato italiano (**Fig. 32**) si distacca parzialmente da quello internazionale.

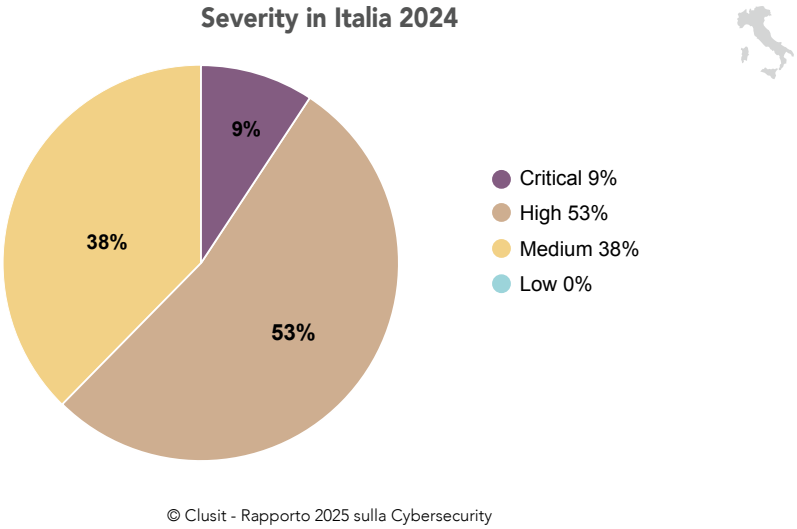


Fig. 32 - Severity degli attacchi in Italia nel 2024

Se la severity *High* è tre punti percentuali più alta di quella globale (53% contro 50%), ma comparabile – intorno alla metà degli incidenti misurati – quella *Critical* è invece significativamente più bassa (9% contro 29%), mentre quella *Medium*, al contrario, è molto più alta: 38% contro 22%. Gli incidenti a basso impatto sono anche per l'Italia in percentuali trascurabili (meno dell'1%). Possiamo interpretare questo dato con un'accezione sia positiva sia negativa: da un lato, è sicuramente un buon segno che gli incidenti danneggino 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

[1] Fonte: https://lab24.ilsole24ore.com/indice-della-criminalita/

loro danni sono più circoscritti. Dall'altro lato, però, la ripartizione potrebbe indicare che le organizzazioni italiane sono più spesso vittime anche di attacchi meno sofisticati, che nel resto del mondo incidono meno, ed essere quindi sintomo di una scarsa capacità di contrastare le minacce cyber.

Anche dai dati dell'Osservatorio Cybersecurity del Politecnico di Milano emerge una riflessione simile: il 73% delle grandi aziende italiane dichiara di aver subito attacchi nel corso degli ultimi 12 mesi[2], che però nel 37% dei casi non hanno rappresentato una reale minaccia per l'organizzazione. Gli incidenti hanno causato invece la necessità di interventi onerosi di mitigazione, con un impatto sui costi e sull'operatività delle aziende, nel 7% dei casi: una percentuale che, trattandosi di grandi organizzazioni presumibilmente strutturate dal punto di vista del presidio della cybersecurity e con rilevanti investimenti sostenuti, tradisce una difficoltà nelle strategie di difesa.

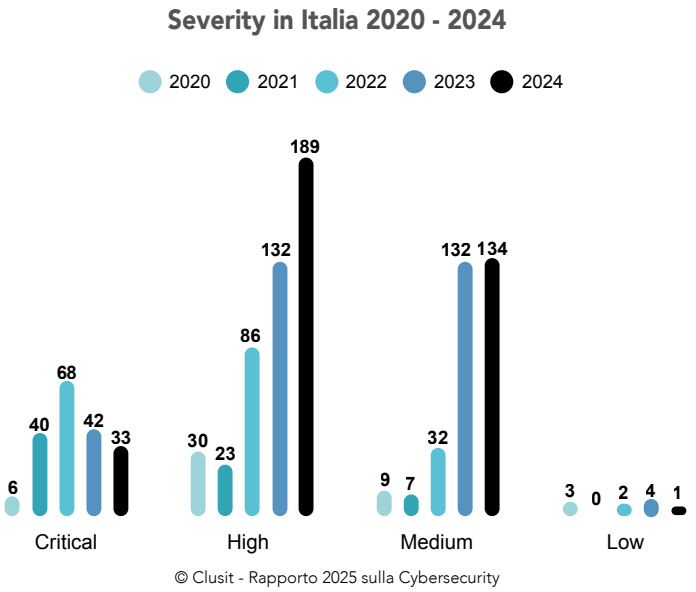


Fig. 33 - Severity degli attacchi in Italia nel periodo 2020-2024

[2] Fonte: survey dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, 131 CISO di grandi organizzazioni (oltre 250 addetti).

Guardando alla progressione storica (**Fig. 33**), è possibile notare il costante calo degli incidenti classificati *Critical* (dal picco del 57,1% del 2021 all'attuale 9,2%, con 35 incidenti in meno rispetto al 2022), più che compensato dall'aumento dell'incidenza degli incidenti con severity *High* (+10 punti percentuali rispetto al 2023, con ben 189 eventi nel 2024). Sebbene gli incidenti con severity *Medium* diminuiscano di 5 punti percentuali nella ripartizione complessiva del campione, guardando ai valori assoluti si nota una stabilità. Gli incidenti con severity bassa, infine, costituiscono una quota minima del campione.

Dall'analisi alla sintesi: dai trend alla strategia

Sebbene i dati che rileviamo e presentiamo anno dopo anno siano, come per altro è riscontrabile dalla cronaca, sempre più allarmanti e sostanzialmente monotòni nella progressione negativa, negli ultimi 18 mesi l'avvicendarsi di cambiamenti rilevanti nello scenario geopolitico, nonché la recrudescenza degli attacchi verso l'Italia, ci permette di "leggere" attraverso le statistiche del Rapporto delle informazioni utili per indirizzare le scelte che imprese, pubbliche amministrazioni e più in generale il Sistema Paese dovrebbero porre al centro dell'agenda della digitalizzazione, ovvero della stessa strategia di cybersecurity.

Questa lettura non può essere scevra di due ulteriori fattori:

- l'evoluzione dello scenario geopolitico degli ultimi mesi, con riferimento al 2025 ed ai cambiamenti in atto nelle politiche delle nazioni a valle dei percorsi elettorali conclusi nel 2024, non ultimi lo spostamento del baricentro delle alleanze degli Stati Uniti nell'ambito dei conflitti Russo-Ucraino e Israeliano-Palestinese;
- l'introduzione e l'evoluzione delle nuove normative Europee e nazionali a cui sono soggette le imprese italiane di molti settori, come l'AI ACT e la Direttiva NIS2.

Come già detto nel Rapporto 2024, "la **capacità di determinare, anticipare e gestire** le evoluzioni legate alle minacce esogene, oltre che al contesto interno dell'organizzazione, è ormai fondamentale nel quadro che il Rapporto ci permette di delineare" con riferimento alla velocità con la quale cambia lo scenario delle minacce, quello degli attaccanti e dei settori più colpiti. Quanto meno rispetto all'Italia, semestre su semestre osserviamo variazioni inedite nella classifica dei settori più colpiti. Nel 2024 assistiamo poi ad un nuovo rovesciamento tra DDOS e Malware tra le tecniche più utilizzate, ed il "caso News / Multimedia" rende evidente come anche una singola campagna particolarmente focalizzata su un settore o tecnologia, possa produrre variazioni significative nello scenario complessivo.

È per questo che riteniamo che al primo posto tra le azioni necessarie sia posizionata la **governance della sicurezza e la capacità di identificare, analizzare, valutare e gestire i rischi**, sia con misure preventive che di mitigazione, ma anche nella prospettiva di gestire il trasferimento del rischio verso terzi (sia in ottica di coperture assicurative, ma anche trasferendo l'onere dell'implementazione delle misure di mitigazione mediante il ricorso ad un outsourcing di qualità, per esempio nell'ambito di percorsi di *Cloud Journey*).

Non possiamo non considerare che la stessa normativa NIS2 richiama alla responsabilizzazione del vertice aziendale sui temi cyber, ed alla capacità, tramite il presidio dei rischi, di adattare la propria postura ai cambiamenti sempre più repentini dello scenario.

La **capacità di determinare, anticipare e gestire** le evoluzioni legate alle minacce esogene, oltre che al contesto interno dell'organizzazione, è ormai fondamentale nel quadro che il Rapporto ci permette di delineare: il risk management non può più essere "uno strumento per pochi esperti". Il GDPR lo ha reso necessario su tutto il perimetro dei trattamenti dei dati personali, è ormai ora di fare tesoro di questa esperienza per gestire anche i rischi cyber contro l'organizzazione.

Resta ancora fondamentale mantenere alta l'attenzione al tema della consapevolezza delle persone: la crescita del 35% degli incidenti cyber basati sul phishing non è l'87% del 2023, ma è ancora un tasso inaccettabile tanto per le piccole/medie, come per le grandi organizzazioni.

Anche guardando ai dati dei successivi capitoli del Rapporto, come, ad esempio, il contributo della Polizia Postale e delle Comunicazioni a cui si rimanda la lettura, sarà evidente come il fenomeno della insicurezza cyber sia di rilevanza economico-sociale, e non certo limitato alle grandi organizzazioni.

Sosteniamo ancora una volta che la Scuola, l'Università, i soggetti pubblici e privati debbano lavorare in sinergia per **sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni**.

Rispetto agli impatti dei cyber attacchi e incidenti informatici verso la società ed i servizi fondamentali rivolti ai cittadini, siamo molto fiduciosi dei benefici che saranno ottenuti dal percorso pluriennale intrapreso per l'attuazione della Direttiva NIS2 orchestrato dall'Agenzia per la Cybersicurezza Nazionale, con un ampio coinvolgimento di Ministeri e Dipartimenti per la definizione delle modalità di attuazione nei diversi settori in perimetro.

Ci aspettiamo, da questo sforzo di portata nazionale, un cambio di passo rispetto a tutta una serie di problematiche e situazioni in cui abbiamo assistito negli ultimi anni, non ultimo il 2024, dovuti a incidenti e attacchi apportati alle infrastrutture digitali. La "resilienza digitale" deve diventare una delle dimensioni del patto di fiducia tra cittadini / utenti e amministrazioni / imprese.

La fiducia è un aspetto fondamentale per assicurare un proficuo sviluppo delle tecnologie innovative. L'AI Act non deve essere percepito come "un'altra compliance", quanto piuttosto i binari nei quali le "magnifiche sorti e progressive" si sposino con temi attualissimi come quelli dell'etica digitale, del rispetto e della tutela dei dati personali dei cittadini, e non ultimo della sicurezza delle informazioni nella sua più ampia accezione.

Il percorso delle compliance non si esaurirà con la NIS2 e l'AI Act: il Cyber Resilience Act, la Direttiva CER sulla Resilienza delle Entità Critiche, sono già oggi temi all'attualità, anche e soprattutto in quegli ambiti dove altri dispositivi normativi attinenti a temi legati alla cybersecurity non sono (fino ad oggi) intervenuti. Uno di questi in particolare è quello delle tecnologie OT/IoT, che comunque saranno già interessate da iniziative di cybersecurity da parte dei soggetti che rientrano nel perimetro NIS2.

Ai soggetti pubblici e privati, pertanto, si paventano due importanti sfide nel medio termine:

- sostenere la crescente pressione degli attacchi, anche in ambiti di particolare innovazione, come l'AI, o fino ad oggi tradizionalmente meno presidiati (OT/IoT);
- adeguarsi e mantenersi adeguati alle normative settoriali e generali, in misura progressivamente crescente.

Avere consapevolezza di questo consentirà di applicare logiche e criteri di convergenza tra adempimenti e azioni volte a mitigare i rischi di sicurezza, evolvere i modelli organizzativi per attribuire le diverse responsabilità in modo bilanciato e adeguato, definire dei meccanismi di funzionamento nei quali le misure necessarie a soddisfare i diversi obiettivi possano agire in modo sinergico, evitando di ingenerare burocrazia, inefficienza e sovrapposizioni.

Agire nei punti più critici e funzionali a ottenere questo risultato sarà cruciale. Uno di questi è certamente il **presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita** (SSDLC - Secure Software Development LifeCycle), sia in ambienti waterfall che agili (SecDevOps), adottando **soluzioni** che affrontino efficacemente l'**ambito della sicurezza delle applicazioni** su ogni elemento (servizi

esposti, front end, middleware, applicazioni mobili, IoT) e non solo in fase di scrittura del codice.

In particolare, le logiche di **security by design** devono diventare parte dei processi di sviluppo di prodotti e servizi a partire da quando i servizi vengono concepiti, dall'on-premise al cloud, con una sempre più stringente **gestione dei processi di sourcing e delle terze parti**, non solo in ottica di compliance, ma anche in ottica di tutela aziendale.

Anche i processi di monitoraggio e gestione degli incidenti e delle crisi cyber devono essere resi più efficienti ed efficaci, creando procedure, playbook, comunicati stampa e simulando la gestione di tali eventi, così da essere certe di essere in grado di limitare i possibili danni.

Infine, molti temi aperti rimangono quelli degli anni passati: i punti di attenzione non cambiano, ne aumenta semplicemente la criticità rispetto alle esigenze di un contesto economico e sociale sempre più legato allo sviluppo del digitale, e in un contesto di aumento del rischio, anche per uno scenario geopolitico sempre meno tranquillizzante.

Appendice metodologica

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

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

I dati riportati si riferiscono ad incidenti reperibili in fonti di informazione pubbliche. Da quando, nel 2011, è iniziata questa attività, il numero di fonti utilizzato è molto aumentato, e le modalità di ripulitura dei dati, ad esempio dalle duplicazioni, sono migliorate. L'utilizzo di fonti pubbliche introduce comunque un *bias* rispetto alla totalità degli incidenti occorsi e, quindi, all'esposizione ai rischi. In questa sezione cerchiamo di dare una maggiore visibilità a questi possibili bias, in modo che se ne possa tenere conto. Per contro, quando un incidente arriva ad essere pubblicato sulle fonti analizzate, di solito le caratteristiche descritte risultano essere abbastanza affidabili. Quando non lo sono, normalmente le parti interessate tendono a pubblicare o chiedere la rettifica con 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, incidenti causati da malware, di minore entità che, per chi deve gestire la sicurezza di un'organizzazione, probabilmente aggiungono poco rispetto alla valutazione della necessità di adottare una baseline di misure di sicurezza che è ormai da considerare indispensabile.

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

in questa analisi, ma pubblicati in altre parti del Rapporto, dando loro anche la giusta e specifica visibilità.

Nel campione di questa analisi sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage, che tendono ad essere condotti con grande cautela e pertanto emergono più difficilmente. Questo può essere un limite importante da considerare: gli attacchi che colpiscono la riservatezza dei dati sono sicuramente sottorappresentati perché, a meno che gli attaccanti per qualche motivo pubblichino l'informazione, le stesse organizzazioni colpite potrebbero non averne evidenza. Si tratta di *known unknown* rispetto ai quali è difficile avere dati statisticamente significativi. Anche venendone a conoscenza, le organizzazioni colpite potrebbero avere interesse a non darne evidenza a nessuno. Un tema analogo è legato alle attività di information warfare, che possono essere condotte con altrettanta cautela, anche per non esporre gli strumenti utilizzati[3]. 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 come 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 rilevati o comunque 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'ulteriore considerazione riguarda il tema della severity. Nel tempo, l'impatto medio degli incidenti è aumentato. Come conseguenza, gli incidenti di impatto "low" stanno diventando marginali. Per mantenere la significatività di questo tipo di analisi, sarà necessario nel tempo rivedere la scala ed i parametri su cui si basa, in modo da dare di nuovo significatività ad una statistica che comincia ad essere troppo appiattita verso l'alto. Questo comporterà necessariamente un momento di stacco e perdita

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

di confrontabilità del dato anno su anno. Proprio per valutare al meglio come gestire questa discontinuità, per quest'anno la scala di criticità non è ancora stata rivista, ma lo sarà quasi certamente al prossimo anno o al più al successivo.

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 ed ampie. È quindi utile focalizzarsi su queste ultime e sull'andamento complessivo, piuttosto che su piccole fluttuazioni annuali. Per questo, anche quest'anno abbiamo aumentato l'attenzione ai fenomeni più significativi, riducendo la disamina di singole variazioni meno rilevanti.

Analisi Fastweb della situazione italiana in materia di cyber-crime

(A cura di Domenico Barresi, Mario Boemi, Laura Bongiorno, Martina D'Agnolo, Sergio Inglima Modica, Luca Memini, Vincenzo Muratore, Corrado Pezzella, Luca Pupillo, Mirko Santocono, Girolamo Tesoriere, Fastweb)

Introduzione

Anche quest'anno Fastweb contribuisce a fotografare la situazione del cyber crime in Italia attraverso il proprio Security Operations Center (SOC), attivo 24/7, e i propri centri di competenza di sicurezza informatica. Grazie alla collaborazione con 7Layers, azienda acquisita da Fastweb nel 2020 e specializzata in soluzioni avanzate di cybersecurity, il report include anche il monitoraggio relativo alle minacce informatiche più sofisticate rilevate e contrastate tramite il servizio di Managed Detection and Response (MDR).

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 7 milioni di indirizzi IP pubblici (in crescita rispetto ai 6,5 milioni monitorati nel 2023) e su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati nel 2024 oltre 69 milioni di eventi di sicurezza, in aumento del 23% rispetto al 2023.

Una crescita significativa delle minacce cyber che segna un netto cambio di tendenza rispetto al 2023 quando il numero di attacchi rilevati era rimasto sostanzialmente stabile rispetto all'anno precedente. L'incremento degli eventi di sicurezza registrati nel 2024 è stato accompagnato da un progressivo avanzamento nelle capacità di risposta, con sistemi di difesa e monitoraggio più sofisticati e metodi di rilevamento più efficaci che hanno permesso una migliore rilevazione e mitigazione delle minacce.

Anche nel 2024 l'impiego dell'AI nello sviluppo di tecniche di attacco e difesa sempre più sofisticate assume un ruolo centrale nell'evoluzione del paradigma della sicurezza informatica. Sul fronte offensivo, l'utilizzo di algoritmi di AI contribuisce ad automatizzare la ricerca di vulnerabilità nei sistemi target, accelera lo sviluppo e l'evoluzione di malware sofisticati, e perfeziona le tecniche di evasione, rendendo gli attacchi più difficili da rilevare e contrastare per i tradizionali sistemi di sicurezza. Parallelamente, sul versante difensivo, l'IA sta trasformando le capacità di protezione migliorando significativamente la rilevazione precoce delle minacce, potenziando la prevenzione degli attacchi e ottimizzando i tempi di risposta agli incidenti. L'integrazione sempre più profonda dell'AI all'interno delle infrastrutture di cybersicurezza di Fastweb ha permesso all'azienda di identificare anomalie ed eventi malevoli con più efficacia riducendo la rilevazione di falsi positivi in linea con le tendenze di settore (fino al 70%).

In controtendenza rispetto al 2023, torna a crescere il numero di infezioni da malware e botnet rilevate in Italia. In particolare le botnet identificate nel 2024 hanno registrato un totale di 180.486 eventi (indicativi sia delle chiamate malevoli che tentativi di chiamate verso botnet) con un incremento di circa il 41%. Un fattore chiave di questa crescita è la botnet 911-socks5-proxy, responsabile del 36,13% delle infezioni, che ha contribuito all'espansione delle minacce informatiche.

Crescono anche le infezioni da malware in aumento del 131%, che passano da 848.000 casi nel 2023 a 1.960.000 nel 2024 (in termini di connessioni provenienti da dispositivi infetti). Cresce anche il numero delle famiglie di malware malevoli in circolazione che passano da 148 a 160, in aumento del 7,5%.

Un incremento sostenuto da diversi fattori come l'aumento dei dispositivi IoT a rischio compromissione, un utilizzo sempre più pervasivo dell'Intelligenza Artificiale e delle tecniche adattative avanzate che consentono ai cyber-criminali di orchestrare attacchi su larga scala, oltre a un'espansione e diversificazione delle infrastrutture digitali (Cloud, Edge Computing, 5G). Le infezioni da malware sconosciuti, invece, sono scese allo 0,12%, segnalando un miglioramento nelle difese zero-day.

L'analisi dei trend rivela un andamento stagionale nelle infezioni da malware e botnet, con picchi significativi osservati nei mesi di giugno e luglio. Questo fenomeno può essere collegato all'incremento dell'utilizzo di dispositivi personali durante il periodo estivo. In questi periodi di elevata mobilità, i dispositivi possono essere esposti più frequentemente a reti Wi-Fi non sicure, aumentando il rischio di compromissione. Inoltre, strategie di distribuzione mirate, come l'attacco *android.vo1d* sui dispositivi Android, sfruttano vulnerabilità legate a versioni obsolete del sistema operativo e/o delle app, aggravate dalla mancata applicazione degli aggiornamenti di sicurezza da parte degli utenti.

In ambito DDoS, si osserva un aumento del 100% del numero di attacchi rispetto al 2023. Emerge, inoltre, un incremento del 167% della distribuzione della banda aggregata media in Tbps e una crescita marcata degli attacchi di maggiore intensità (>100 Gbps). Si registra, in particolare, un aumento di attacchi di tipo "carpet bombing" in cui il traffico malevolo viene distribuito su un ampio range di indirizzi IP appartenenti alla stessa rete target, rendendo l'attacco più difficile da rilevare e mitigare. I settori più colpiti dagli attacchi DDoS si confermano la Pubblica Amministrazione e il Finance & Insurance in linea con il trend rilevato nel 2023.

Proprio il Finance & Insurance, nonostante abbia registrato un aumento del 36% degli attacchi rilevati rispetto al 2023 , è riuscito a contenere gli attacchi DDoS in modo più efficace rispetto ad altri settori grazie a maggiori investimenti in strategie

di difesa cyber, e nuove tecnologie come l'AI che continueranno a essere favoriti anche dall'entrata in vigore del Digital Operational Resilience Act (DORA) nel 2025.

Gli attacchi alla Pubblica Amministrazione hanno registrato un significativo incremento, passando da 560 a 1.430 (+155%). Un fenomeno correlato alla crescente instabilità geopolitica e all'incremento delle attività di hacktivisti, oltre all'espansione del perimetro di attacco con la crescente disponibilità di servizi digitali a cittadini, imprese e PA.

Il numero di sistemi che espongono su internet servizi critici è in calo costante, con una riduzione dell'11% nel 2024 (33.800 sistemi) rispetto al 2023 (38.000 sistemi). Questo trend positivo, in atto dal 2019, riflette un progressivo miglioramento nella sicurezza delle organizzazioni grazie a strumenti di monitoraggio avanzati e maggiore consapevolezza dei rischi informatici.

L'analisi delle vulnerabilità applicative da parte del SOC di Fastweb evidenzia quest'anno un significativo miglioramento della sicurezza dei software di dispositivi e applicazioni frutto della sempre maggiore consapevolezza dei rischi informatici. L'adozione di diverse contromisure raggruppate nella categoria di mitigazione chiamata WebApp Untarget Scan, indirizza le attività di scansioni esterne non mirate (Untargeted Scan Blocking) e quindi ostacola l'Information Gathering utile alle fasi successive per l'avvio di attacchi mirati. Questa strategia di mitigazione nel 2024 risulta tra le tipologie di contromisura maggiormente intervenuta a protezione degli attacchi applicativi (53% dei casi). Tra le altre tecniche di attacco si confermano al primo posto le SQL-Injection (25,96%), seguite da Directory Traversal (20,49%), attraverso tentativi di accesso non autorizzato ai file di sistema. Il Cross Site Scripting (XSS) mantiene una quota rilevante (14,77%) e infine gli attacchi RFI Injection (6,96%) e File Injection (6,70%) crescono rispetto al 2023, confermando come le tecniche di attacco vengono diversificate in conseguenza alle soluzioni usate per lo sviluppo di applicazioni web.

L'analisi della distribuzione geografica degli attacchi informatici nel 2024 rivela uno scenario in evoluzione. Gli Stati Uniti mantengono il primato come principale fonte di attacchi, seguiti dall'Italia, che sale al secondo posto, e dai Paesi Bassi, new entry nella classifica. L'ascesa dell'Italia si attribuisce principalmente all'incremento dell'utilizzo, da parte degli attaccanti, di piattaforme cloud e botnet nel Paese, strategia che permette di eludere i filtri geografici.

Gli USA restano leader anche nella distribuzione dei centri di controllo malware (C&C) rappresentando il 50% del totale (in crescita dal 36% del 2023), seguiti da Brasile (6%) e Regno Unito (4%). Nonostante l'Italia presenti una bassa concentrazione di C&C sul

proprio territorio, il rischio di attacchi rimane elevato a causa del traffico malevolo che può originarsi da server C&C situati in altri Paesi.

Fastweb ha continuato a monitorare anche le minacce legate ai servizi e-mail. Nel 2024 si registra un aumento degli attacchi tramite URL malevoli (+8,6% rispetto al 2023), mentre la presenza di allegati infetti è in lieve calo (-2,5%). Anche in questo caso, l'uso crescente dell'intelligenza artificiale da parte dei cybercriminali rende questi attacchi sempre più sofisticati, inducendo gli utenti a cliccare su link dannosi con maggiore facilità. Il Credential Phishing basato su GenerativeAI, sebbene in calo del 60% rispetto al 2023, resta la minaccia più diffusa (71,7%) grazie a contenuti sempre più convincenti e privi di errori mentre gli attacchi basati sulla distribuzione di Malware tramite mail sono in crescita del 20% (confermandosi anche quest'anno una delle minacce più diffuse), con software dannosi come Astaroth, WikiLoader e Agent Tesla usati per furto di dati e crimini informatici. A livello di metodologia utilizzate dai cybercriminali nel veicolare le minacce via e-mail, la tecnica di social engineering, che aveva fatto registrare un aumento notevole nell'anno 2023, riporta una tendenza in decrescita facendo registrare volumi medi più bassi, a dimostrazione del miglioramento dei presidi di sicurezza nel riconoscere questo tipo di minacce. Infine, la categoria Banking Malware seppur non si classifichi più tra le prime minacce, registra un andamento in crescita dall' 1,30% del 2023 al 2,40% del 2024, e continua a rappresentare un rischio per il furto di credenziali bancarie e la frode online.

Anche nel 2024 le principali tipologie di frodi rimangono legate alla sottoscrizione con furto di identità e al CLI Spoofing, ovvero la manipolazione del numero chiamante per truffe telefoniche. Si osserva una riduzione dei tempi di rilevazione e denuncia del furto di identità, con il 60% dei casi scoperti entro 12 mesi. Un fenomeno emergente nel 2024 è l'uso combinato di chiamate da numeri esteri e successivi contatti via WhatsApp, mirati al furto di account tramite tecniche di social engineering. Inoltre, si registra un aumento delle frodi sugli SMS commerciali (A2P), con tentativi di bypassare i costi di interconnessione attraverso canali fraudolenti.

Alle rilevazioni Fastweb, si aggiungono quelle dei sistemi MDx di 7Layers, che hanno registrato un aumento del 100% degli eventi e alert gestiti, grazie all'espansione del perimetro di monitoraggio e all'introduzione di nuove soluzioni EDR (Endpoint Detection and Response). La maggiore adozione dei servizi di sicurezza da parte delle aziende e l'espansione delle fonti di dati, hanno permesso a 7Layers di tracciare un quadro sempre più preciso delle tattiche sfruttate dagli attaccanti evidenziando, secondo la classificazione MITRE, una prevalenza significativa della tattica Execution che prevede l'esecuzione di codice dannoso all'interno dell'ambiente target.

Questa tecnica, complice anche il significativo aumento degli eventi e alert gestiti, mostra un trend in crescita nella frequenza di utilizzo rispetto al 2023 passando dal 10% al 38%.

In conclusione, le rilevazioni di Fastweb e 7Layers del 2024 confermano un panorama di minacce in continua evoluzione, con un turnover più marcato delle tipologie di attacco e con fenomeni di concentrazione, intensificazione, diversificazione e stagionalità degli attacchi, agevolati sempre più dall'uso dell'AI. La complessità di questo scenario però è stata ben contenuta da parte delle aziende grazie a una crescente consapevolezza, all'adozione di soluzioni di sicurezza evolute, sistemi di rilevazione sempre più accurati e grazie alla formazione in ambito cybersecurity. Un esempio virtuoso che dimostra l'efficacia di queste azioni è relativo al settore Finance & Insurance che ha visto un trend generale di decrescita degli attacchi subiti.

L'adozione di soluzioni di sicurezza by design e il loro continuo aggiornamento assume un ruolo centrale per contrastare attacchi sempre più sofisticati e diversificati. I trend osservati confermano che la cybersecurity rappresenta una priorità strategica: se gli attacchi aumentano e diventano più sofisticati, anche gli strumenti di difesa devono evolvere rapidamente.

Malware e Botnet

Le infezioni malware e gli attacchi veicolati tramite botnet, che interessano i server e i dispositivi appartenenti all'Autonomous System di Fastweb, nel 2024 hanno registrato un incremento. In particolare le botnet identificate nel 2024 raggiungono quota 180.486 con un incremento di circa il 41%. Un fattore chiave di questa crescita è la botnet 911-socks5-proxy, responsabile del 36,13% delle infezioni, che ha contribuito all'espansione delle minacce informatiche. Crescono anche le infezioni da malware in aumento del 131%, che passano da 848.000 casi nel 2023 a 1.960.000 nel 2024 (in termini di connessioni provenienti da dispositivi infetti verso sinkhole HTTP e non-HTTP).

In aumento del +7,5% rispetto al 2023, anche le famiglie malware rilevate che passano da 148 famiglie a 160.

Se nel 2023 si era manifestato un incremento costante nel corso dell'anno, nel 2024 le infezioni hanno mostrato una crescita più marcata nei mesi primaverili ed estivi, con un picco significativo a giugno, superiore a qualsiasi altro valore registrato nei due anni precedenti. Dopo questo massimo, nei mesi successivi le infezioni sono tornate all'andamento di partenza, suggerendo pertanto una stagionalità più accentuata rispetto agli anni passati.

Il forte aumento nel periodo estivo, indica la tendenza a sfruttare vulnerabilità specifiche in un periodo caratterizzato, da un lato, dal fatto che molte aziende operano con personale ridotto e quindi meno reattive nelle risposte agli incidenti, dall'altro, da un aumento delle attività in mobilità dovute ai più frequenti spostamenti esponendo maggiormente i dispositivi a reti meno sicure (Wi-Fi di aeroporti, strutture alberghiere, ecc…).

Nello specifico, tra maggio e giugno, è stato rilevato un incremento significativo di eventi riconducibili all'attività della botnet 911-socks5-proxy. A partire dal mese di luglio, si osserva una netta riduzione di tali attività, in seguito alle operazioni di blocco e smantellamento condotte dal Dipartimento di Giustizia degli Stati Uniti, che hanno portato all'arresto dei responsabili.

Dal grafico riportato sotto, che mostra la distribuzione percentuale di diverse famiglie di malware e botnet rilevate, emerge che il segmento più rilevante è occupato proprio dalla botnet 911-socks5-proxy, con un 36,13% del totale, evidenziando il suo impatto significativo e concentrato rispetto alle altre minacce.

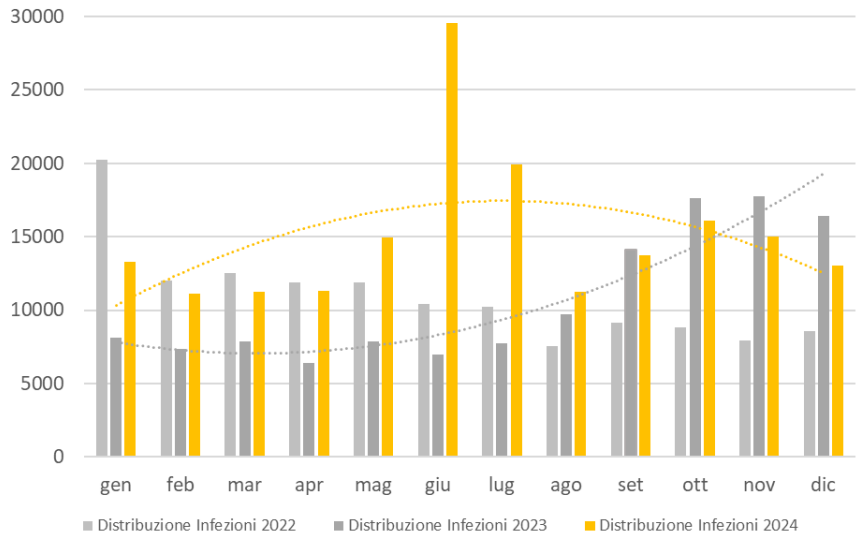


Figura 1 - Distribuzione temporale del numero di infezioni rilevate
(Dati Fastweb relativi agli anni 2022, 2023 e 2024)

La vulnerabilità 911 S5 è collegata al servizio proxy 911 S5, che offre una soluzione proxy SOCKS5 ai suoi utenti. I proxy SOCKS5 sono comunemente utilizzati per reindirizzare il traffico Internet tramite un server di terze parti, consentendo l'anonimato e la possibilità di aggirare le restrizioni geografiche. La vulnerabilità 911 S5 si verifica quando i criminali informatici sfruttano le debolezze nella configurazione o nel software del server proxy, portando all'accesso non autorizzato ai dati degli utenti o alla possibilità di utilizzare il servizio per attività dannose.

Segue la famiglia di malware "Adload", con il 18,16% del totale delle infezioni. Questo valore mostra una riduzione rispetto al 2023, quando Adload aveva raggiunto il 27% del totale delle infezioni. In particolare, ADload è un adware malevolo, ossia una applicazione potenzialmente indesiderata che, passando tramite applicazioni apparentemente legittime (come riproduttori video o agenti di supporto), viene scaricato tramite link maligni. Questi malware possono fungere da installatori per malware aggiuntivi o programmi potenzialmente indesiderati (PUP), reindirizzare gli utenti a siti web maligni o inserire annunci fraudolenti nelle pagine web.

Al terzo posto troviamo "Avalanche-Andromeda", responsabile del 15,68% delle infezioni. Questa piattaforma modulare è utilizzata per distribuire un'ampia gamma di varianti di malware (80 famiglie circa) tra cui ransomware, trojan bancari, robot spam e malware antifrode. Ciò che l'ha resa estremamente interessante per i cybercriminali è stata la sua proprio la sua natura modulare. Un primo modulo, per poche centinaia di dollari consente di acquistare il plug-in keylogger per leggere i dati della tastiera della vittima oppure, per una cifra poco superiore, il plug-in Formgetter, con il compito di acquisire i dati inviati dal browser web del computer infettato.

La famiglia di malware"Downadup", nota anche come "Conficker", si colloca in quarta posizione con 14,59% del totale. Questi virus, per propagarsi, sfruttano falle del servizio di rete Microsoft Windows e hanno l'obiettivo di prendere il controllo della macchina e rubare informazioni e credenziali all'utente, che rimane ignaro dell'attacco. Scoperti nel 2009, la loro diffusione è aumentata notevolmente grazie a una variabile silente distribuita probabilmente attraverso circuiti P2P dal 2021.

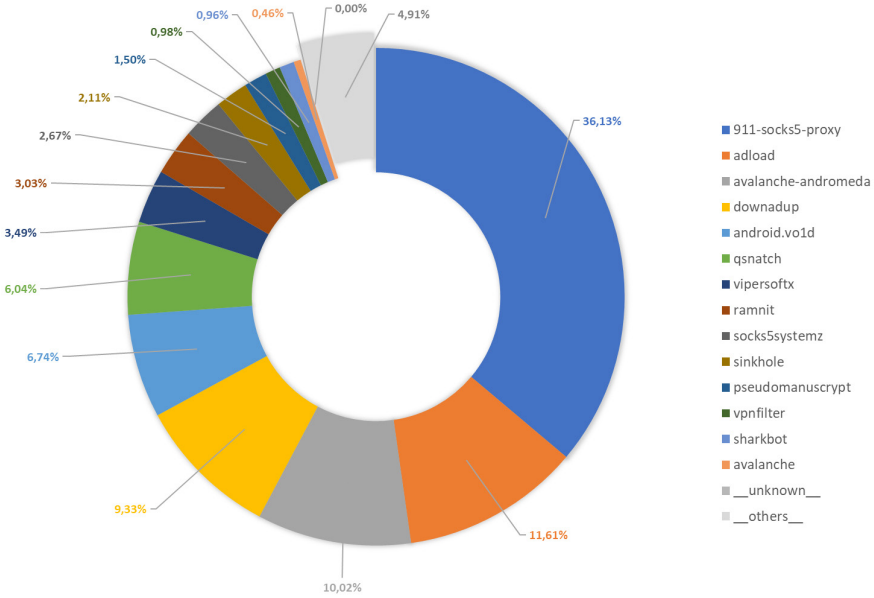


Figura 2 - Analisi delle infezioni rilevate *(Dati Fastweb relativi all'anno 2024)*

Come è visibile nel grafico di Figura 3 che mostra l'andamento mensile (per facilitarne la lettura è stato omesso l'andamento relativo alla botnet 911-socks5-proxy), emerge un aumento significativo delle infezioni tra agosto e novembre, con un picco particolarmente evidente per il malware **"Android.Vo1d"**, che raggiunge il valore massimo a ottobre. Questo andamento potrebbe essere legato all'aumento degli attacchi rivolti ai dispositivi mobili, spesso meno protetti rispetto ai sistemi desktop, con utenti che non utilizzano soluzioni di sicurezza avanzate come antivirus o sistemi di rilevamento delle minacce. Inoltre, il crescente utilizzo di app di terze parti e store non ufficiali aumenta il rischio di installazione di software malevolo così come l'aumento dell'uso dei dispositivi mobili per operazioni sensibili (pagamenti digitali, autenticazione 2FA, e-commerce) li rende un bersaglio più interessante per i cybercriminali. A questo si aggiunge anche, come riportato in alcuni articoli sul web, l'attacco di oltre 1,3 milioni di set-top box Android TV a livello globale sfruttando delle vulnerabilità spesso dovute all'uso di versioni obsolete del sistema operativo e alla mancanza di aggiornamenti di sicurezza.

"Adload" mostra un andamento crescente a partire da agosto, confermando la sua diffusione soprattutto nell'ultimo trimestre dell'anno. Questo fenomeno, in generale per tutti i tipi di infezioni mobile, dipende da una combinazione di fattori tra cui campagne di diffusione da parte degli attaccanti durante il periodo estivo, periodo in cui i dispositivi personali degli utenti sono più esposti, per poi intraprendere attività non autorizzate una volta preso possesso del dispositivo.

Nel 2023, le infezioni attribuite a famiglie sconosciute ("unknown") rappresentavano lo 0,18% del totale, mentre nel 2024 sono scese allo 0,12%. Questo dato conferma un miglioramento nella capacità di rilevazione delle minacce da parte degli esperti di sicurezza e dei sistemi di protezione zero-day, riducendo ulteriormente la quota di malware non identificati.

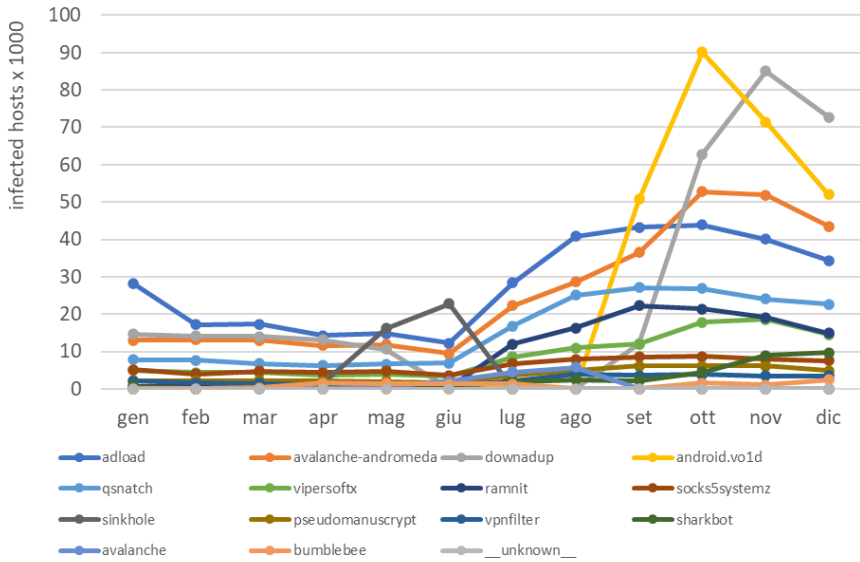


Figura 3 - Rilevazione mensile dei Malware *(Dati Fastweb relativi all'anno 2024)*

In sintesi, nel 2024 assistiamo a una ridefinizione delle principali minacce, con un aumento delle infezioni su dispositivi mobili e una riduzione della dominanza di Adload, a vantaggio di altre famiglie di malware in crescita.

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di Command and Control (C&C) rappresentano tipicamente sistemi compromessi utilizzati come macchina ponte per l'invio dei comandi ai dispositivi infetti da malware (bot) utilizzati per la costruzione delle botnet.

La tendenza degli ultimi anni è stata quella di utilizzare come C&C server geograficamente posizionati in paesi tipicamente non considerati "a rischio" o che generano una notevole mole di traffico. La logica è quella di rendere inefficaci i meccanismi di difesa basati sulla caratterizzazione geografica dei flussi malevoli e nascondere il più possibile queste connessioni persistenti con il centro di controllo.

Rispetto al 2019, quando circa l'80% dei centri di C&C si trovavano negli USA, nel 2024 si conferma la distribuzione globale più eterogenea già osservata nel 2023.

Gli Stati Uniti rimangono il paese con la maggiore concentrazione di C&C, con una quota del 50%, in crescita rispetto al 36% del 2023. Questo suggerisce un ritorno verso l'uso di infrastrutture consolidate in paesi con elevata capacità di traffico internet. Inoltre, il dato potrebbe essere influenzato anche dagli investimenti in infrastrutture per utenze residenziali in alcune aree geografiche del paese. Questo sviluppo ha portato a un incremento della superficie di attacco, offrendo agli attori malevoli un numero maggiore di dispositivi vulnerabili da compromettere e utilizzare per le loro operazioni illecite.

Nonostante una decrescita rispetto al 10% del 2023 Il Brasile continua a essere un punto di interesse, posizionandosi al secondo posto con il 6% dei C&C. Così come il Regno Unito, che nel 2023 occupava il secondo posto con l'11%, scende al terzo posto con circa il 4% dei C&C totali. Paesi come India, Corea del Sud, Lituania e Tailandia, registrano una crescita nella distribuzione di server malevoli.

A livello continentale, nel 2024 il Nord America ospita il 57% dei C&C, mostrando un incremento rispetto al 38% del 2023. L'Asia raggiunge il 18%, rispetto al 14% del 2023, confermando un aumento costante negli ultimi anni, mentre il Sud America si attesta al 10%. L'Europa mantiene una percentuale bassa attestandosi al 13%. Il restante traffico si distribuisce tra Oceania (1%) e Africa (1%).

L'aumento della concentrazione negli Stati Uniti e in Asia, insieme alla riduzione dell'Europa, suggerisce che gli attori malevoli stanno ridefinendo le strategie per garantire resilienza alle botnet. L'eterogeneità della distribuzione geografica, seppur

con un ritorno su alcuni paesi chiave, mostra come la geolocalizzazione da sola non sia più un meccanismo sufficiente per contrastare questi attacchi.

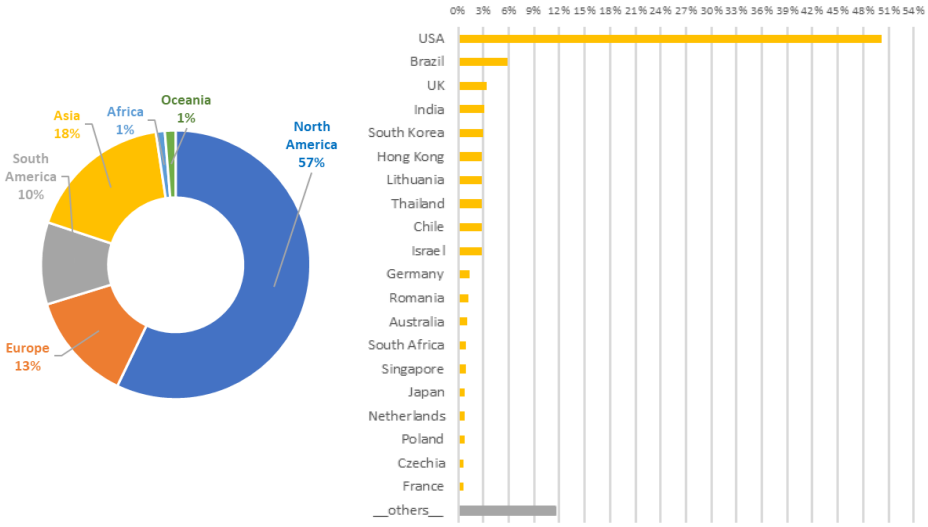


Figura 4 - Dislocazione dei centri di Comando e Controllo *(Dati Fastweb relativi all'anno 2024)*

Attacchi DDoS (Distributed Denial of Service)

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio.

Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete. Gli attacchi DDoS (Distributed Denial of Service) amplificano la portata di tali minacce, utilizzando delle botnet, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile.

In particolare, gli effetti di un attacco DDoS possono risultare estremamente dannosi sia a causa della potenza che possono esprimere, ma anche per le difficoltà insite nel poterli mitigare in tempi rapidi (se non attraverso la sottoscrizione di uno specifico servizio di mitigation).

Il mercato dei DDoSaaS (DDoS as a Service) continua a crescere e il costo del servizio si aggira sui 10-20$ mese per botnet in grado di erogare un attacco di 5-10 minuti a oltre 100Gbps.

Nel 2024, si assiste a un aumento di attacchi DDoS di tipo carpet bombing in cui il traffico malevolo viene distribuito su un ampio range di indirizzi IP appartenenti alla stessa rete target, invece di concentrarsi su un singolo IP. Questo rende l'attacco più difficile da rilevare e mitigare rispetto a un attacco DDoS tradizionale, poiché il traffico malevolo si mescola con il traffico legittimo e può passare inosservato ai sistemi di protezione.

Durante il 2024 sono stati rilevati 4.720 attacchi DDoS registrando un aumento del 100% rispetto al 2023 (2.368 attacchi). Si conferma, quindi, un trend ascendente iniziato nel 2023, con picchi significativi nei mesi estivi, in particolare a giugno e luglio, dove si è osservato un incremento straordinario del volume di attacchi.

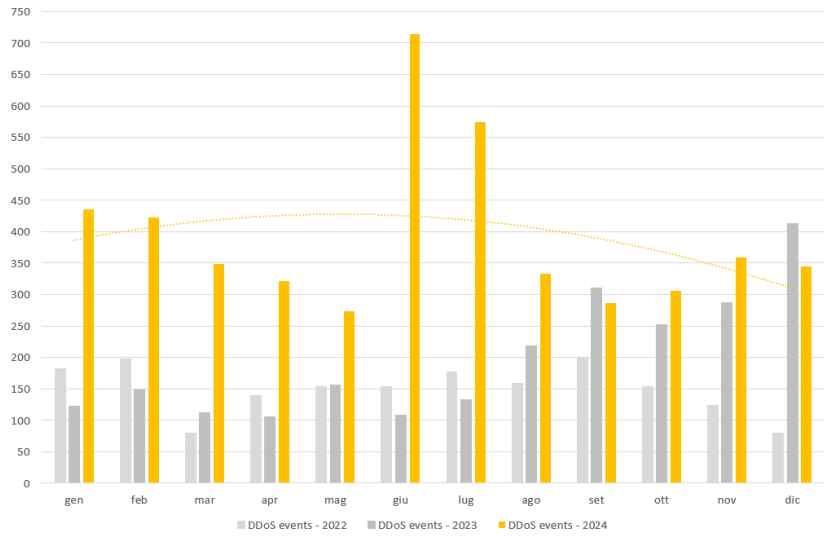


Figura 5 - Distribuzione mensile delle anomalie DDoS *(Dati Fastweb relativi agli anni 2022 – 2024)*

Come viene evidenziato nel grafico di **Figura 6**, a livello di attacchi, misurati attraverso gli aggregati mensili di banda, notiamo un incremento del 167% rispetto al 2023: questo è causato in primis da un incremento dei singoli eventi malevoli e da un aumento della disponibilità di banda dei sistemi compromessi grazie alla presenza degli stessi negli ambienti cloud o in aree geografiche dove la banda larga è più diffusa.

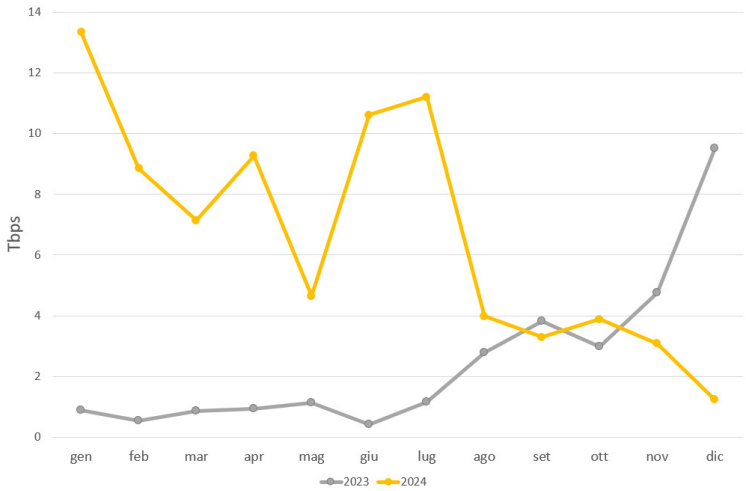


Figura 6 - Distribuzione mensile della banda aggregata degli attacchi DDoS *(Dati Fastweb anni 2023 e 2024)*

Dall'analisi della distribuzione dei target degli attacchi DDoS, sono stati individuati i settori merceologici maggiormente colpiti da questo tipo di attacchi.

Come evidenzia il grafico di **Figura 7**, il fenomeno riguarda un ampio numero di settori colpiti, tra i quali i più esposti si confermano essere la Pubblica Amministrazione (Government) con il 30,3% e il settore Finance & Insurance con il 18,18%, che insieme rappresentano quasi il 50% degli attacchi.

Finance & Insurance: sebbene un aumento degli attacchi rilevati rispetto al 2023 (+36%), ha contenuto questo fenomeno rispetto agli altri settori grazie a miglioramenti nei sistemi di difesa, con strategie più avanzate di mitigazione DDoS e maggiore preparazione del settore, che tradizionalmente investe molto in cybersecurity per contrastare le minacce. Inoltre, l'entrata in vigore della Digital Operational Resilience Act (DORA) nei primi mesi del 2025, emanata dalla Commissione Europea, ha incentivato il settore a strutturarsi ulteriormente, rafforzando le misure di protezione e resilienza operativa contro le minacce informatiche.

Government: si osserva un aumento significativo degli attachi, rispetto al 2023, passando da 560 a 1.430 (+155%) consolidandosi come il settore più colpito. Un fenomeno correlato alla crescente instabilità geopolitica e all'incremento delle attività di hacktivisti, oltre all' espansione del perimetro di attacco con la crescente disponibilità diservizi digitali a cittadini, imprese e PA.

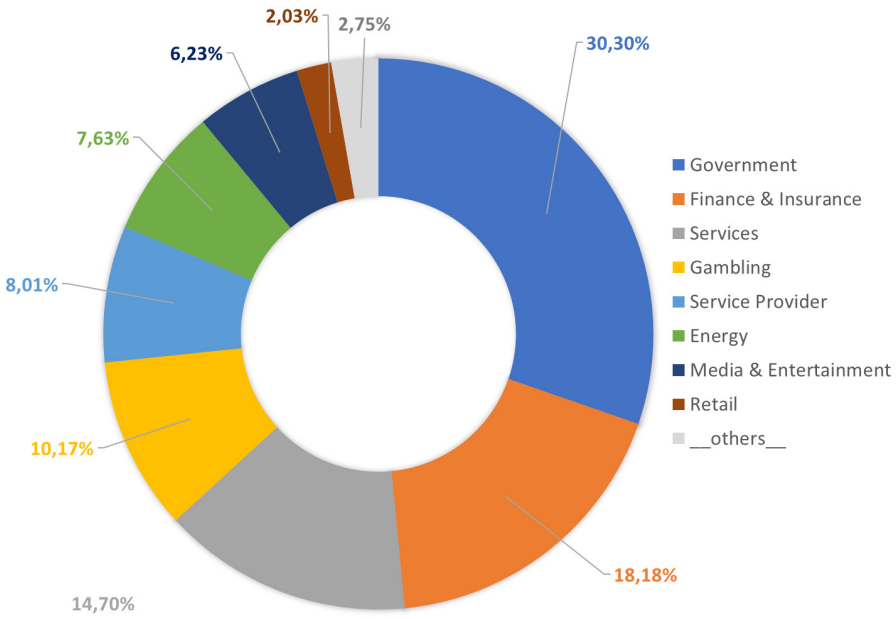


Figura 7 - Segmenti di mercato target di attacchi DDoS volumetrici *(Dati Fastweb relativi all'anno 2024)*

Un dato interessante riguarda anche gli altri settori tra cui Servizi (Services), che registra un aumento significativo del numero degli attacchi rispetto al 2023 (+250%), mantenendo una posizione rilevante tra i target più colpiti. Il Gambling segna un aumento rispetto all'anno precedente del +70%, restando anch'esso tra i settori più impattati. Anche gli altri comparti, tra cui Service Provider (+45%), Energy (+88%), Media & Entertainment (+268%) e Retail (+268%) evidenziano che il trend degli attacchi DDoS non esclude alcun segmento di mercato. Infine, il settore classificato come "Others" conferma che esistono attacchi diffusi anche in categorie meno rappresentate nel grafico, a dimostrazione di una minaccia che continua a evolversi e colpire trasversalmente diversi ambiti economici.

Di seguito viene riportata la distribuzione della banda media in Gbps di un attacco DDoS nel 2024.

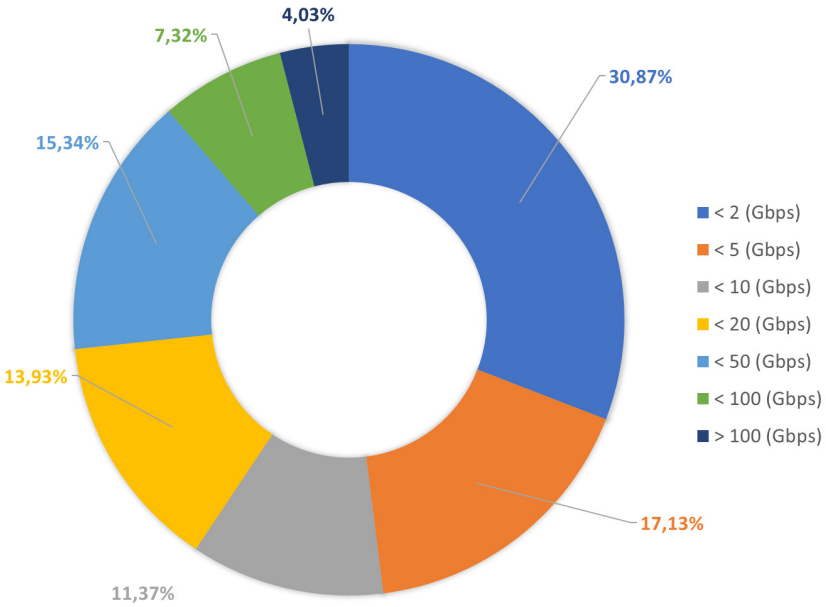


Figura 8 - Distribuzione della dimensione di un attacco DDoS *(Dati Fastweb relativi all'anno 2024)*

Il trend mostrato nei dati in tabella indica un significativo aumento del numero di attacchi DdoS nel 2024 rispetto al 2023, in tutte le fasce di dimensione, con una crescita particolarmente marcata per attacchi di maggiore intensità (>100 Gbps).:

Dimensione attacco	2024	2023
< 2 (Gbps)	1485	792
< 5 (Gbps)	824	621
< 10 (Gbps)	547	317
< 20 (Gbps)	670	229
< 50 (Gbps)	738	257
< 100 (Gbps)	352	106
> 100 (Gbps)	194	46

Questo fenomeno può essere giustificato da diversi fattori:

- aumento della diffusione delle botnet grazie anche alla crescita dei dispositivi IoT compromessi;
- l'uso di AI e automazione facilita la creazione di attacchi adattativi più sofisticati e mirati che eludono le tecniche di mitigazione;
- con l'espansione delle infrastrutture digitali (cloud, edge computing, 5G), le superfici di attacco aumentano e diventano più vulnerabili a offensive più grandi.

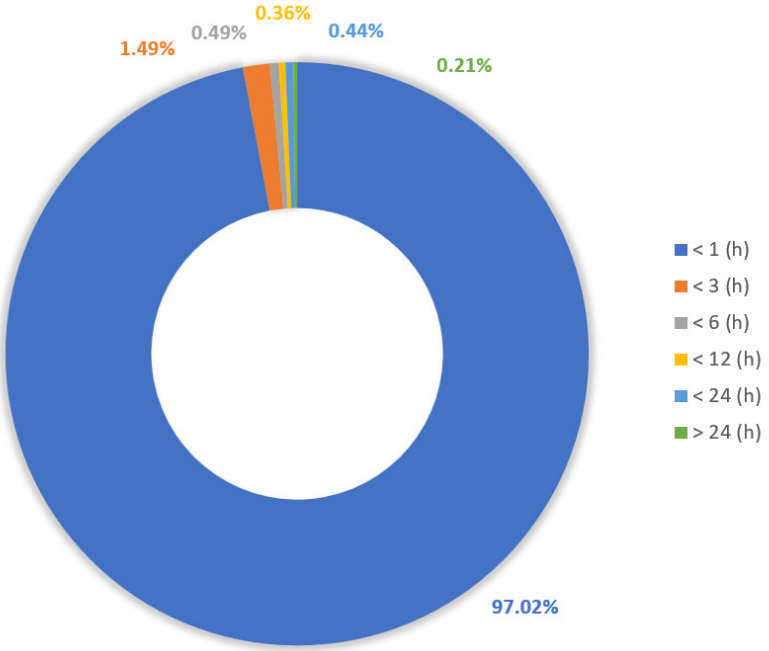


Figura 9 - Durata dei possibili attacchi DDoS *(Dati Fastweb relativi all'anno 2024)*

Nel 2024, oltre il 97% degli attacchi è durato meno di 1 ora (rispetto al 93% del 2023). La maggior parte degli attacchi con durate superiori a 1 ora resta limitata a valori molto ridotti: solo l'1,49% degli attacchi (rispetto al 2,58% del 2023) ha avuto una durata compresa tra 1 e 3 ore, mentre gli attacchi di durata superiore a 24 ore rappresentano appena lo 0,21% (in netta diminuzione rispetto al 2,44% del 2023).

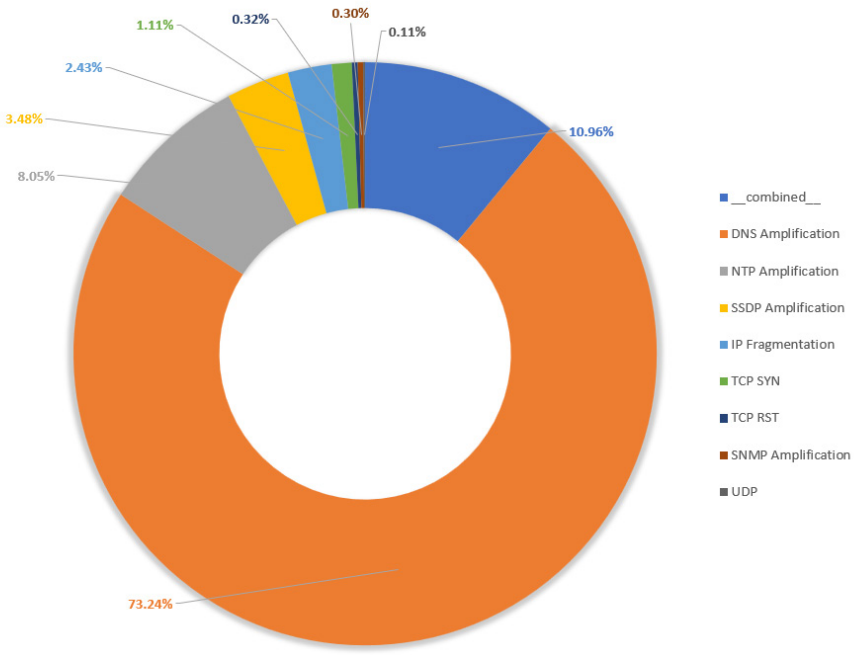


Figura 10 - Tipologie di attacchi DDoS *(Dati Fastweb relativi all'anno 2024)*

Nel 2024, la principale tipologia di attacco DDoS si conferma essere la "DNS amplification", che rappresenta il 73,24% degli attacchi, consolidando ulteriormente la sua crescita anche rispetto al 2023 (62,11%). La crescita è giustificata dall'alta efficacia dato che sfrutta server DNS aperti per generare traffico amplificato e sovraccaricare il bersaglio, difficoltà di mitigazione poichè il traffico DNS è essenziale per il funzionamento delle reti rendendone quindi più complessa l'individuazione degli attacchi senza impattare il traffico legittimo e ampia disponibilità di server vulnerabili poichè molti server DNS non sono ancora configurati correttamente per prevenire l'abuso.

Seguono la "NTP amplification" (ridotta all'8,05% vs 13,78% del 2023), la SSDP Amplification che sale al 3,48% (rispetto al 1,28% del 2023) e la "IP Fragmentation" che si attesta al 2,43% (lieve crescita rispetto al 2,24% del 2023). L'aumento della SSDP (*Simple Service Discovery Protocol*) potrebbe dipendere dal fatto che quest'ultimo è usato da dispositivi IoT e UPnP, molti dei quali risultano vulnerabili. Inoltre, l'aumento dei dispositivi IoT esposti in rete amplia la superficie di attacco.

La tecnica di attacco "IP Fragmentation" sfrutta il principio di frammentazione del protocollo IP. In effetti, il protocollo IP è previsto per frammentare i pacchetti di grandi dimensioni in differenti pacchetti IP che possiedono ognuno un numero sequenziale e un numero di identificazione comune. Una volta ricevuti i dati, il destinatario riordina i pacchetti grazie ai valori di spaziatura (in inglese offset) da questi contenuti. L'eccessiva dispersione di questi pacchetti nella fase di ricezione causa un rallentamento o blocco nel riassemblaggio. L' SSDP amplification è una tecnica di attacco DDoS (Distributed Denial of Service) che sfrutta il protocollo SSDP (Simple Service Discovery Protocol) per amplificare il traffico indirizzato a una vittima. Questo tipo di attacco è una forma di amplification attack, in cui un attaccante utilizza un piccolo volume di traffico per generare una quantità molto maggiore di dati inviati verso il bersaglio.

Gli attacchi più diffusi sono quelli che sfruttano il protocollo UDP, che permette di fare "rimbalzare" il traffico su server DNS o NTP impropriamente configurati. Grazie a questo "rimbalzo" e alle caratteristiche dei servizi DNS e NTP, l'attaccante ottiene il doppio scopo di nascondere i propri indirizzi IP (e quindi la propria identità e collocazione geografica) e di moltiplicare la portata dell'attacco: per ogni megabit di banda immesso dall'attaccante, la vittima può ricevere da 30 a 50 megabit di traffico indesiderato nel caso della DNS amplification, fino a 500 megabit nel caso della NTP amplification.

L'amplificazione del traffico è ciò che consente all'attaccante di rendere irraggiungibile il sito (o servizio) della vittima, saturandone la banda disponibile.

Infine, è da evidenziare come gli attacchi combinati (tecnica mista) si siano ridotti rispetto al 2023 passando dal 17,62% al 10,96% degli attacchi nel 2024. Questa riduzione riflette un'evoluzione nel panorama delle minacce DDoS. I miglioramenti delle difese con l'introduzione dell'AI e del machine learning contro attacchi complessi (, uniti alla preferenza degli attaccanti per vettori più diretti e ad alto impatto, spiegano questa tendenza. Nonostante ciò, gli attacchi combinati rimangono una minaccia significativa, poiché la loro complessità rende difficile contrastarli in modo sistematico.

In tale tipologia di eventi rientrano gli attacchi che variano nel tempo a seconda delle contromisure messe in atto dai cybersecurity specialist a difesa delle infrastrutture; in questi scenari si crea un'interazione indiretta tra attaccante e defense center: l'attaccante, nel momento in cui si accorge dell'inefficacia dell'azione, cambia modalità offensiva e chi difende deve essere pronto a cambiare la strategia di difesa.

Servizi critici esposti su internet

In questa sezione si riporta l'analisi sui server e device che espongono servizi pericolosi direttamente su internet e che risultano privi di livelli minimi di protezione. Questa rilevazione fornisce indicazioni sui volumi delle macchine facilmente attaccabili ed esposte a elevati rischi di compromissione.

Rispetto al 2023, anno in cui erano stati rilevati circa 38.000 sistemi esposti, nel 2024 si registra una diminuzione significativa, pari all'11%, con circa 33.800 sistemi esposti.

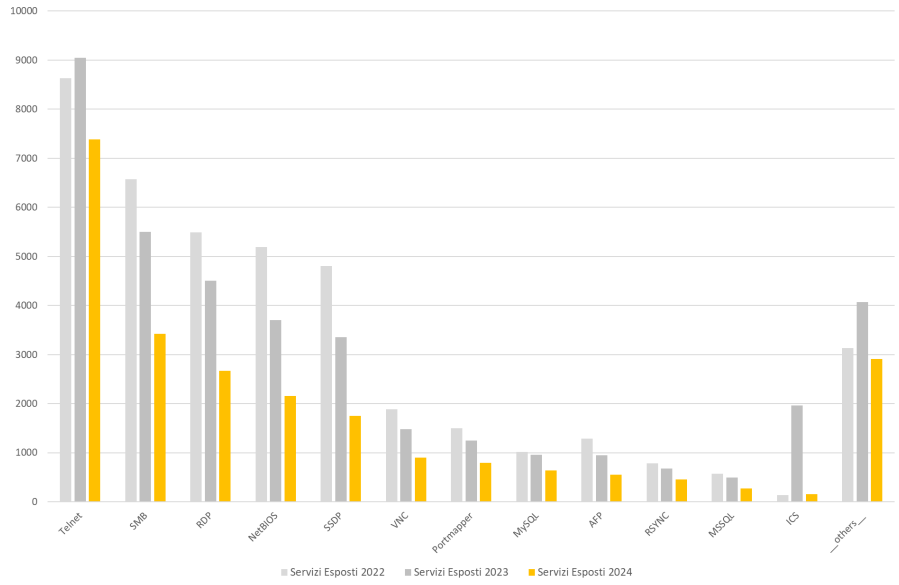


Figura 11 - Servizi critici esposti su Internet *(Dati Fastweb relativi agli anni 2022, 2023 e 2024)*

Rispetto al dettaglio dei servizi critici esposti su internet, possiamo notare come lo scenario risulta immutato rispetto agli anni precedenti: nuovamente, al primo posto tra i servizi esposti troviamo Telnet, il protocollo utilizzato per la gestione dei server remoti, accessibile da riga di comando. In termini percentuali, con 7.386 servizi esposti, registra un calo del 18,32% rispetto al 2023, ma resta il protocollo più frequentemente esposto in quanto obsoleto e insicuro e, quindi, facilmente sfruttabile per accessi non autorizzati.

Se nel 2022 abbiamo registrato per la prima volta un aumento dei casi di SMB (Server Message Block, protocollo di condivisione file di rete particolarmente utilizzato per veicolare i movimenti laterali da virus e che risulta secondo tra servizi pericolosi più esposti su internet), nel 2024 continua il trend discendente visto negli anni precedenti, con una riduzione significativa del 37,73% (con 3.426 servizi esposti).

Rimane al terzo posto l'RDP che presenta una diminuzione ancora più marcata, del 40,72%, passando da 4.509 (2023) a 2.673 servizi esposti nel 2024. Quest'ultimo è utilizzato per la connessione remota a un PC e che permette di prendere il controllo completo di un apparato se sfruttato dall'esterno.

In sintesi, questa riduzione testimonia un miglioramento generale nella postura di sicurezza delle organizzazioni, supportato da una combinazione di tecnologie, consapevolezza e obblighi normativi. Tuttavia, anche se in calo, questi servizi restano tra i più pericolosi e devono essere adeguatamente protetti dato che gli attaccanti trovano continuamente nuovi modi per sfruttare le vulnerabilità.

BlockList

Una blocklist è una lista nella quale vengono inseriti e catalogati indirizzi IP classificati principalmente come fonte di e-mail di SPAM o sorgente di generica attività malevola in internet. I motivi per cui si può venir inseriti nelle liste di blocco sono tra i più vari, ma i principali risultano:

- invio massivo di e-mail generate da un indirizzo IP non autorizzato a eseguire questo tipo di attività per conto dell'organizzazione mittente;
- nel testo o nell'oggetto delle e-mail inviate sono presenti caratteri e simboli in genere utilizzati nelle mail di SPAM;
- il PC è infetto da virus che invia autonomamente e ciclicamente e-mail pericolose/indesiderate e/o che esegue tentativi di exploit verso target esterni su internet.

Nel 2024, le rilevazioni effettuate mostrano che circa 1.500 IP sono stati inseriti almeno una volta nelle blocklist. Il dato nel 2024 (-6,25%) conferma il calo rispetto al 2023, dove si erano registrati circa 1.600 azioni di blocklisting, e risulta nettamente inferiore al dato del 2022, pari a 3.400 azioni di blocklisting (-55,88%).

La rilevazione mostra la tendenza in discesa, iniziata nel 2022, come evidenzia il grafico di **Figura 12**.

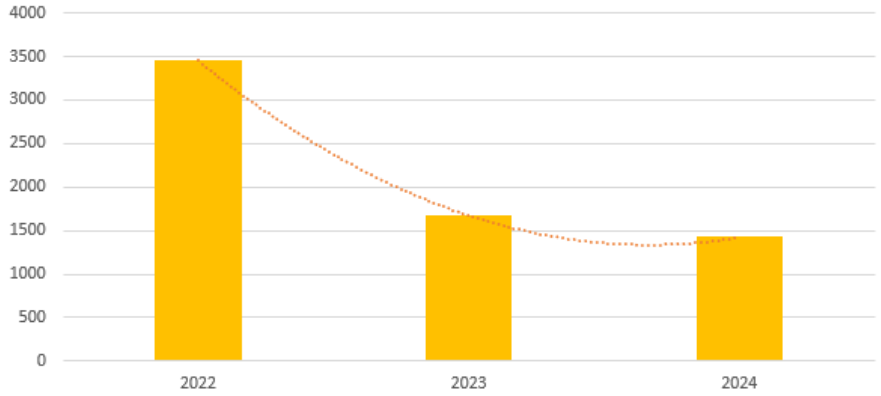


Figura 12 - Quantità di IP in Blocklist dal 2022 al 2024

Un dato rilevante che emerge dal grafico riportato sopra è la chiara proporzione lineare tra il numero di infezioni e il numero di host in blacklist nelle principali città italiane nel 2024.

Milano, Roma e Napoli confermano, come nel 2023, il loro primato per numero di dispositivi infetti (giallo) e host inseriti in blocklist (rosso), con Milano che domina significativamente in entrambe le categorie.

Nelle città di media grandezza, come Torino, Firenze e Bari, il rapporto tra dispositivi infetti e host in blocklist rimane costante, pur registrando volumi complessivamente inferiori rispetto alle prime tre città.

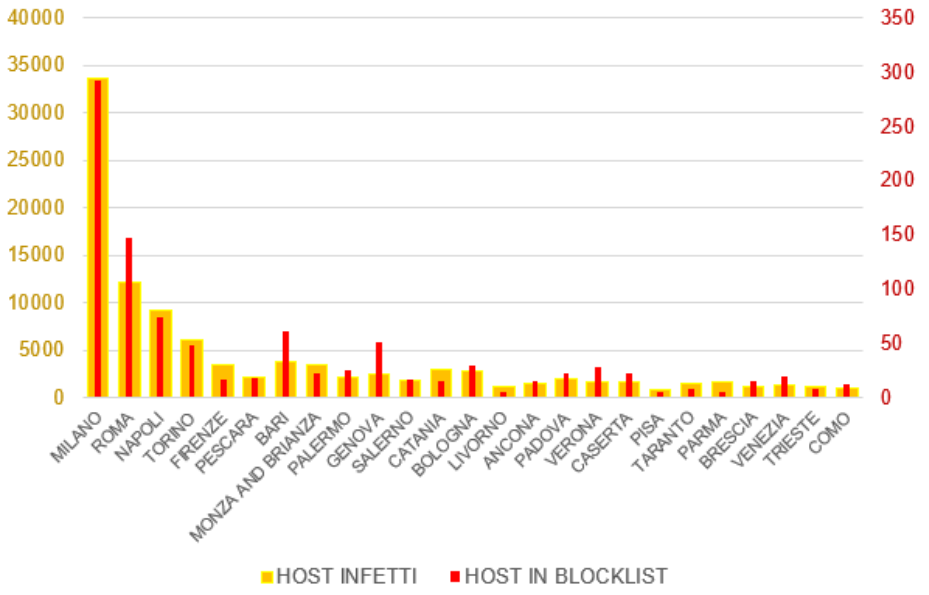


Figura 13 - Relazione tra dispositivi in Blocklist e infezioni rilevate per città *(Dati Fastweb relativi all'anno 2024)*

A livello nazionale, le differenze territoriali nel 2024 confermano quanto osservato negli anni precedenti per regioni del Nord Italia che si mantengono in testa con il 55,63% delle infezioni totali (55,10% nel 2023), seguite dal Sud con il 23,49% (in aumento rispetto al 18,45% nel 2023) e dal Centro con il 20,89% (in calo rispetto al 26,45% nel 2023).

Nonostante la predominanza del Nord, si evidenzia una distribuzione lievemente più equilibrata rispetto agli anni precedenti. Questa distribuzione rispecchia la maggiore concentrazione di dispositivi connessi e infrastrutture IT nel Nord Italia, che rimane l'area più esposta e colpita dal fenomeno delle infezioni informatiche.

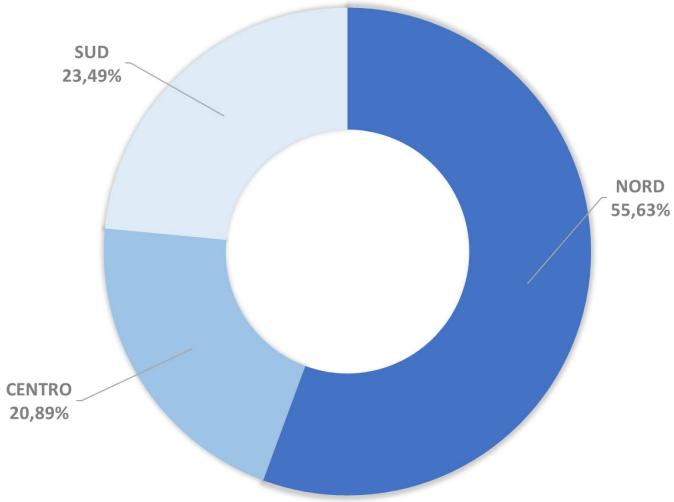


Figura 14 - Distribuzione geografica dei server in blacklist *(Dati Fastweb relativi all'anno 2024)*

Sicurezza applicativa Web

Di seguito un'analisi sul mondo delle vulnerabilità e degli attacchi rilevati sulla rete di Fastweb attraverso tecnologie di tipo Web Application Firewall e bloccati dai servizi di cyber sicurezza attivi.

I campioni analizzati relativi ai dati del 2024 confermano la tendenza già osservata nel 2023, con SQL Injection (attacco diretto ad avere accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database) che rimane l'attacco più diffuso, rappresentando il 25,96% del totale (rispetto al 14,27% del 2023).

Tuttavia, rispetto al 2023, si registra una crescita significativa degli attacchi di tipo Directory Traversal (attacco utile ad avere accesso a file in directory in cui non si è autorizzati ad accedere), che ora costituiscono il 20,49% del totale (rispetto al 14,24% del 2023), evidenziando un aumento delle minacce mirate a ottenere accesso non autorizzato ai file di sistema.

Gli attacchi di tipo Cross Site Scripting o XSS (iniezione di codice finalizzato all'esecuzione di azioni non previste dallo sviluppatore o che costringe l'utente a eseguire azioni non volute) mantengono una quota significativa del 14,77%, in lieve aumento rispetto all'anno precedente.

Gli attacchi RFI Injection (6,96%) e File Injection (6,70%) risultano essere presenti tra le principali minacce, evidenziando una crescita rispetto al 2023. La **Remote File Inclusion** (RFI) è una vulnerabilità che consente agli aggressori di includere file esterni o remoti all'interno di un'applicazione web. La **File Injection** è una vulnerabilità in cui un attaccante riesce a caricare o manipolare file non autorizzati sul server, spesso sfruttando funzioni di upload o inclusione di file. Diversamente dall'RFI, qui l'attaccante carica file direttamente nel sistema senza doverli richiamare da una posizione remota.

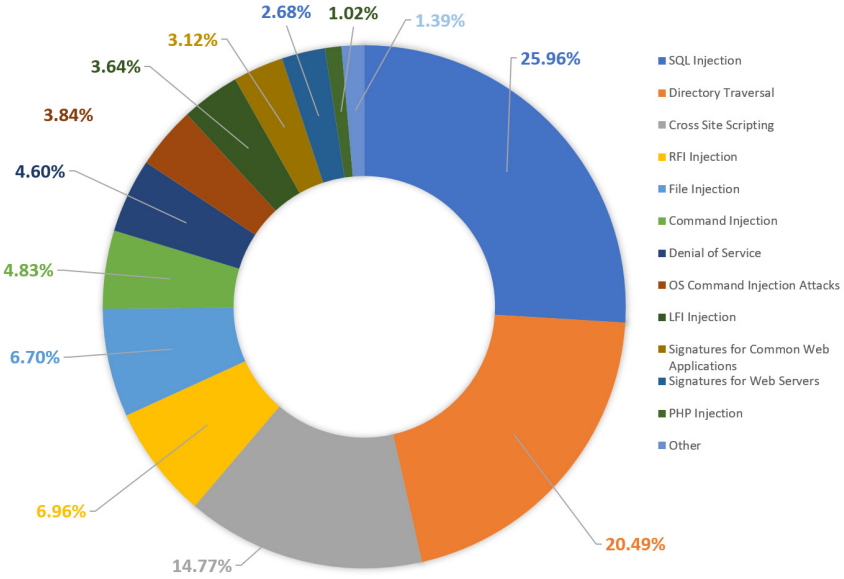


Figura 15 - Tecniche di attacco applicativo rilevate dai WAF del segmento Enterprise *(Dati Fastweb anno 2024)*

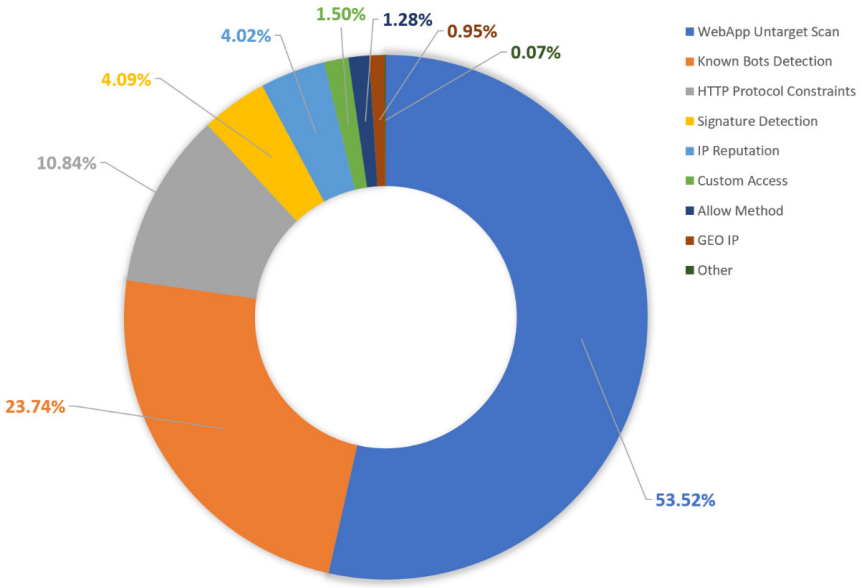


Figura 16 - Tipologie di contromisure maggiormente intervenute a protezione degli attacchi applicativi *(Dati Fastweb relativi all'anno 2024)*

Nel 2024 osserviamo un elevato numero di attacchi informatici provenienti dagli Stati Uniti (in linea con il 2023), seguiti dall'Italia, che passa dal quarto al secondo posto (in precedenza occupato dalla Germania, che scende in quarta posizione). Al terzo posto si posizionano i Paesi Bassi, che entrano per la prima volta in classifica.

Per quanto riguarda il posizionamento dell'Italia, riteniamo questo fenomeno legato al tentativo da parte degli attaccanti di bypassare il filtraggio degli indirizzi IP basato sulla posizione geografica, utilizzando le infrastrutture dei cloud provider presenti in Italia e botnet composte da dispositivi connessi su tutto il territorio nazionale.

Rispetto al 2024, pur sparendo alcune aree geografiche, dovute alla restrizione applicate, gli attacchi informatici rimangono sostenuti e in continua crescita: compaiono i primi blocchi disposti mediante l'uso del IA (Intelligenza Artificiale).

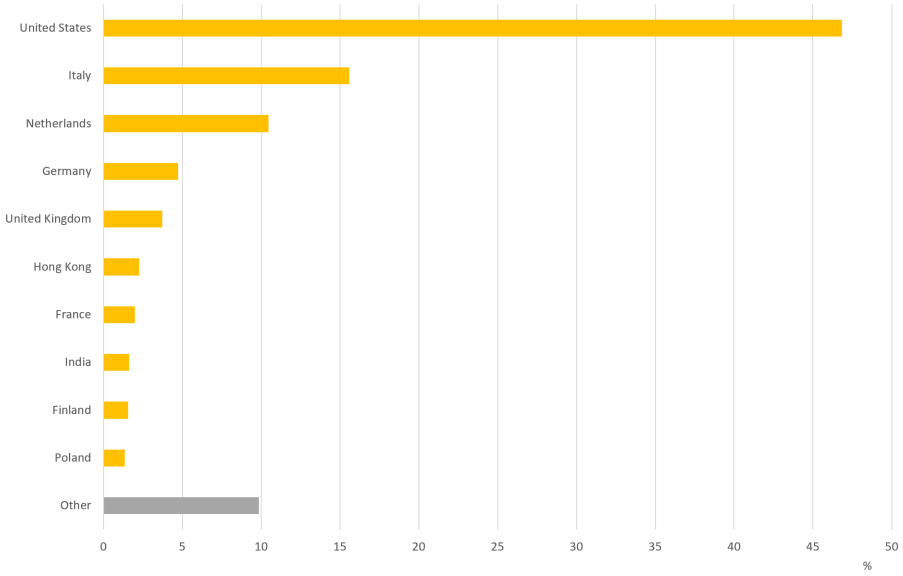


Figura 17 - Dislocazione delle sorgenti di attacco applicativo rilevate dai WAF del segmento Enterprise *(Dati Fastweb relativi all'anno 2024)*

Trend e minacce in ambito Mail

In questa sezione vengono riportati i principali trend del 2024 rilevati da Fastweb nell'ambito Mail Security.

Il vettore principale utilizzato per veicolare attacchi tramite e-mail è rappresentato dall'utilizzo di URL malevoli. Considerando l'andamento annuo, la presenza diretta di allegati malevoli all'interno delle e-mail, appare in diminuzione (-2,5% sul 2023) anche se i «*malware threats*» risultano in aumento rispetto all'anno passato (+8,6% sul 2023). La spiegazione del fenomeno è data dal fatto che la minaccia nella e-mail è presente nel formato URL su cui l'utente è indotto a fare click. Bisogna precisare che in questa seconda fase il file scaricato risulta essere un «*loader*» ovvero un intermediario che ha il compito di superare eventuali contromisure per poi scaricare il malware finale.

In crescita è la classificazione delle «Minacce Individuali». Questo conferma la tendenza dell'ultimo periodo dove differenti attori malevoli singolari, non noti oppure emergenti, si sono strutturati per veicolare mail malevole. Diviene dunque comples-

sa, proprio per la mancanza di visibilità, riuscire ad attribuire l'evento malevolo a uno specifico *Threat Actor* e/o determinare gli elementi in comuni di una minaccia.

Resta comunque salda, anche se in diminuzione rispetto all'anno precedente (-5,8% sul 2023), una percentuale relativa alle «Campagne», dove il fattor comune è il tema e/o l'identità dei soggetti da colpire.

Le tipologie di minacce sono in continua crescita, spinta anche dall'uso dell'intelligenza artificiale (IA) sintomo che gli attaccanti escogitano sempre nuove modalità per eludere i sistemi di monitoraggio.

Figura 18 - KPI Minacce Mail 2024

Ad eccezione di *Phorpiex*, la distribuzione delle minacce che hanno come finalità l'esfiltrazione di informazioni e dati delle vittime (denominate genericamente «*info-stealer*») è predominante, tuttavia si identifica anche un aumento dell'utilizzo dei «loader» generici per veicolare componenti malware terzi con diverse finalità.

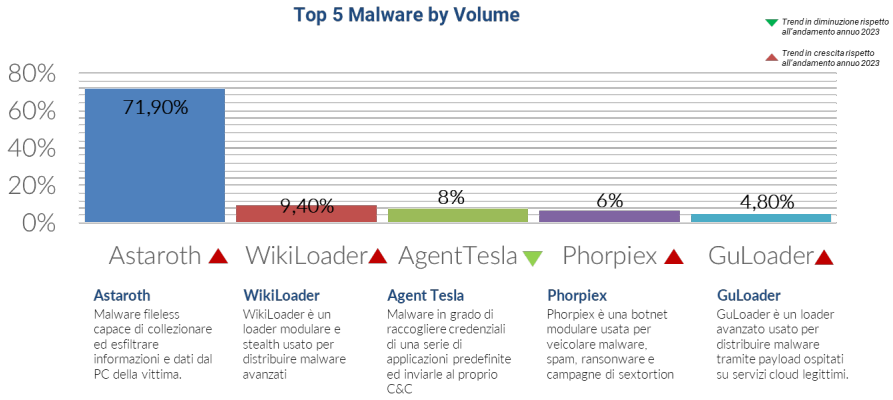


Figura 19 - Top 5 Malware per volume 2024

A livello di metodologia utilizzate dai cybercriminali nel veicolare le minacce via e-mail la tecnica di social engineering, che aveva fatto registrare un aumento notevole nell'anno 2023, riporta una tendenza in decrescita facendo registrare volumi medi più bassi. Questo andamento giustifica il miglioramento dei presidi di sicurezza nel riconoscere minacce mail afferenti a questa tipologia.Il social engineering è infatti una tecnica di attacco cyber sempre più sofisticata grazie all'AI, in grado di colpire direttamente persone o dipendenti di un'azienda. Questa consiste nell'ingannare le persone toccando leve psicologiche e comportamentali. Rispetto alle altre modalità di cybercrime il social engineering non sfrutta le falle dei sistemi informatici, ma utilizza metodi che hanno come scopo quello di ottenere informazioni personali tramite l'inganno.

Il grafico di **Figura 21** rappresenta una classificazione delle minacce e-mail le cui modalità di attacco variano dall'installazione di software malevolo, al furto dei dati personali degli utenti.

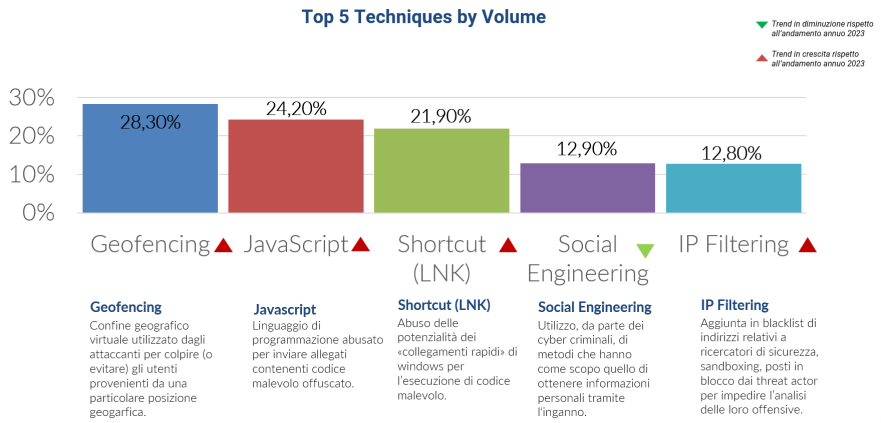


Figura 20 - Top 5 tecniche per volume 2024

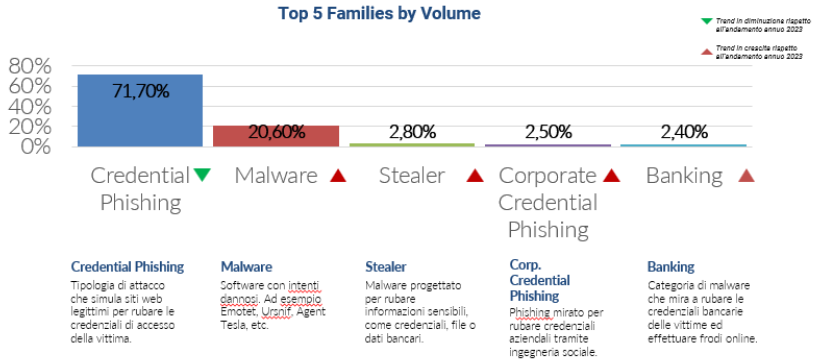


Figura 21 - Top 5 famiglie di minacce per volume 2024

I dati mostrano che il **Credential Phishing** rappresenta la minaccia più diffusa, costituendo il 71,7% delle attività malevole analizzate, nonostante un trend in diminuzione rispetto all'anno precedente. Questo attacco si basa su siti web fraudolenti che simulano portali legittimi per sottrarre credenziali di accesso, sfruttando l'ingenuità e la fiducia delle vittime.

In netto aumento, invece, le campagne basate su **Malware**, che coprono il 20,6% delle minacce. Questi software dannosi, come *Astaroth, WikiLoader* e *Agent Tesla*, vengono utilizzati per scopi fraudolenti come il furto di dati sensibili e il sabotaggio aziendale. La loro crescita evidenzia un'attenzione maggiore dei cyber criminali verso strumenti più distruttivi e personalizzabili.
Anche le attività legate agli **Stealer** e al **Corporate Credential Phishing** stanno crescendo, seppur con volumi inferiori. Gli **Stealer** (2,8%) sono progettati per carpire informazioni come credenziali e dati finanziari, mentre il **Corporate Credential Phishing** (2,5%) si concentra su attacchi mirati al personale aziendale, sfruttando tecniche di ingegneria sociale per ottenere accesso a risorse aziendali strategiche.

Infine, la categoria **Banking Malware** (2,4%) seppur non si classifichi più tra le prime minacce, il suo andamento in crescita rispetto al 2023 continua a rappresentare un rischio per il furto di credenziali bancarie e la frode online.

Questi dati evidenziano come la sicurezza aziendale debba evolversi costantemente per affrontare minacce sempre più diversificate e sofisticate, con un'attenzione particolare alla formazione del personale e all'adozione di tecnologie avanzate di protezione.

Il team Fastweb CSIRT&SOC, nel corso dell'anno 2024, tramite i sistemi di monitoraggio del presidio e-mail, ha attenzionato un volume di messaggi malevoli afferenti a diversi threat actor. Come è possibile osservare dal grafico sottostante, i principali sono stati:

TA569 (SocGholish)

TA569, noto anche come SocGholish, è un gruppo di cybercriminali noto per le sue attività di attacco mirato e campagne di phishing. Questo attore minaccioso sfrutta frequentemente software legittimi e vulnerabilità nei browser per diffondere malware, spesso utilizzando tecniche di social engineering. SocGholish è noto per distribuire malware attraverso siti web compromessi che sembrano provenire da fonti affidabili, come aggiornamenti di software. Gli attacchi sono principalmente rivolti a utenti aziendali e istituzioni, con l'obiettivo di rubare credenziali e compromettere sistemi. Le sue operazioni includono anche attacchi "*fileless*", difficili da rilevare.

TA544 (Hastur / Narwhal Spider)

TA544 rappresenta un gruppo di tipo Cyber Crime attivo almeno dalla prima metà del 2017 e presumibilmente originario dell'Europa Orientale.

È noto per l'uso di campagne di phishing altamente mirate che sfruttano e-mail ingannevoli per infettare le vittime con malware come Ursnif, un trojan bancario. I suoi obiettivi principali includono organizzazioni finanziarie, aziende e utenti aziendali. Il gruppo utilizza anche tecniche di social engineering per ingannare le vittime e raccogliere informazioni sensibili. TA544 è legato a un'infrastruttura che spesso cambia per evitare la rilevazione e continuare a operare sotto i radar.

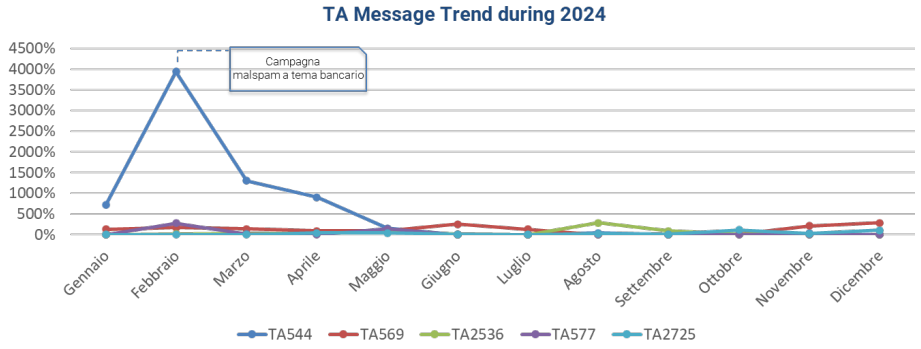


Figura 22 - Threat Actor durante il 2024

Per quanto concerne l'intelligenza artificiale, possiamo notare come l'utilizzo dell'AI abbia impattato sia il lato offensivo che difensivo dell'e-mail security.

Grazie a strumenti che sfruttano la generative AI i threat actor possono generare contenuti personalizzati direttamente nella lingua della vittima, o tradurre testi in maniera sempre più accurata, rendendo più complicato il riconoscimento di un tentativo di phishing anche quando proveniente da un attore straniero. Inoltre, avanzati algoritmi di machine learning permettono di incrociare e accorpare dati provenienti da più piattaforme, creando così una profilazione più completa della vittima e permettendo attacchi più mirati.

Nel corso del 2024 l'utilizzo di tecniche di intelligenza artificiale ha consentito di ridurre le competenze tecniche necessarie per sviluppare e distribuire elementi nocivi anche via mail. Questa riduzione della barriera d'ingresso ha portato a un crescente numero di minacce individuali.

L'utilizzo dell'intelligenza artificiale ha anche permesso di migliorare l'efficacia degli strumenti di detection e prevention. Riconoscendo determinati pattern, l'intelligenza artificiale è in grado di contribuire a identificare possibili minacce all'interno degli

allegati delle mail, riconoscere i segni caratteristici degli attacchi di social engineering e predire possibili minacce emergenti e zero day.

Infine, grazie all'AI, gli strumenti di security sono in grado di raccogliere un maggior numero di informazioni sui threat actor e di distinguere con maggiore precisione le individual threats dalle campaigns. Questo è evidenziato dal calo nel numero di campaigns identificate e nella crescita delle individual threats rispetto al 2023.

AI Trends in Email Security

Trend e nuovi fenomeni in ambito Frodi

I principali fenomeni di frode osservati da Fastweb nel 2024 sono ancora le frodi da sottoscrizione con furto d'identità e alcune frodi tecniche legate al fenomeno del CLI Spoofing e del social engineering.

Come noto, le ***frodi da sottoscrizione*** con furto d'identità sfruttano i dati anagrafici e i documenti di identità di cittadini inconsapevoli, per sottoscrivere contratti di servizi e/o acquistare prodotti, non solo in ambito Telco. Spesso i furti di identità sono utilizzati per attivare contratti di telefonia mobile prepagati, con sottoscrizioni che avvengono presso canali di vendita fisici.
Le contromisure messe in atto e i monitoraggi continui limitano il fenomeno, ma i truffatori riescono, in alcuni casi, ad aggirare, in modo artificioso, i controlli e i sistemi informativi, cagionando danni a cittadini ignari, che devono tutelarsi tramite denuncia per furto di identità.

Rispetto al 2023, Fastweb ha rilevato una riduzione dei fenomeni di frode che coinvolgono i dati bancari di soggetti terzi, per l'attivazione e il pagamento dei servizi.

Il furto di identità miete vittime in tutte le fasce d'età dei cittadini, con una incidenza superiore al 30% - 35% per le Generazioni "boomers" (nati nel periodo 1946 – 1964) e "Gen X" (nati nel periodo 1965 – 1979) , senza distinzioni sul Paese di origine, come mostra il grafico sottostante.

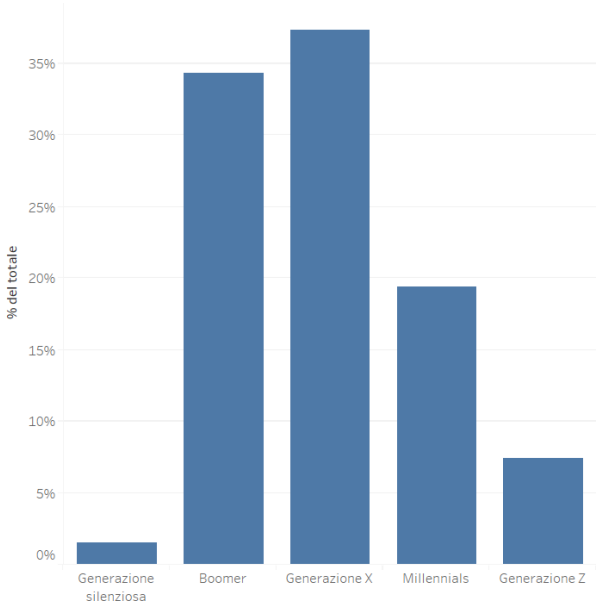


Figura 23 - Distribuzione vittime di furto identità per Generazione

Di contro Fastweb ha osservato una riduzione dei tempi di rilevazione e denuncia del furto di identità subito, da parte delle vittime. Il grafico sottostante mostra che la scoperta avviene entro 12 mesi dal fatto, per quasi il 60% dei casi; rilevante è il fatto che quasi il 15% dei casi viene scoperto dopo oltre 5 anni dalla sottoscrizione fraudolenta (**Figura 24**).

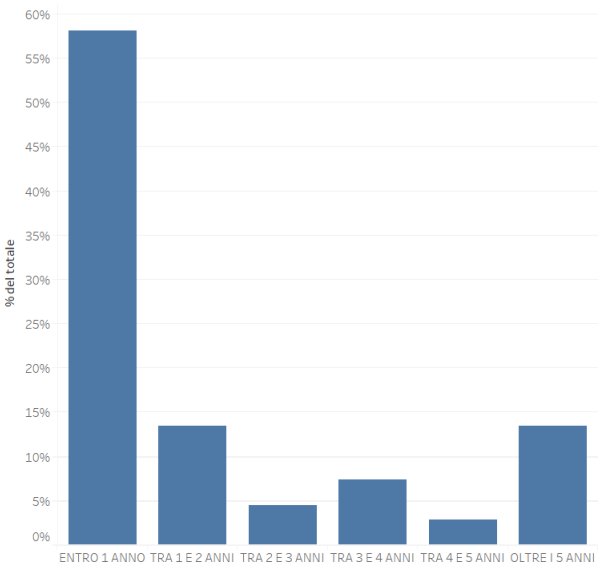


Figura 24 - Distribuzione tempi di rilevazione furto identità

Nell'ambito delle ***frodi tecniche*** specifiche per il mondo Telco, il CLI spoofing utilizzato per chiamate commerciali aggressive e robocalling, rimane il fenomeno con i volumi più significativi, in termini di numero di chiamate e tentativi di chiamate verso gli utenti.

Per cercare di ottenere in ogni modo una risposta, i truffatori cambiano numero di telefono chiamante con notevole rapidità e frequenza, diventando così più difficilmente individuabili. Non è infrequente l'utilizzo di numerazioni reali, assegnate a grandi aziende o a singoli utenti, con grave danno agli stessi.

Da agosto 2024, Fastweb ha osservato l'incremento di truffe che combinano una chiamata da numero estero, in genere europeo, con successivi contatti via whatsapp, allo scopo di impossessarsi di account whatsapp e Telegram (*account takeover)*. Questi fenomeni, oltre a danneggiare utenti poco accorti o poco eruditi in ambito cyber-fraud, arrecano danno di immagine anche gli operatori telco.

Sempre nella seconda parte dell'anno, Fastweb ha rilevato e bloccato un fenomeno importante di SMS commerciali (cosiddetti A2P – Application to Person) consegnati in modo fraudolento da player di mercato che cercano in ogni modo di bypassare i costi di interconnessione.

Questi fenomeni rappresentano un danno economico per le Telco e possono risultare commercialmente poco efficaci, se l'utente che li riceve non riconosce il mittente.

Il team Antifrode di Fastweb, insieme alle funzioni Tecnologiche e di Security è costantemente impegnato a irrobustire le azioni di prevenzione delle frodi; il monitoraggio continuo e la rapida reaction in caso di detection assicurano un buon contrastano di queste attività malevole.

Tattiche di attacco e gestione degli Incident

Le rilevazioni di 7Layers mostrano come le tattiche utilizzate dai cyber attaccanti siano differenziate tra loro, come si evince dal grafico sotto.

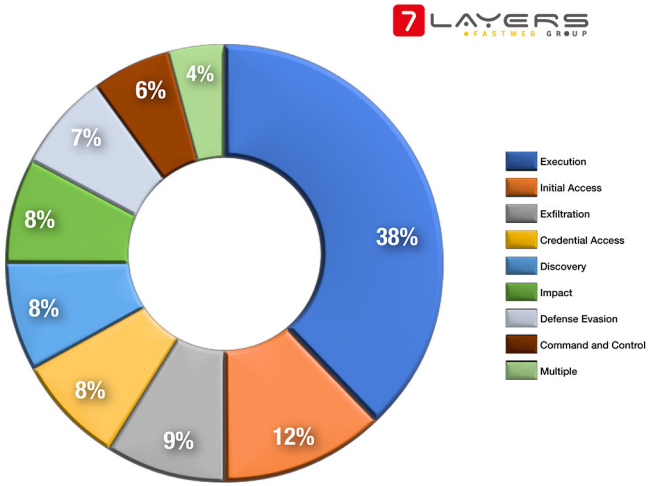


Figura 25 - Tattiche di attacco più comunemente utilizzate sulla base dei dati di agent EDR, Firewall perimetrali, Sonde IDS e Identity Protection

Nel corso dell'anno 2024, le analisi di 7Layers hanno evidenziato una prevalenza significativa di alcune specifiche tattiche MITRE relativamente agli attacchi informatici monitorati. In particolare, le prime quattro tattiche per frequenza di osservazione sono state:

Execution (38%): Questa tattica, indica l'esecuzione di codice dannoso, ed è risultata essere la più diffusa. E' stato osservato un aumento significativo rispetto allo scorso anno di alert associati ad attività di esecuzione malware. Questo può essere associato

anche a cattive abitudini da parte degli utenti finali che possono essere corrette anche tramite training mirato. In questo caso l'utilizzo di soluzioni EDR aiuta monitorare a prevenire potenziali compromissioni che possono rivelarsi anche molto dannose.

Initial Access (12%): Gli attacchi che sfruttavano tecniche di accesso iniziale sono in linea con il trend degli ultimi anni. L'Accesso Iniziale si riferisce alle tecniche che sfruttano diverse vie d'ingresso per ottenere un primo accesso non autorizzato a una rete. Queste tecniche includono il phishing mirato e l'exploit di vulnerabilità nei server web pubblici. L'accesso iniziale può fornire agli attaccanti un punto di appoggio persistente, come l'utilizzo di account compromessi o l'accesso a servizi remoti.

Exfiltration (9%): Una volta ottenuto l'accesso al sistema, gli attaccanti si focalizzano sull'esfiltrazione dei dati. E' ststo osservato un aumento di attacchi che sfruttavano protocolli legittimi o tool leciti, per trasferire dati rubati verso server di Command and Control.

Credential Access (8%): L'accesso alle credenziali è stato un altro obiettivo primario degli attaccanti. E' stato rilevato un aumento di eventi mirati a sfruttare malware per rubare le credenziali degli utenti, come password e token di autenticazione. Queste credenziali sono state poi utilizzate per accedere o tentare di accedere ad altri sistemi o servizi esposti come terminatori VPN o webmail.

I numeri sopra riportati derivano dalle attività di Realtime Monitoring e Incident Handling effettuate dal team di analisti di 7Layers e sono possibili grazie ai dati raccolti da fonti come agent EDR, Firewall perimetrali, sonde IDS e servizi di Identity Protection.

Il sistema MDx di 7Layers ha dimostrato la sua efficacia nel 2024, registrando un aumento del 100% degli eventi e degli alert gestiti. Questo risultato è stato reso possibile anche grazie all'ampliamento della superficie di monitoraggio, oltre che all'introduzione di nuove soluzioni tecnologiche che ha permesso quindi di intercettare un numero sempre maggiore di minacce.

L'espansione dei servizi offerti sul mercato e delle fonti di dati provenienti dalle aziende clienti, ha permesso a 7Layers di tracciare un quadro sempre più preciso delle tattiche sfruttate dagli attaccanti segnando un significativo aumento di eventi e di alert gestiti rispetto al 2023. Grazie anche all'utilizzo dell'AI da parte degli analisti, è possibile individuare e gestire con maggiore precisione gli eventi malevoli realmente impattanti ("true positive") e scartare i falsi positivi.

Attività e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica nel 2024

Le forze di polizia e le organizzazioni criminali nel cyberspazio: questioni etiche, uso dell'intelligenza artificiale e il ruolo di aziende e mondo accademico

Sul fronte della criminalità cibernetica, che, come ogni altra attività umana, si integra nel dominio digitale, la Polizia Postale ha affrontato molteplici sfide nel 2024. Il confronto, complesso e in continua evoluzione, tra le forze di polizia e le organizzazioni criminali nel cyberspazio, produce scenari sempre nuovi e spesso con importanti ripercussioni nei confronti degli utenti della rete, dai singoli cittadini alle aziende, comprese le infrastrutture strategiche e i servizi essenziali. Questo scontro va oltre le tecnologie impiegate, richiedendo un delicato equilibrio tra sicurezza, libertà individuali e giustizia. In questo contesto, la tecnologia avanzata (IA) ha assunto un ruolo centrale, presentando da una parte innegabili opportunità e dall'altra la necessità di un'attenta analisi nell'uso consapevole ed etico di questa risorsa.

Le organizzazioni criminali, sempre più propense a utilizzare la rete, operano oltre i confini nazionali e legali, sfruttando tecnologie avanzate e risorse strutturali ed economiche significative.

Nonostante l'apparente asimmetria di potere tra i cyber criminali e le forze di polizia, il valore etico di "giocare secondo le regole" rafforza la legittimità e il rispetto per le istituzioni, che si dedicano a collaborare con altre nazioni, promuovendo una coesione internazionale che rafforza l'unità di intenti e obiettivi di polizia e giustizia, anche se le normative penali possono differire. Questo sforzo congiunto mette in luce la determinazione delle forze dell'ordine nel combattere la criminalità con trasparenza e impegno.

L'uso della tecnologia avanzata (IA) da parte delle forze di polizia può essere un valido strumento per prevenire e combattere il crimine, senza compromettere le libertà individuali. È fondamentale trovare un equilibrio tra libertà e sicurezza per mantenere intatti i valori democratici. Investire nella prevenzione e nell'educazione digitale è essenziale per rafforzare la fiducia dei cittadini nelle istituzioni.

L'implementazione dell'IA e degli strumenti di sorveglianza digitale deve avvenire in modo proporzionato e trasparente, rispettando i principi etici e legali. È essenziale gestire i rischi legati a bias, discriminazione, responsabilità, privacy e trasparenza. Inoltre, sarebbe auspicabile sviluppare normative che possano supportare l'uso di

tecniche di "hacking etico", utili per infiltrarsi nelle reti criminali, sempre nel rispetto dei valori etici e legali, garantendo la legittimità delle azioni intraprese.
Le aziende tecnologiche e il mondo accademico hanno un ruolo fondamentale in questo contesto. Le aziende creano tecnologie basate su IA per le forze di polizia, mentre il mondo accademico offre ricerca e analisi critiche. La collaborazione tra questi attori ha già portato a soluzioni innovative e ha assicurato un utilizzo etico ed efficace delle tecnologie. Inoltre, le aziende tecnologiche collaborano strettamente con le forze dell'ordine per sviluppare strumenti che soddisfino le esigenze operative senza violare i diritti dei cittadini e il mondo accademico fornisce conoscenze approfondite e nuove prospettive su come migliorare l'uso dell'IA nella sicurezza, considerando le implicazioni etiche e sociali.

Le istituzioni internazionali, insieme alle forze di polizia, alle aziende e al mondo accademico, hanno contribuito a definire quadri normativi e standard etici per l'uso delle tecnologie di sorveglianza e IA. La diffusione della tecnologia avanzata deve avvenire nel rispetto della centralità dell'essere umano e della sua affidabilità. Un'IA antropocentrica è progettata e utilizzata per servire gli interessi umani, rispettando i diritti e le libertà fondamentali. La trasparenza, il controllo umano e l'affidabilità sono principi fondamentali nell'implementazione dell'IA. Gli algoritmi devono essere comprensibili e le decisioni che ne derivano devono essere spiegabili in termini umani. Gli esseri umani devono mantenere il controllo finale sui sistemi di IA, assicurando che tutte le decisioni siano prese con considerazione etica e morale, prive di bias, garantendo giustizia ed equità, in linea con il principio di uguaglianza prevista dall'articolo 3 della Costituzione.
È essenziale affrontare la lotta al crimine con integrità e rispetto dei diritti fondamentali, mantenendo la fiducia della società civile. La vera vittoria non consiste solo nello sconfiggere i criminali, ma nel farlo preservando i valori etici che definiscono una società democratica e giusta.

In questo contesto, il progetto europeo STARLIGHT[1] rappresenta un esempio concreto di collaborazione efficace. Questo progetto, che coinvolge la Polizia Postale tra i principali attori, si concentra sullo sviluppo di applicativi di IA per prevenire e contrastare i crimini informatici. Grazie a STARLIGHT, le forze dell'ordine europee avranno accesso a strumenti avanzati che miglioreranno le loro capacità di indagine e prevenzione, garantendo un approccio più efficace ed etico nella lotta contro la criminalità informatica.

[1] Finanziato dal Programma di Ricerca e Innovazione Horizon 2020 dell'Unione Europea in base all'accordo di sovvenzione n. 101021797

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

La protezione dei diritti di bambini e adolescenti rappresenta una priorità per la Polizia di Stato e richiede un'attenta valutazione delle minacce emergenti, l'impiego di tecnologie innovative e un approccio metodologico e operativo in linea con lo sviluppo dei mezzi di comunicazione che possa consentire nuove prospettive in termini di conoscenza e interazione sociale.
Le competenze della Specialità in materia di tutela dei minori si sono ampliate grazie a disposizioni normative[2] volte a rafforzare il sistema di protezione e a contrastare fenomeni come il *cyberbullismo* e bullismo, le tendenze giovanili emergenti, incluse le *challenge* – sfide rischiose diffuse sui *social network* – che hanno incrementato i pericoli per i ragazzi nel contesto digitale.

I *social media*, le piattaforme di messaggistica e i nuovi strumenti digitali sono considerati dagli adolescenti ambienti privilegiati per creare e mantenere relazioni sociali. Tuttavia, i pericoli della rete sono numerosi: i minori possono essere vittime di adescamento (*grooming*) o essere spinti da predatori *online* a produrre immagini intime, con il rischio di incorrere in minacce come la pedopornografia, il *revenge porn* e la *sextortion*. Possono altresì subire atti di prepotenza, scherzi crudeli e molestie da parte di coetanei, spesso durante le sessioni di gioco *online* (*cyberbullismo*), oltre a rischiare violazioni della *privacy* o truffe informatiche (*romance scam*).
La rete può anche offrire spazi di confronto e supporto emotivo tra coetanei, ma talvolta questi ambienti si trasformano in luoghi di condivisione di disagi psicologici, autolesionismo o disturbi alimentari. Inoltre, contenuti inappropriati risultano facilmente accessibili anche ai più piccoli, diventando un mezzo per esplorare precocemente la sessualità e partecipare a gruppi chiusi in cui si scambiano immagini di ogni genere, comprese rappresentazioni di violenza estrema, come il materiale "*gore*".

In qualità di organo del Ministero dell'Interno, il Servizio Polizia Postale detiene competenze istituzionali esclusive, sancite dalla normativa istitutiva del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), incaricato della prevenzione e repressione dei reati legati allo sfruttamento sessuale dei minori sul web[3].

---

[2] Legge 29 maggio 2017 "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*" oggi integrato dalla L. n.70 del 2024 per il bullismo e cyberbullismo.

[3] Legge 6 febbraio 2006 n. 38, l'art.14 bis con l'istituzione del (C.N.C.P.O), *con compiti di raccolta di tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi della rete INTERNET e di altre reti di comunicazione, nonché i gestori e gli eventuali beneficiari dei relativi pagamenti.*

Per svolgere queste funzioni, il Servizio si avvale di avanzate tecniche investigative assicurando il coordinamento internazionale con le forze di polizia estere e, a livello nazionale, i 18 Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) e le 82 Sezioni Operative (S.O.S.C.) della Polizia Postale.
Il lavoro di prevenzione e contrasto alle varie forme di aggressione, anche sessuale, ai minori in rete si integrano con le scienze sociali attraverso l'operatività dell'Unità di Analisi del Crimine Informatico, un'equipe di psicologi della Polizia di Stato, che contribuisce a costruire analisi criminologiche, buone prassi e azioni di sensibilizzazione che siano più efficaci nel mantenere al sicuro i minori.

La Polizia Postale partecipa a numerosi tavoli di lavoro interistituzionali per la protezione dei minori, tra cui il *Safer Internet Center Italy* in collaborazione con il Ministero dell'Istruzione e del Merito, l'*Osservatorio Nazionale per l'Infanzia e l'Adolescenza* e l'*Osservatorio per la Prevenzione e il Contrasto della Pedofilia e della Pornografia Minorile*, promosso dal Ministero della Famiglia. Inoltre, il *Gruppo di Lavoro sulle Sfide e Opportunità del Gaming*, istituito dal Dipartimento per la Trasformazione Digitale, dimostra come la complessità di questi fenomeni richieda un approccio sinergico per una comprensione e gestione efficace.

In considerazione della dimensione transnazionale di questi reati è stato rafforzato attraverso gli uffici di *Europol* e *Interpol* anche lo scambio di informazioni nei canali di cooperazione internazionale con l'obiettivo di promuovere a livello nazionale un'azione coordinata da parte degli Uffici della Specialità, per individuare autori e vittime di abusi. L'identificazione delle vittime è una priorità e viene affidata a un'unità investigativa specializzata che analizza e gestisce i file multimediali illeciti attraverso la Banca Dati I.C.S.E. (*International Child Sexual Exploitation Database*), accessibile tramite *Interpol* e alimentata dalle segnalazioni delle forze di polizia di tutto il mondo.
A tale settore affluiscono anche le informazioni fornite dall'*Unità di Informazione Finanziaria* (U.I.F.) della Banca d'Italia che segnalano transazioni sospette legate alla vendita di materiale pedopornografico sul web, utili per approfondimenti investigativi.

Su questo percorso il C.N.C.P.O. ha rinnovato l'impegno, in considerazione della particolare sensibilità riconosciuta verso la fragilità delle fasce deboli, nel redigere protocolli operativi di collaborazione con gli enti del terzo settore impegnati nel contrasto allo sfruttamento dei minori, rinnovando la tradizione di strutturare la funzionalità operativa a logiche efficaci ed inclusive di 'parteniariato pubblico e privato' e tra queste figurano quelle con *Telefono Azzurro*, *Save The Children*, *Terres Des Hommes*, *Operation Underground Railroad Rescue*, *National Centre for Missing and Exploited Children*, *Child Rescue Coalition* (C.R.C.) e l'*Associazione Meter di don Fortunato di Noto.*

L'attività di indagine, avviata a seguito delle numerose segnalazioni ricevute quotidianamente da varie fonti, ha consentito di raggiungere importanti risultati operativi, portando all'identificazione di 1.184 soggetti e all'esecuzione di 986 provvedimenti di perquisizione.

Pedopornografia e adescamento - *Anno 2024*

CNCPO	Anno 2023	Anno 2024
Casi trattati	2.702	2.828
Persone arrestate	108	147
Persone indagate	1.131	1.037
Perquisizioni	927	986
Siti in Black List	2.739	2.775
Siti visionati	28.355	42.231

Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

Il lavoro svolto dal **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** rappresenta un baluardo nella lotta contro lo sfruttamento sessuale dei minori su internet, un fenomeno che continua a evolversi e a manifestarsi in forme sempre più insidiose. L'analisi dei dati relativi agli ultimi due anni evidenzia un'intensificazione delle attività investigative con risultati significativi nella prevenzione e nel contrasto di questi crimini.

Nel 2024 il numero di **casi trattati** è risultato in aumento rispetto all'anno precedente, passando da **2.702 a 2.828**, un dato che testimonia non solo una crescita del fenomeno ma anche una maggiore azione sia in termini preventivi che repressivi. In tal senso l'attività di monitoraggio del web, supportata dall'uso di tecnologie avanzate, è stata orientata ad una più incisiva efficacia per l'individuazione e il contrasto dei reati legati alla pedopornografia online.

Il dato relativo all'aumento delle **persone arrestate**, passate da **108 nel 2023 a 147 nel 2024,** è connesso ad un rafforzamento delle operazioni repressive volte ad iden-

tificare e arrestare tempestivamente gli autori di gravi reati mentre il numero delle **persone denunciate in stato di libertà** è risultato in leggera diminuzione, da **1.131 a 1.037.**
Le analisi delle attività hanno evidenziato un aumento delle **perquisizioni**, passate da **927 nel 2023 a 986 nel 2024**. Questo dato dimostra un approccio investigativo più incisivo e capillare, con operazioni che hanno permesso di raccogliere prove fondamentali per i procedimenti giudiziari e di smantellare reti criminali attive nella diffusione di materiale pedopornografico.

Nell'ambito delle attività preventiva svolta dal C.N.C.P.O. incisiva è l'attività di 'sorveglianza della rete' attraverso la gestione dell'elenco dei siti che diffondono contenuti illeciti e che vengono segnalati per il blocco agli internet provider, meglio conosciuta come Black List. Il numero di siti inseriti in questa lista è passato da **2.739 a 2.775**, segno che la l'azione di vigilanza su questi contenuti è continua e in espansione così come il numero di **siti visionati**, che è aumentato in modo esponenziale, passando da **28.355 nel 2023 a 42.231 nel 2024**. Questo incremento evidenzia un l'impegno costante nell'attività di monitoraggio, reso possibile grazie a strumenti tecnologici avanzati e a una maggiore cooperazione internazionale. L'analisi di un numero così elevato di siti è essenziale per individuare nuove minacce, intercettare reti criminali e proteggere le vittime assicurando un ambiente digitale più sicuro per le nuove generazioni.

Adescamento online

L'adescamento di minori online rappresenta una delle minacce più insidiose e pericolose per i bambini e gli adolescenti, un fenomeno che il **Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)** affronta con costante impegno e strategie mirate. L'analisi dei dati relativi agli ultimi due anni evidenzia come questo reato, pur mantenendosi su livelli allarmanti, mostri un'evoluzione che richiede interventi sempre più specializzati e tempestivi.

Nel 2024, il numero complessivo dei casi trattati si attesta a **374**, un dato leggermente superiore rispetto ai **353** del 2023, che può essere interpretato come il frutto di un'intensificazione delle attività di prevenzione e educazione. L'adescamento online infatti è un fenomeno che si sviluppa e si manifesta nelle piattaforme digitali sempre più precocemente utilizzate da bambini e ragazzi come i *social network* le app di messaggistica istantanea e, più recentemente i videogiochi *online*, luoghi virtuali adatti per "predatori" pronti ad usare tecniche di manipolazione affettiva per ottenere immagini sessuali, video e addirittura incontri reali con potenziali vittime.

Un'analisi più approfondita dei dati mostra come il rischio non sia distribuito in modo uniforme tra le diverse fasce d'età. Se è vero che i **bambini tra 0 e 9 anni** rappresentano ancora una quota relativamente minore di vittime, con **26 casi nel 2024 rispetto ai 32 del 2023**, è altrettanto vero che si tratta di una tipologia di vittime particolarmente fragili per le quali un approccio sessuale precoce e tecnomediato può costituirsi come trauma concreto con potenzialità dannose piuttosto elevate. Spesso è nei luoghi virtuali del gioco che gli adescatori "avvicinano" le loro vittime, sfruttando l'entusiasmo di vincere una partita nel gioco online preferito, nascondendosi dietro profili falsi di sedicenti coetanei.

La **fascia d'età 10-13 anni**, che registra **207 casi in entrambi gli anni**, continua a essere la più esposta. In questa fase dello sviluppo i minori iniziano a esplorare il mondo digitale in maniera più autonoma utilizzando i *social media* e le *chat* per stringere nuove amicizie. Gli adescatori sfruttano questa apertura per avvicinarsi alle vittime, fingendo di condividere interessi comuni e instaurando un rapporto basato su fiducia e manipolazione. È in questo contesto che la Polizia Postale ha rafforzato le proprie strategie di prevenzione, promuovendo campagne di sensibilizzazione rivolte sia ai ragazzi che ai genitori, affinché possano riconoscere segnali di pericolo e adottare comportamenti più sicuri online.

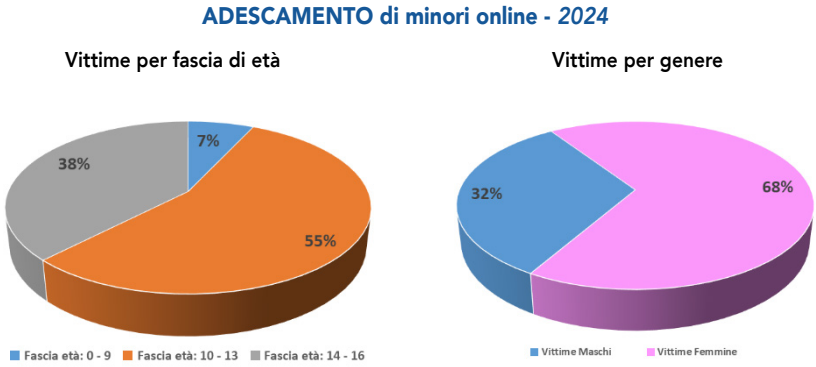
Il dato più significativo riguarda la **fascia 14-16 anni**, che mostra un incremento del **24%**, passando da **114 casi nel 2023 a 141 nel 2024**. Questo aumento riflette la crescente esposizione degli adolescenti a dinamiche digitali complesse, che vanno dal *sexting* alla condivisione di immagini intime, talvolta indotte con minacce o ricatti. Gli adescatori mirano a minori di questa età consapevoli della loro naturale curiosità per la seduzione, la sessualità e l'interazione libera, consapevoli di quanto i ragazzi si sentano sicuri in un dominio, quello digitale, in cui credono di muoversi con maggiore dimestichezza, minore esposizione corporea senza particolari controlli.

In questo contesto, il **Centro Nazionale per il Contrasto alla Pedopornografia Online** ha intensificato le proprie attività investigative, adottando tecniche avanzate di monitoraggio del *deep* e *dark web*, collaborando con le principali piattaforme digitali per segnalare e rimuovere contenuti illeciti e rafforzando la cooperazione con le forze dell'ordine internazionali per identificare e fermare i responsabili di questi crimini. L'impegno del C.N.C.P.O. non si limita alla repressione, ma si estende alla prevenzione e alla tutela delle vittime. Il lavoro svolto in collaborazione con l'*Unità di Analisi del Crimine Informatico* (U.A.C.I.) del Servizio Polizia Postale e per la Sicurezza Cibernetica, consente di offrire supporto ai minori coinvolti, aiutandoli a superare le conseguenze dell'adescamento e a riconquistare un senso di fiducia nonché a fornire al personale impegnato nell'attività di prevenzione sui temi della sicurezza online

le metodologie, i contenuti standard più adeguati con particolare attenzione ai più piccoli. Le iniziative di educazione digitale nelle scuole, promosse in collaborazione con il Ministero dell'Istruzione e le istituzioni competenti, sono risultate e costituiscono obiettivi fondamentali per fornire ad adolescenti e piccoli strumenti adeguati per difendersi dai pericoli della rete.

ADESCAMENTO MINORI online	TOTALE casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-16 anni
Anno 2022	**430**	33	231	166
Anno 2023	**353**	32	207	114
Anno 2024	**374**	26	207	141

Fonte - Polizia Postale e per la sicurezza cibernetica © 2025



Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

Sextortion – Vittime minori

La **sextortion** rappresenta una delle minacce più insidiose e devastanti per i minori nel panorama dei crimini online. Questo fenomeno si manifesta attraverso il ricatto sessuale: i malintenzionati inducono le vittime, spesso con l'inganno o la manipolazione emotiva, a condividere immagini intime per poi minacciarle della diffusione di tali materiali al fine di ottenere ulteriori contenuti, denaro o favori personali.

Singoli sfruttatori e organizzazioni criminali sfruttano le vulnerabilità psicologiche e

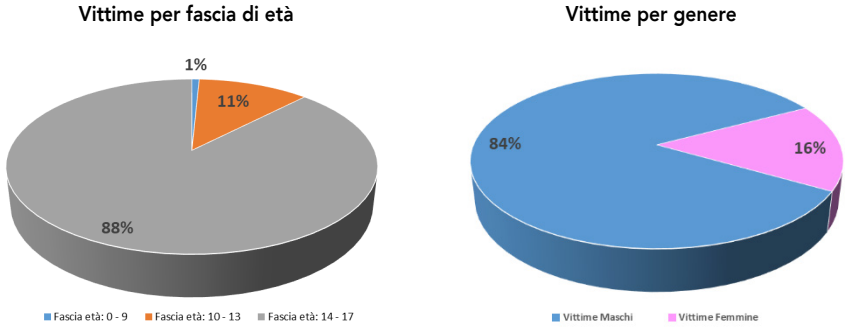
sociali dei giovani, le loro curiosità, la naturale fiducia negli altri per realizzare contatti online discreti e apparentemente anonimi attraverso i quali indurre a produrre, inviare e condividere con sconosciuti immagini intime e video personali estorti con minacce e raggiri.

Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** è in prima linea nella lotta contro questa forma di abuso, adottando strategie avanzate di investigazione, prevenzione e supporto alle vittime.

SEXTORTION Vittime minori	**TOTALE casi trattati**	**Casi trattati vittime 0-9 anni**	**Casi trattati vittime 10-13 anni**	**Casi trattati vittime 14-17 anni**
Anno 2022	**132**	3	18	111
Anno 2023	**137**	2	20	115
Anno 2024	**130**	1	15	114

Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

SEXTORTION a danno di minori - *2024*



Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

L'analisi dei dati relativi agli anni 2023 e 2024 mostra una sostanziale stabilità nel numero complessivo dei casi trattati, da **137 nel 2023 a 130 nel 2024**.

Un'analisi dettagliata delle fasce d'età delle vittime evidenzia come la minaccia della *sextortion* colpisca principalmente gli **adolescenti tra i 14 e i 17 anni**, con **115 casi nel 2023 e 114 nel 2024**. Questa stabilità nei numeri conferma come gli adolescenti, per la loro tendenza ad affidare le esplorazioni sentimentali ai servizi del web, *social*

network e messaggistica in primis, siano più esposti a questa tipologia di attacchi dai quali credono di sapersi difendere perché portatori di un'abitudine d'uso della tecnologia che diventa prassi consolidata.
In questa fascia d'età i ricattatori spesso si fingono coetanei per stimolare la curiosità, costruendo il miraggio di un'interazione sessuale autentica, spontanea, libera e reciprocamente partecipata nella quale invece tali elementi diventano poi strumento ubiquo di coercizione.
L'intensa attività del C.N.C.P.O. ha portato a smascherare numerosi *network* di sfruttamento, dimostrando come dietro molti casi di *sextortion* ci siano organizzazioni criminali con strategie ben strutturate e finalizzate all'estorsione su larga scala.

Appare opportuno evidenziare come la fascia **10-13 anni** abbia registrato un leggero calo da **20 casi nel 2023 a 15 nel 2024**. Anche se il numero complessivo è più contenuto rispetto agli adolescenti più grandi, questa categoria è particolarmente vulnerabile perché meno consapevole dei pericoli del web e più incline a fidarsi degli interlocutori online. I casi trattati in questa fascia evidenziano una dinamica ricorrente: le vittime vengono spinte con l'inganno a produrre immagini sessualmente esplicite, spesso senza rendersi conto delle implicazioni e successivamente vengono minacciate per ottenere ulteriore materiale.

Il dato relativo ai **bambini di età compresa tra 0 e 9 anni** è il più basso in termini numerici, con **due casi registrati nel 2023 e uno nel 2024**. Tuttavia, anche se statisticamente meno rilevante, questa fascia d'età rappresenta una delle più delicate poiché spesso le vittime non hanno gli strumenti per comprendere ciò che sta accadendo e possono essere manipolate con estrema facilità. I casi trattati mostrano che gli autori di questi crimini cercano di entrare in contatto con i minori attraverso piattaforme di gioco o sfruttano la mancanza di supervisione da parte degli adulti per interagire con loro. Il lavoro del C.N.C.P.O. in questi casi è particolarmente complesso e richiede un'immediata identificazione dei responsabili, spesso nascosti dietro false identità digitali, oltre a un intervento mirato per proteggere le vittime e le loro famiglie.

In questo ambito, un'altra priorità del CNCPO è il **supporto alle vittime**. La *sextortion* può avere gravi conseguenze psicologiche, portando i minori a vissuti di panico, ansia, vergogna e, nei casi più gravi, alla depressione e al rischio di autolesionismo. Per questo motivo, il Centro lavora in sinergia con i funzionari psicologi dell'*Unità di Analisi del Crimine Informatico* (U.A.C.I.) per fornire aiuto immediato a chi subisce questi ricatti, a chi utilizza il portale istituzionale *www.commissariatodips.it* per richiedere aiuto, alle famiglie che si trovano ad affrontare situazioni tanto delicate e pericolose per le giovani vittime. Il C.N.C.P.O. si impegna per l'identificazione e la denuncia dei responsabili ma offre accoglienza alle vittime e alle loro famiglie, for-

nendo strumenti concreti per affrontare le conseguenze emotive del reato e riprendere il controllo della propria vita.
Il contrasto delle *sextortion* con vittime minorenni continua a rappresentare uno dei target strategici del **Centro Nazionale per il Contrasto alla Pedopornografia Online**.

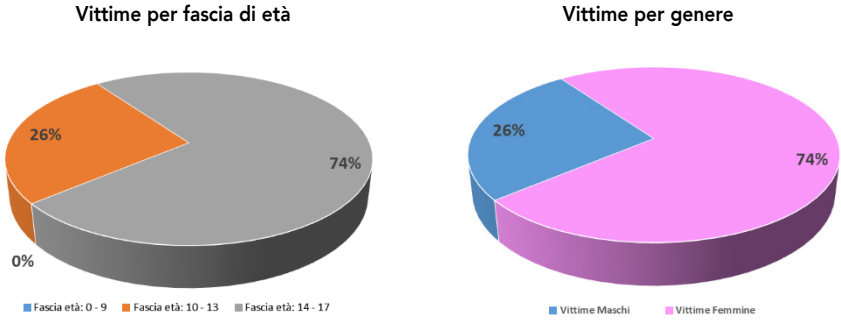
Diffusione illecita di immagini o video sessualmente espliciti (612 ter c.p.) – Vittime minori

Il revenge porn, ovvero la pubblicazione o diffusione di immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è una delle forme più gravi di aggressione online, con conseguenze devastanti per le vittime, in particolare quando sono minorenni. Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** è costantemente impegnato nel contrasto a questa minaccia attraverso attività investigative avanzate, azioni di prevenzione e supporto psicologico alle vittime realizzato dall'UACI.

REVENGE PORN Vittime minori	**TOTALE casi trattati**	**Casi trattati vittime 10-13 anni**	**Casi trattati vittime 14-17 anni**
Anno 2022	**34**	5	28
Anno 2023	**29**	6	23
Anno 2024	**42**	11	31

Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

REVENGE PORN a danno di minori - *2024*



Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

L'analisi dei dati relativi agli anni 2023 e 2024 evidenzia un aumento significativo dei casi trattati, passando da **29 nel 2023 a 42 nel 2024**, con una crescita del **45%**. Questo incremento indica una maggiore diffusione del fenomeno, ma al tempo stesso testimonia l'efficacia del lavoro del CNCPO, che attraverso monitoraggi sempre più capillari e una crescente sensibilizzazione ha portato a un aumento delle denunce e degli interventi.

Il *revenge porn* colpisce prevalentemente preadolescenti e adolescenti, ovvero coloro che iniziano a sviluppare una vita sociale *online* più attiva e un rapporto più stretto con la tecnologia e la condivisione di contenuti personali. Il fenomeno riguarda principalmente la diffusione non consensuale di immagini intime, spesso in seguito a relazioni affettive o a forme di adescamento online. Questo abuso si verifica soprattutto attraverso social network e applicazioni di messaggistica, strumenti che permettono la rapida e incontrollata propagazione dei contenuti.

Un dato particolarmente allarmante emerge nella fascia **10-13 anni** che registra un aumento da **6 casi nel 2023 a 11 nel 2024**, quasi raddoppiando in un solo anno. Questo incremento evidenzia come anche i più giovani siano esposti al rischio di subire forme di violenza sessuale digitale. Spesso questi casi coinvolgono situazioni in cui i minori vengono indotti con l'inganno o la manipolazione psicologica a condividere immagini intime, senza comprendere appieno le conseguenze di tale azione. L'incremento dei casi in questa fascia d'età ha suggerito un potenziamento delle attività di sensibilizzazione, affinché bambini e preadolescenti siano adeguatamente informati sui pericoli legati alla condivisione di immagini personali in rete.

La fascia **14-17 anni** rappresenta la categoria più colpita, con un sensibile incremento da **23 casi nel 2023 a 31 nel 2024**. Gli adolescenti sono spesso vittime di *revenge porn* in contesti di relazioni sentimentali finite male, vendette personali o dinamiche di pressione tra pari. L'abuso si manifesta con la minaccia o la diffusione di immagini intime al fine di esercitare un controllo sulla vittima, danneggiarne la reputazione o ricattarla emotivamente. Il C.N.C.P.O. interviene con tempestività per identificare i responsabili e bloccare la diffusione dei materiali, collaborando con le principali piattaforme digitali per la rimozione dei contenuti e attivando procedure di supporto psicologico per le vittime, che spesso subiscono gravi ripercussioni emotive e sociali.

Il lavoro della Polizia Postale nel contrasto al *revenge porn* minorile si articola su più livelli. Da un lato vi è l'attività investigativa che grazie all'uso di tecnologie avanzate consente di tracciare la diffusione dei contenuti illeciti e risalire ai responsabili. Dall'altro, la collaborazione con enti istituzionali, scuole e famiglie gioca un ruolo fondamentale per la prevenzione, attraverso campagne di educazione digitale mirate a

informare i giovani sui pericoli della condivisione di immagini intime e sulle strategie di difesa in caso di abuso.

Cyberbullismo

Dopo l'entrata in vigore della Legge 71/2017 (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyberbullismo*), integrata dalla L.70/2024 (Disposizioni e delega al governo in materia di prevenzione e il contrasto del fenomeno del bullismo *cyberbullismo*) sono stati previsti percorsi educativi obbligatori, interventi mirati per la rieducazione, un rafforzamento delle sanzioni nei casi più gravi e previsione di strumenti più incisivi per rimuovere contenuti lesivi in tempi rapidi e intervenire con maggiore efficacia nei casi di recidiva.

In questo contesto l'attività della Polizia Postale, affiancata da un quadro normativo più stringente, continua dunque a rappresentare un punto di riferimento nella difesa dei minori nel mondo digitale, lavorando senza sosta per individuare e fermare i responsabili, proteggere le vittime e diffondere una cultura di responsabilità e rispetto online.

Il fenomeno del *cyberbullismo* rappresenta una delle sfide più complesse e insidiose nel panorama della sicurezza *online*, soprattutto per i minori. Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** è impegnato in prima linea nel contrastare questa forma di violenza digitale che si manifesta attraverso minacce, insulti, diffamazione, diffusione di contenuti privati e attacchi psicologici perpetrati sui *social network*, nelle principali piattaforme di comunicazione e nelle *chat* dei videogiochi *online*. L'analisi dei dati relativi agli anni 2023 e 2024 evidenzia un aumento dei casi trattati che sono passati da **291 nel 2023 a 323 nel 2024**, segnando una crescita di circa il **10%**. Questo lieve incremento può essere collegato verosimilmente all'accresciuta consapevolezza del fenomeno che inducono le vittime ad uscire dal tunnel del silenzio e a cercare sostegno nelle famiglie nella rete istituzionale e di collaborazione creata tra istituzioni.

Sebbene il *cyberbullismo* colpisca prevalentemente gli adolescenti, i dati mostrano che nessuna fascia d'età è esente da questo fenomeno; nella fascia **0-9 anni** si registrano **8 casi nel 2023 a 9 casi nel 2024**. Questo dato, sebbene numericamente contenuto evidenzia che episodi di prevaricazione digitale possono verificarsi anche tra i più piccoli, spesso in ambienti di gioco *online* o attraverso piattaforme di messaggistica utilizzate senza una piena consapevolezza dei rischi.

Nella fascia **10-13 anni** si osserva un incremento, con i casi che salgono da **72 nel 2023 a 91 nel 2024** con un aumento del **26%**. In questa fase della crescita, la ricer-

ca di approvazione sociale e l'appartenenza al gruppo diventano fondamentali, e proprio per questo il *cyberbullismo* può avere conseguenze psicologiche devastanti. Spesso gli atti di prevaricazione si verificano attraverso gruppi di messaggistica privata, dove le vittime vengono isolate, umiliate o sottoposte a pressioni psicologiche che possono portare a conseguenze gravi, come ansia, depressione e perdita di autostima.

La fascia **14-17 anni** si conferma la più colpita, con un incremento da **211 casi nel 2023 a 223 nel 2024**. Gli adolescenti che vivono una parte sempre più significativa della loro vita online sono particolarmente esposti a forme di *cyberbullismo* che possono includere la diffusione non consensuale di immagini intime, minacce, insulti e fenomeni di esclusione sociale virtuale. In questa fascia d'età, il *cyberbullismo* può intrecciarsi con altre dinamiche digitali pericolose, come il *revenge porn*, la *sextortion* o l'adescamento *online*. La rapidità con cui i contenuti possono essere diffusi in rete rende ancora più difficile per le vittime gestire le conseguenze di questi attacchi, portando in alcuni casi a veri e propri stati di profonda sofferenza psichica.

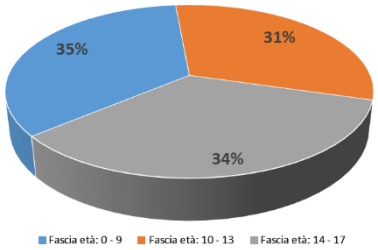
L'attività del C.N.C.P.O. nel contrasto al *cyberbullismo* si sviluppa su più livelli. L'aspetto investigativo gioca un ruolo centrale: l'identificazione degli autori, spesso coetanei delle vittime, richiede tecniche di analisi forense e un monitoraggio attento dei canali digitali utilizzati per diffondere contenuti offensivi o minacciosi. Parallelamente, la collaborazione con scuole, istituzioni e associazioni è essenziale per la prevenzione. Le campagne di sensibilizzazione, rivolte sia ai minori che alle loro famiglie mirano a educare all'uso responsabile dei *social media* e a fornire strumenti per difendersi da atti di bullismo digitale.

CYBERBULLISMO Vittime minori	**TOTALE casi trattati**	**Casi trattati vittime 0-9 anni**	**Casi trattati vittime 10-13 anni**	**Casi trattati vittime 14-17 anni**
Anno 2022	**326**	17	87	222
Anno 2023	**291**	8	72	211
Anno 2024	**323**	9	91	223

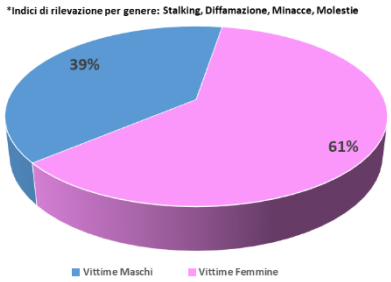
Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

CYBERBULLISMO a danno di minori - *2024*

Vittime per fascia di età



Vittime per genere*



Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

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

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.

Nel corso del 2024, l'Unità si è concentrata sui fenomeni prodromici alla violenza di genere online, anche fra minori, promuovendo momenti formativi dedicati agli operatori impiegati nel contatto con vittime fragili. Sempre più spesso i ragazzi "tollerano" forme di controllo tecnomediato (obbligo di geolocalizzazione, di documentazione fotografica dei luoghi e delle persone con cui si esce, supervisione degli outfit, etc.) scambiando prodromi di atteggiamenti di ipercontrollo e manipolazione per segnali di amore, affezione e trasporto.

La formazione degli operatori è tesa all'aggiornamento sulle varie forme di violenza che possono interessare i più giovani e le vittime femminili, allo scopo di aumentarne la capacità di ascolto, riducendo il rischio di vittimizzazione secondaria nella gestione delle richieste di aiuto e tutela.

L'UACI ha affiancato le squadre operative in investigazioni ad alto impatto emotivo, fornendo al personale le adeguate misure di riduzione dello stress lavoro correlato, attraverso incontri individuali e di gruppo finalizzati alla decompressione emotiva in diversi uffici territoriali.

Ha supportato l'attività investigativa conducendo audizioni di minori coinvolti in varie forme di aggressione tecnomediata, fornendo aiuto diretto ai ragazzi che contattano

il portale istituzionale www.commissariatodips.it, supportando le famiglie e favorendo quindi la messa in sicurezza delle piccole vittime.
I funzionari psicologi hanno inoltre contribuito all'ideazione di iniziative di comunicazione e sensibilizzazione rivolte ai minori, ai genitori e agli insegnanti, al fine di aumentare la consapevolezza collettiva in materia di rischio online, con sessioni formative rivolte alle aziende, alle scuole e agli operatori del sociale.

È stata dato inoltre largo spazio allo studio dei fenomeni emergenti di rischio online, alle metodologie più efficaci per realizzare interventi di prevenzione, con la finalità di standardizzare e qualificare gli interventi diretti a fasce di età di potenziali vittime sempre più precoci e fragili.

La Sezione Operativa

L'analisi dei dati contenuti nella rilevazione nazionale dei reati contro la persona per l'anno 2024 evidenzia il ruolo cruciale svolto dalla **Sezione Operativa incardinata presso la II Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica** nella tutela dei cittadini, con particolare attenzione ai fenomeni di criminalità informatica e alle minacce digitali contro la persona che sempre più frequentemente colpiscono individui di ogni fascia d'età.
Con un totale di **9.300 casi trattati** e **1.393 persone indagate** emerge chiaramente come il lavoro di monitoraggio e intervento sia stato intenso e capillare, coinvolgendo una molteplicità di reati che vanno dalla **diffamazione *online*** allo ***stalking***, dal ***revenge porn*** alla ***sextortion***, fino a comportamenti sempre più insidiosi come l'***hate speech*** e la **sostituzione di persona**.

Uno degli aspetti più rilevanti è l'alta incidenza dei reati legati alla **diffamazione *online***, con **1.977 casi trattati e 626 persone indagate**. Questo dato sottolinea la crescente tendenza dell'utilizzo delle piattaforme digitali anche per ledere la reputazione di individui o gruppi, fenomeno amplificato dalla rapidità con cui i contenuti si diffondono sul web. La Polizia Postale è intervenuta con indagini mirate, spesso in collaborazione con i gestori delle piattaforme, per identificare gli autori e rimuovere i contenuti diffamatori.

Tra i vari reati trattati emerge quello della ***sextortion***, **1.525 i casi trattati e 131 le persone indagate**. Questo fenomeno – che prevede l'estorsione a sfondo sessuale attraverso minacce di diffusione di immagini intime – rappresenta una delle forme di ricatto digitale più devastanti per le vittime. L'attività della Polizia Postale è stata fondamentale per identificare le reti criminali dietro questi episodi.
Di particolare gravità è anche il fenomeno del ***revenge porn***, con **266 casi trattati e 93 persone indagate**. La condivisione non consensuale di immagini intime conti-

nua a essere una problematica diffusa, con pesanti conseguenze psicologiche per le vittime. In decine di casi l'intervento tempestivo degli operatori della Polizia Postale è stato determinante nel rimuovere il materiale compromettente e perseguire i responsabili.

Per quanto riguarda i casi di ***stalking* e molestie**, il numero di episodi trattati (rispettivamente **185 e 545**) conferma l'ampia diffusione di comportamenti persecutori nel contesto digitale. Grazie a strumenti avanzati di tracciamento e analisi delle comunicazioni, la Polizia Postale è riuscita a individuare e fermare numerosi *stalker*, tutelando l'incolumità delle vittime.

Un dato particolarmente significativo è quello relativo alla **sostituzione di persona**, che ha registrato **3.088 casi trattati e 164 persone indagate**. L'utilizzo illecito di identità digitali è spesso connesso a truffe, estorsioni e altre attività fraudolente.

Un aspetto che merita particolare attenzione riguarda i **propositi suicidari**, con **56 casi trattati**. Sebbene non vi siano indagati, il ruolo delle forze dell'ordine in questi episodi è stato fondamentale per intervenire in tempo, fornendo supporto psicologico e assistenza. L'attività di monitoraggio delle segnalazioni e la collaborazione con i servizi di emergenza hanno permesso di intervenire tempestivamente e mettere in sicurezza diversi soggetti.

Infine, il fenomeno dell'***hate speech***, con **79 casi trattati e 31 persone indagate**, dimostra come il linguaggio d'odio continui a rappresentare una minaccia per la convivenza civile online. L'intervento della Polizia Postale in questo ambito si è concentrato sull'identificazione dei responsabili e sulla rimozione dei contenuti offensivi. L'insieme di questi dati evidenzia il significativo impegno della Polizia Postale nel contrasto ai reati digitali, con particolare attenzione alla protezione delle persone dalle insidie del web, garantendo la sicurezza e il rispetto della legalità anche in rete.

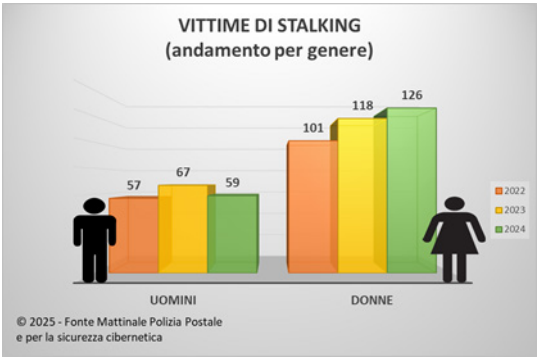
Stalking

Il **reato di stalking** (dall'inglese to stalk, letteralmente "fare la posta") è entrato a far parte dell'ordinamento penale italiano mediante il d.l. n. 11/2009 (convertito dalla l. n. 38/2009) che ha introdotto all'**art. 612-bis c.p.**, il reato di "**atti persecutori**", il quale punisce chiunque "con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita".

Dal 2022 al 2024, il numero totale dei casi trattati di cyber stalking è aumentato da 158 a 185, mostrando un incremento del 17% dal 2022 al 2023 e una stabilizzazione nel 2024. Le vittime di stalking sono prevalentemente donne, con una percentuale che è salita dal 64% nel 2023 al 68% nel 2024.
Il numero di persone indagate per *stalking* ha visto una crescita significativa. Nel 2022, erano 66, salite a 81 nel 2023 (+23%) e ulteriormente a 123 nel 2024 (+52%).
La distribuzione di genere delle vittime mostra che la percentuale di vittime uomini è scesa dal 36% nel 2023 al 32% nel 2024, mentre la percentuale di vittime donne è aumentata, passando dal 64% nel 2023 al 68% nel 2024.

STALKING	**2022**		**2023**		**2024**	
Uomini/Donne	Vittime Uomini 57 (36%)	Vittime Donne 101 (64%)	Vittime Uomini 67 (36%)	Vittime Donne 118 (64%)	Vittime Uomini 59 (32%)	Vittime Donne 126 (68%)
Casi trattati	**158**		**185**		**185**	
	Variazione percentuale		***+17%***	***+0%***		

STALKING	**2022**	**2023**	**2024**
Persone indagate	**66**	**81**	**123**
	Variazione percentuale	***+23%***	***+52%***



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 le vittime sono reduci da relazioni sentimentali ormai concluse o con figli che vivono in autonomia.

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, magari 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.

Nel 2024, la Polizia Postale ha indagato su 461 casi di truffe romantiche (di cui 4 in danno di minori), deferendo all'Autorità giudiziaria 140 persone.

Molestie

Dal 2022 al 2024, il numero totale dei casi di molestie online trattati è diminuito da 632 a 545. Nel 2022, le vittime di molestie erano suddivise tra 220 uomini (35%) e 412 donne (65%). Nel 2023, i casi trattati sono sostanzialmente invariati, con 187 vittime uomini (30%) e 444 vittime donne (70%). Tuttavia, nel 2024, si è registrata una diminuzione totale dei casi, con 545 vittime complessive, il 38% delle quali uomini.

Dal 2023 al 2024, si è osservata una diminuzione del 14% dei casi di molestie.

MOLESTIE	**2022**		**2023**		**2024**	
Uomini/Donne	Vittime Uomini 220 (35%)	Vittime Donne 412 (65%)	Vittime Uomini 187 (30%)	Vittime Donne 444 (70%)	Vittime Uomini 210 (38%)	Vittime Donne 335 (62%)
Casi trattati	**632**		**631**		**545**	
	Variazione percentuale		***0%***		***-14%***	

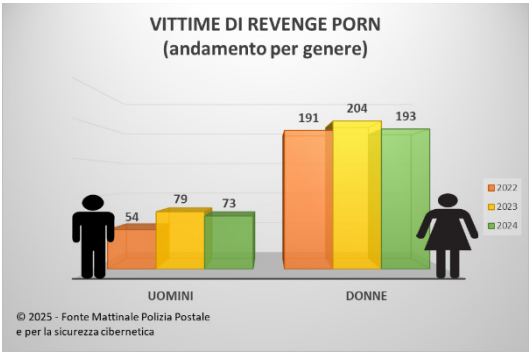
MOLESTIE	**2022**	**2023**	**2024**
Persone indagate	**56**	**74**	**83**
	Variazione percentuale	***+32%***	***+12%***

Revenge Porn

Nel 2023, il numero totale dei casi di "Revenge Porn" trattati era 283, mentre nel 2024 è diminuito a 266, registrando una variazione percentuale negativa del 6%. Le vittime di "Revenge Porn" nel 2023 erano 79 uomini (28%) e 204 donne (72%). Nel 2024, le vittime uomini erano 73 (28%) e le vittime donne 193 (72%).
Il numero di persone indagate per "Revenge Porn" ha registrato una diminuzione nel periodo analizzato. Nel 2023, erano 115 le persone indagate, scese a 93 nel 2024, con una diminuzione del 19%.

REVENGE PORN	2022		2023		2024	
Uomini/Donne	Vittime Uomini 54 (22%)	Vittime Donne 191 (78%)	Vittime Uomini 79 (28%)	Vittime Donne 204 (72%)	Vittime Uomini 73 (28%)	Vittime Donne 193 (72%)
Casi trattati	245		283		266	
Variazione percentuale			*+16%*	*-6%*		

REVENGE PORN	2022	2023	2024
Persone indagate	72	115	93
Variazione percentuale		*+60%*	*-19%*

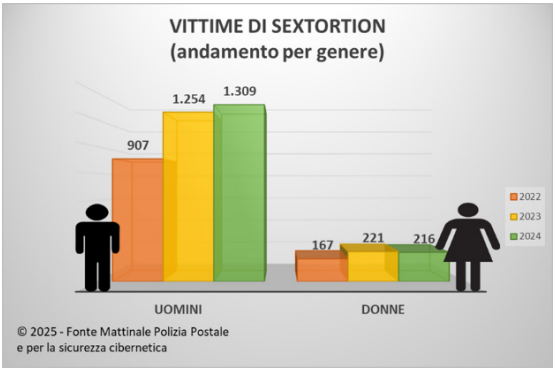


Sextortion

Nel 2023, il numero totale dei casi di *sextortion* trattati è stato di 1.475, mentre nel 2024 è aumentato a 1.525, registrando una variazione percentuale positiva del 3%. Le vittime di *sextortion* nel 2023 erano principalmente uomini, con 1.254 casi (85%), mentre le donne costituivano 221 casi (15%). Nel 2024, le vittime uomini sono aumentate a 1.309 (86%) e le vittime donne sono leggermente diminuite a 216 (14%). Il numero di persone indagate per *sextortion* ha visto una diminuzione nel periodo analizzato. Nel 2023, le persone indagate erano 168, mentre nel 2024 il numero è sceso a 131, registrandosi una variazione percentuale negativa del 22%.

SEXTORTION	**2022**		**2023**		**2024**	
Uomini/Donne	Vittime Uomini 907 (84%)	Vittime Donne 167 (16%)	Vittime Uomini 1.254 (85%)	Vittime Donne 221 (15%)	Vittime Uomini 1.309 (86%)	Vittime Donne 216 (14%)
Casi trattati	**1.074**		**1.475**		**1.525**	
	Variazione percentuale		***+37%***		***+3%***	

SEXTORTION	**2022**	**2023**	**2024**
Persone indagate	**96**	**168**	**131**
	Variazione percentuale	***+75%***	***-22%***



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

Fulcro dell'attività istituzionale a presidio delle infrastrutture critiche da attacchi di matrice comune, organizzata o terroristica, il CNAIPIC del Servizio polizia postale, organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, nel corso del 2024 ha consolidato il proprio ruolo all'interno dell'architettura nazionale della *cybersicurezza* quale Autorità preposta alla prevenzione ed al contrasto di settore.

In continuità con l'azione esplicata nell'arco di quasi un ventennio, l'attività sviluppata lungo il crinale della *prevenzione* ha continuato a riconoscere, innanzitutto, centralità alla condivisione delle informazioni di sicurezza qualificate a beneficio di infrastrutture critiche nazionali ed attori istituzionali, ma anche di realtà territoriali di carattere sensibile raggiunte grazie alla capillarità del comparto postale, che oggi vede nei Nuclei per la Sicurezza Cibernetica – NOSC , all'interno dei Centri Operativi – un'articolazione tanto indispensabile quanto strategica del proprio assetto operativo.

Efficace, sotto questo profilo, continua a essere il ricorso a modelli di partenariato pubblico-privato e pubblico-pubblico soprattutto laddove, attraverso il coinvolgimento di organismi esponenziali, sta consentendo la raggiungibilità di un numero sempre maggiore di realtà da tutelare.

Parimenti efficace, per quantità e qualità del dato, risulta essere l'attività prodromica all'acquisizione dell'informazione, che si alimenta lungo quattro grandi direttrici: la collaborazione istituzionale con partner qualificati, l'elaborazione interna frutto dell'attività di analisi, la collaborazione a livello internazionale e, ovviamente, il monitoraggio di iniziativa.

In tal senso, il 2024 testimonia un aumento delle capacità preventive, espresso da un aumento degli *alert* di sicurezza ed *early warning* diramati (59.875 in totale), che ha saputo beneficiare, in particolar modo, dell'incrementata capacità di *networking* con le omologhe strutture specialistiche di *law enforcement* a livello europeo ed internazionale.

Sul fronte del *contrasto* alla minaccia cyber sul territorio italiano, la lettura dei dati testimoniano un significativo aumento degli attacchi, diversificati per tipologia e natura degli obiettivi, che hanno coinvolto indistintamente enti e realtà economiche del tessuto nazionale: andamento che, parallelamente ad un incrementato ricorso allo strumento cibernetico da parte delle organizzazioni criminali, necessariamente

risente del contesto geopolitico attuale, in cui le ostilità in atto trovano una loro proiezione anche nel dominio cibernetico (cd. *cyber warfare*).

C.N.A.I.P.I.C. e N.O.S.C.	2022	2023	2024
TOTALE ATTACCHI RILEVATI *(target: Infrastrutture Critiche, Operatori di Servizi Essenziali, Pubbliche Amministrazioni Locali, Aziende e Privati)*	**13.099**	**12.101**	**12.058**
*Variazione percentuale **per anno***		*-8%*	*+0%*
Variazione percentuale nel biennio		*-8%*	

L'analisi degli attacchi per *matrice* restituisce un quadro in cui la quasi totalità degli stessi appare riconducibile a gruppi, per lo più stranieri, rimanendo residuale – benché rilevanti per la loro portata – la casistica di manovre attribuibili ad attori solitari.

Ciò posto, tuttavia, non sempre appare possibile attribuire una manovra ostile ad una determinata crew.

Da un lato, l'analisi tecnica dell'azione non restituisce sempre un "marchio di fabbrica" univocamente riconducibile ad un dato gruppo criminale; dall'altro, frequente è l'impiego a tattiche di elusione volte a ricondurre volutamente la responsabilità su altri attori (c.d. *false flags*)

In ultimo, anche l'analisi degli obiettivi perseguiti può non fornire elementi determinanti per il processo di *attribution*, posto come sia dimostrato che un determinato gruppo possa agire, in momenti diversi, sia per finalità prettamente criminali/predatorie, sia per finalità più prettamente orientate sotto il profilo ideologico.

Pertanto, si può infatti sostenere ragionevolmente la riconducibilità di una manovra ad una determinata *crew* laddove si abbia una rivendicazione (tipicamente nei casi DDos e *ransonware*) ovvero laddove le tecniche, tattiche e procedure impiegate offrano chiari elementi di riconducibilità dell'azione ad un collettivo noto.

L'analisi della minaccia sotto il profilo della *finalità* restituisce in termini ideali una distinzione degli attacchi tra manovre motivati da scopi predatorio e quelle orientate da ragioni politiche.
Invero, sempre più spesso emerge una sovrapposizione degli obiettivi perseguiti, e le stesse tecniche utilizzate per l'uno divengono funzionali per ottenere o mascherare l'altro.

Esempio tipico in tal senso è l'attacco di tipo *ransomware*, minaccia che - come testimoniato dall'andamento del fenomeno nel 2024, in crescita rispetto al 2023 - continua a classificarsi tra le più significative nel panorama italiano oggetto di analisi della Polizia Postale e per la Sicurezza Cibernetica.
L'utilizzo di tale tipo di *malware* - inoculato per carpire i dati e criptarli, rendendoli di fatto inaccessibili alla vittima – si riscontra tanto nei confronti di aziende private quanto pubbliche amministrazioni, a dimostrazione di come non sempre sia finalizzato da interessi meramente economici.
Ciò trova giustificazione, principalmente, nell'affermazione di un modello di business che ha trasformato il software malevolo in un servizio posto a disposizione della criminalità (RAAS).

Più chiara, invece, appare la natura attribuibile alle manovre di tipo DDos, ove la rivendicazione che solitamente accompagna l'attacco esplicita la ragione politico - ideologica che l'ha motivata. Il 2024 ha segnato una recrudescenza del fenomeno, con un picco registrato nella seconda meta del semestre, recante il segno distintivo di gruppi già noti o di altri di recente affermazione, ma già particolarmente attivi sul fronte dell'*hacktivismo*, per lo più di matrice russofona.

Sotto il profilo tecnico si configurano, tendenzialmente, come manovre poco impattanti sulle strutture attaccate, determinando solo in rari casi un malfunzionamento dei servizi offerti, a dimostrazione di una generale efficacia e reattività dei sistemi di mitigazione posti in essere dalle strutture di sicurezza dei soggetti colpiti. Molto più incisive, benché statisticamente più limitate da un punto di vista numerico, appaiono le manovre di *defacement*, anch'esse prevalentemente finalizzate alle manifestazioni di posizioni filorusse o filopalestinesi e rivendicate nei canali d'area degli stessi attori. Ciononostante, per la rilevanza degli obiettivi raggiunti – tra cui istituzioni di primo livello – sono in grado di ottenere un discreto clamore mediatico.

Un cenno a parte meritano infine le manovre volte a garantire la persistenza nei sistemi informatici, meglio conosciute come *Advanced Persistent Threats* (APT).
Finalizzate ad acquisire sia la conoscenza approfondita del sistema impattato, sia le informazioni in esso contenute, dette operazioni cibernetiche risultano per lo più

mirate a target strategici quali infrastrutture, pubbliche amministrazioni, aziende partecipate o imprese di rilievo nel rispettivo settore produttivo.
In quest'ambito, l'elevata competenza tecnica e le risorse – sia economiche che umane – che tali manovre richiedono, implicano il coinvolgimento di attori ostili connessi o sponsorizzati direttamente da stati o da organizzazioni governative.

Nel contesto finora illustrato vanno inoltre ascritte le nuove forme di minaccia derivanti dall'impiego di tecnologie avanzate, prime fra tutte l'Intelligenza Artificiale. Attraverso tali strumenti digitali, i *cybercriminali* non necessitano più di *skill* avanzate poiché, proprio come accade nell'utilizzo di software malevolo "*As A Service*", le piattaforme di A.I. forniscono molteplici soluzioni per sferrare attacchi sempre più sofisticati. Alla stessa stregua, anche le tecniche criminali adottate si sono evolute grazie l'impiego di artefatti che sfruttano la manipolazione cognitiva e l'ingegneria sociale, difficilmente rilevabili dalle tradizionali difese informatiche.

In questa competizione asimmetrica, orientata all'adozione di tecnologie sempre più evolute, è indispensabile rimanere al passo con i tempi e sviluppare soluzioni proattive che impieghino modelli di Intelligenza Artificiale, ad esempio, per correlare eventi, riconoscere pattern nascosti e prevedere minacce inedite, in modo da anticipare quanto più possibile il contrasto alle azioni malevole.

Attività di Polizia Giudiziaria

Si riportano di seguito due delle principali operazioni del 2024

Attacco a Giustizia: il 01.10.2024 il CNAIPIC del Servizio Polizia Postale e per la Sicurezza Cibernetica, dopo una complessa ed articolata attività investigativa, ha tratto in arresto il più importante hacker mai individuato in Italia, autore del più esteso attacco informatico perpetrato in danno di un servizio pubblico essenziale mai occorso a livello nazionale reo di aver interamente compromesso ed asservito al proprio controllo l'infrastruttura informatica del Ministero della Giustizia. L'autore del reato, attraverso inedite capacità di attacco, oltre ad accedere abusivamente all'infrastruttura informatica del Ministero della Giustizia, ha compromesso la rete satellitare servente la flotta aeronavale della Guardia di Finanza, ha compromesso i sistemi di telecomunicazione dell'operatore TIM S.p.A. e l'infrastruttura di rete della WindTre s.p.a

Accesso abusivo ai sistemi informatici dell'ASL Roma 1: il 22.02.2024 personale del CNAIPIC del Servizio Polizia Postale e per la Sicurezza Cibernetica ha concluso una complessa attività investigativa individuando l'autore dell'accesso abusivo, a scopo estorsivo, eseguito in danno dei sistemi informatici dell'ASL Roma 1. L'autore della condotta criminosa è stato individuato grazie ad una meticolosa attività di

OSINT suffragata da elementi investigativi di rilievo ottenuti grazie ad approfondite indagini e la collaborazione di provider e fornitori di servizi ubicati all'estero.

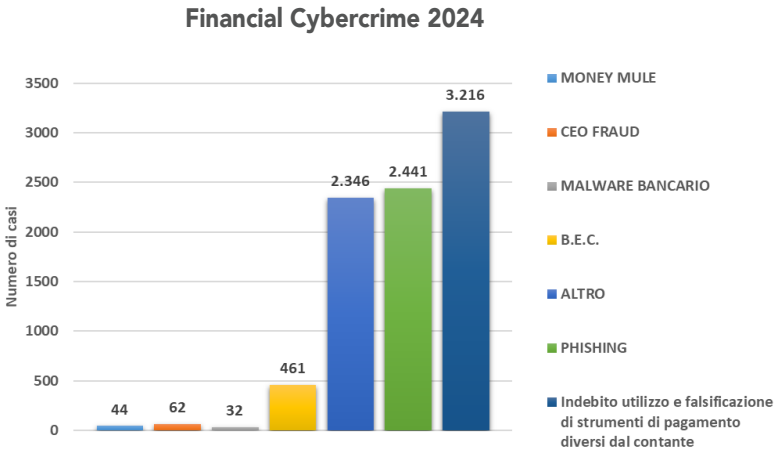
Financial Cybercrime

L'analisi delle evidenze riferibili al decorso anno 2024 rivela come il *financial cybercrime* sia sempre più una delle forme predominanti e preminenti del crimine informatico, con una tendenza in aumento che permane a livello globale.
Molteplici e in continua evoluzione risultano le tecniche utilizzate dalle organizzazioni criminali, attivate in danno di cittadini, piccole e medie imprese (che costituiscono il tessuto economico portante del Paese), nonché, sovente, in danno delle più grandi ed importanti aziende.
Persistono i più tradizionali *modi operandi*, tipici del crimine finanziario di interesse della Polizia Postale e per la Sicurezza Cibernetica. In primo luogo il c.d. *"phishing"*[4] che consente il furto dei dati sensibili per l'accesso ai sistemi di *home banking*, funzionale a illecite operazioni bancarie: lo scopo di tali tecniche di attacco è quello di entrare in possesso delle credenziali finanziarie delle vittime, per poter poi operare dai conti correnti online con le carte di credito/debito, attraverso prelievi, con bonifici o con l'acquisto di beni online.

	2022	2023	2024
Frodi Informatiche e monetica (Ril. nazionale)	9.423	10.755	8.602
Persone indagate	867	927	923
Somme sottratte	€ 39.387.485	€ 40.503.616	€ 48.674.917

Fonte - Polizia Postale e per la sicurezza cibernetica © 2025

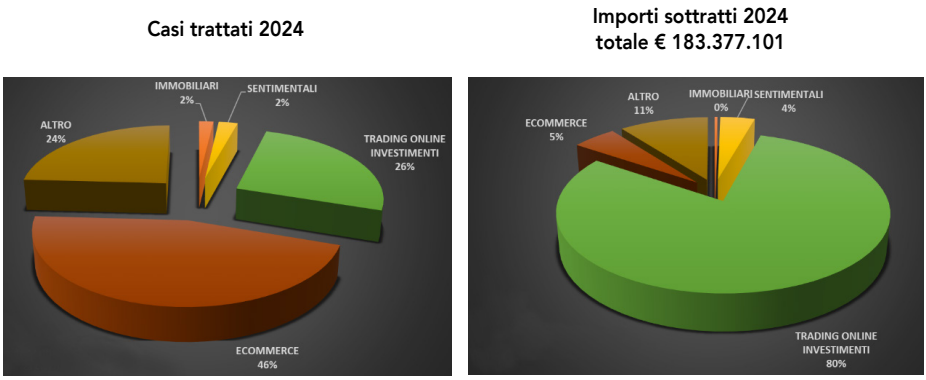
[4] Realizzabile anche nelle varianti del c.d. "smishing" (allorché non si utilizzi la classica email, ma il "veicolo" utilizzato per ingannare la vittima sia un messaggio telefonico) e del c.d. "vishing" (qualora si ricorra ad un contatto diretto a voce).



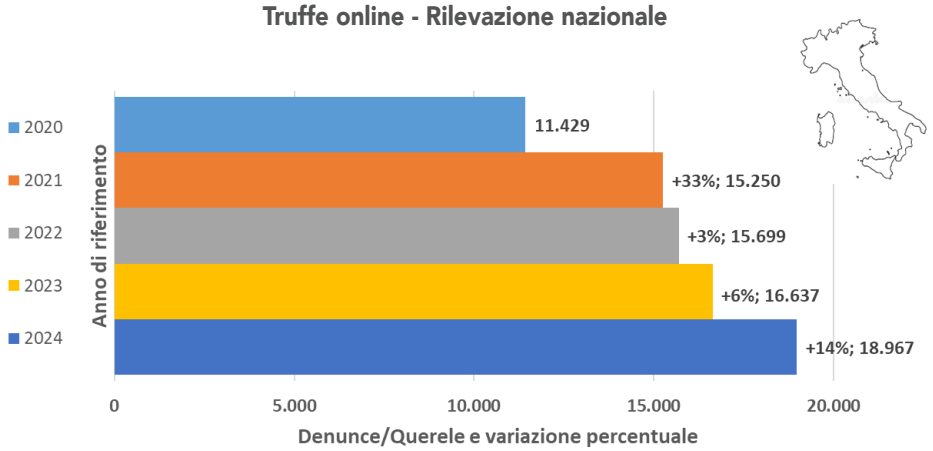
Fonte - Mattinale Polizia Postale e per sicurezza cibernetica © 2025

Per quanto riguarda le fattispecie di truffe più comuni e tradizionali, come ad esempio le vendite piramidali, le offerte di lavoro fasulle, i falsi prestiti di denaro, le finte locazioni immobiliari, le false vincite alle Lotterie e le polizze assicurative fraudolente, rispetto all'anno 2023 si registra un moderato aumento dei casi trattati.
Parimenti in crescita sono le fattispecie di truffe originate da acquisti online su piattaforme digitali di vendita, c.d. *e-commerce*, aventi a oggetto qualsiasi tipo di prodotto o servizio e rivolte a un bacino di utenza sempre più ampio e composto anche da giovanissimi.

	2020	2021	2022	2023	2024
Truffe OnLine (Ril. nazionale)	11.429	15.250	15.699	16.637	18.967
Persone indagate	3.654	3.441	3.570	3.610	3.627
Somme sottratte	€ 36.344.718	€ 73.245.740	€ 116.454.550	€ 139.536.457	€ 183.377.101



Fonte - Mattinale Polizia Postale e per sicurezza cibernetica © 2025

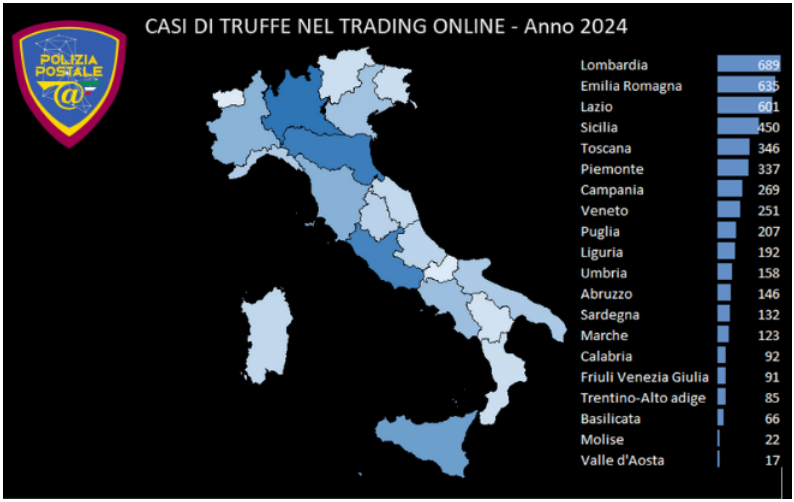


Fonte - Mattinale Polizia Postale e per sicurezza cibernetica © 2025

Inoltre, nel 2024 si è registrato un significativo aumento dei casi di *spoofing*, fenomeno che sta diventando sempre più preoccupante sia per le aziende che per gli utenti privati. Con l'evoluzione delle tecnologie digitali e l'adozione massiccia di strumenti di comunicazione online, i criminali informatici hanno affinato le loro tecniche di inganno, utilizzando lo *spoofing* per travisare la propria identità e ottenere accesso a informazioni sensibili.

Questo Servizio ha registrato l'evoluzione di fenomeni criminali già collaudati e conosciuti come il *trading online*, che grazie alle nuove tecnologie a disposizione di cyber

criminali, come l'IA, che riesce a modificare in maniera verosimile immagini e audio di noti personaggi pubblici, rendono credibili informazioni artefatte, inducendo in errore e creando grave nocumento a una vasta pletora di utenti del web.



Distribuzione geografica dei casi di truffe nel trading online denunciati presso gli uffici territoriali della Polizia Postale nel 2024. *(Fonte: Mattinale Polizia Postale e per la sicurezza cibernetica © 2025*)

Distribuzione geografica delle somme sottratte tramite truffe nel trading online denunciate presso gli uffici territoriali della Polizia Postale nel 2024. *(Fonte - Mattinale Polizia Postale e per la sicurezza cibernetica © 2025)*

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

Di seguito si riporta la descrizione dei principali fenomeni criminali registrati nell'ambito del *financial cybercrime*

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.

Trading Online

Tale fenomeno criminoso si registra in relazione alla promozione sulle principali piattaforme social (ad esempio *Facebook* o *Youtube*), di falsi investimenti finanziari.

I *cybercriminali* sfruttando varie tecniche, quali l'ingegneria sociale, inducono gli utenti mossi dalla possibilità di realizzare guadagni facili a investire su piattaforme di *trading online*. Le telefonate di *marketing* sono il classico metodo operativo, mediante il quale un finto broker spinge forzatamente gli utenti a depositare su conti pilotati o investire su un determinato tipo di *asset* (spesso criptovalute le quali presentano un grado di volatilità e anonimato superiore). In

particolare, viene richiesto all'utente di iscriversi su una piattaforma di *trading online*, apparentemente semplice e intuitiva, per facilitare le operazioni, il falso operatore può anche proporsi di effettuare l'iscrizione al posto dell'utente o proponendo l'installazione di software che permetteranno il controllo remoto sui dispositivi del malcapitato. Inizialmente vengono richieste piccole somme di denaro, che apparentemente sembrano fruttare bene, ma ben presto vengono richiesti importi sempre più ingenti, il tutto fin quando il soggetto truffato non ha più modo di accedere a quanto investito.

Deep Fake

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

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

Non ultimo, lo sfruttamento della IA, sta portando all'evoluzione del su citato *CEO Fraud*, dove i *cybercriminali* con l'acquisizione di fonti aperte relative al soggetto bersaglio, possono ricrearne la voce o le movenze permettendo al falso amministratore di impartire disposizioni su uno o più bonifici correlati ad una inesistente operazione finanziaria riservata ed urgente.

Criptovalute

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

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

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

Quest'ultima può essere definita come una sorta di "registro digitale", che rien-

tra nella più ampia categoria della c.d. "tecnologia del registro pubblico distribuito" (*DLT Distributed Ledger Technology*).

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

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

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

La caratterizzazione bifronte della valuta virtuale, pertanto, oscillante tra "moneta" e "rappresentazione di valore" genera di fatto problematiche operative nella fase delle indagini di polizia, soprattutto nella configurazione di reati, come il riciclaggio, storicamente collegati al trasferimento fraudolento di beni e fondi monetari in moneta di conto, laddove le transazioni registrate sulla *blockchain*, benché pubbliche, garantiscono l'anonimato degli attori coinvolti nella transazione e l'oggettiva difficoltà della tracciabilità delle stesse.

Seguire le *cryptocurrencies* rappresenta la nuova sfida della moderna polizia giudiziaria e dell'Autorità giudiziaria per contrastare le attività criminali, con strumenti tecnologici e collaborazioni internazionali senza che però ne sia automaticamente svelato il possessore, come avviene per il contante o moneta "fisica".

Phishing

Analoga persistenza, tra le principali condotte criminose, si registra in relazione all'indebita acquisizione dei dati sensibili che consentono l'accesso ai sistemi di *home banking* (generalmente indicati con i termini di "*pishing*", "*smishing*" e "*vishing*" a seconda dello strumento utilizzato: tramite mail, sms o contatto diretto a voce; il cui scopo è quello di entrare in possesso delle credenziali finanziarie delle vittime, per poter poi operare dai conti correnti online, con le carte di credito/debito con prelievi, ove possibile bonifici o acquisto di beni online.

Spoofing

Lo *spoofing* è una tecnica di attacco informatico che mira a ingannare un sistema o

un utente, simulando che una comunicazione provenga da una fonte affidabile, quando in realtà è manipolata da un attaccante.

Lo *spoofing* è spesso utilizzato in combinazione con altre tecniche di attacco, come il *phishing*, per rubare informazioni sensibili, come credenziali bancarie o dati personali.

La modalità più diffusa e in progressivo aumento è il c.d. "*vishing*" - *voice phishing*, che utilizza numerazioni VoIP provenienti dall'estero, attraverso la riproduzione fittizia di numerazioni apparentemente in uso alle Forze dell'Ordine, a istituti bancari e uffici postali, per rendere più credibile l'inganno alle potenziali vittime.

Al fine di contrastare tale dinamica delittuosa il Servizio Polizia Postale e per la Sicurezza Cibernetica ha avviato interlocuzioni con l'Autorità per le Garanzie nelle Comunicazioni (AGCOM) e con i principali gestori di telefonia e connettività dati al fine di verificare la sussistenza di strumenti idonei a identificare e "bloccare" il flusso telefonico fraudolento.

Prevenzione e contrasto

Allo scopo di innalzare i livelli di contrasto alle specifiche fenomenologie criminose, l'azione della Specialità, anche nel settore del *financial cybercrime*, non si connota solo per i profili repressivi, ma anche per la particolare attenzione rivolta alla prevenzione, con campagne mirate di informazione destinate sia alle *Law Enforcement* che al pubblico, anche attraverso i canali *social* ufficiali.

Nel corso del 2024 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli. Analoga attività di prevenzione e monitoraggio viene svolta su siti e spazi web (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine sia per contrastarne la diffusione irregolare o illegale che per tutelare gli interessi dei consumatori specie se minori d'età.

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

A tal proposito significativa, soprattutto ai fini della tempestività dell'azione, risulta essere la collaborazione internazionale, sia in ambito europeo che extraeuropeo: spesso, nei casi di prontezza di reazione delle vittime e, quindi, nell'immediatezza dei fatti, 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, attraverso la collaborazione con le forze di polizia di quei paesi stranieri dove vengono indirizzate le somme sottratte o dove operano gli autori dell'illecito (cooperazione che si presenta utile, anche se più complessa da attuare, quando ci si trova a dover interagire con alcuni paesi extraeuropei). In tale contesto di collaborazione internazionale, è da segnalare la partecipazione, fra i vari tavoli di lavoro, a quello denominato *EMMA* (*European Money Mule Action*), a cui aderiscono ulteriori Stati europei e l'Agenzia EUROPOL, che permette di realizzare efficacemente, con impegno sinergico, indagini congiunte con risultati investigativi di notevole rilievo.

Approfondimento - Distribuzione dei metodi di furto di identità

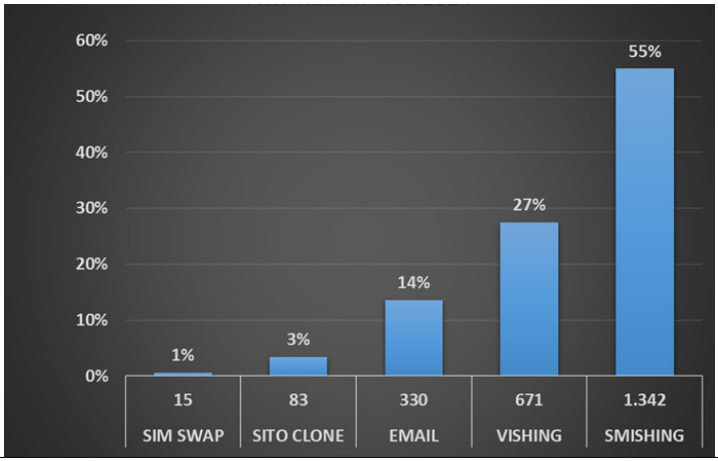
Nel 2024, il furto di identità ha continuato a essere una delle minacce più gravi nel contesto dei reati economico-finanziari online. Questo approfondimento, a cura del Settore del settore analisi e pianificazione strategica del Servizio Polizia Postale, presenta un'analisi dettagliata dei metodi di furto di identità utilizzati e delle relative statistiche, fornendo raccomandazioni sulle misure di sicurezza da adottare per contrastare questo fenomeno, rilevate consultando il sito del Commissariato di P.S. online (www.commissariatodips.it) e in particolare gli *alert* diramati.

Metodologia

I dati presentati sono stati raccolti dalla Polizia Postale e per la sicurezza cibernetica. Le informazioni comprendono sia i casi denunciati presso gli Uffici della Specialità Cibernetica della Polizia di Stato nel corso del 2024, sia quelli delegati alla Polizia Postale nello stesso anno dall'Autorità giudiziaria. Tuttavia, è importante notare che i casi evidenziati sono solo quelli in cui è stato possibile rilevare la metodologia con cui è avvenuto il furto di identità digitale. Non sempre le denunce o gli elementi raccolti durante le indagini sono sufficienti per determinare con esattezza la metodologia utilizzata. Questo report include dettagli sui vari metodi impiegati per il furto di identità.

I dati mostrano la distribuzione percentuale dei diversi metodi di furto di identità nel 2024, insieme al numero effettivo di casi per ciascun metodo: *SIM Swap* (1% con 15 casi), Sito Clone (3% con 83 casi), *Email* (14% con 330 casi), *Vishing* (27% con 671 casi) e *Smishing* (55% con 1.342 casi).

Furto identità nei reati economico - finanziari nel 2024



Fonte - Mattinale Polizia Postale e per sicurezza cibernetica © 2025

Lo ***smishing*** (**1.342 casi, con un'incidenza 55%**) si è confermato anche per il 2024, il metodo più comune di furto di identità. Questa tecnica sfrutta l'invio di messaggi SMS fraudolenti per indurre le vittime a fornire informazioni personali o finanziarie. La prevalenza dello *smishing* può essere attribuita alla crescente dipendenza dagli smartphone e alla fiducia che gli utenti ripongono nei messaggi SMS. Una tecnica criminale di particolare preoccupazione, utilizzata in combinazione con lo *smishing*, è l'alias telefonico. Attraverso questa pratica, comunicazioni bancarie fraudolente si inseriscono nella sequenza di messaggi autentici provenienti dalla banca, rendendo così i tentativi di frode ancora più difficili da rilevare. La Polizia Postale ha intensificato le campagne di sensibilizzazione per educare gli utenti sui rischi dello *smishing* e sulle pratiche di sicurezza da adottare.

Il ***vishing*** (**671 casi, con un'incidenza 27%**), ovvero il *phishing* telefonico, rappresenta il secondo metodo più comune. Questo metodo coinvolge chiamate telefoniche fraudolente in cui i truffatori si spacciano per rappresentanti di istituti finanziari o altre autorità per ottenere informazioni sensibili. Per contrastare il *vishing*, è essenziale educare gli utenti a verificare sempre l'identità del chiamante e a non fornire mai informazioni personali per telefono.

L'email *phishing* (**330 casi, con un'incidenza 14%**) continua a essere un metodo significativo di furto di identità. I truffatori inviano email fraudolente che sembrano provenire da fonti affidabili per convincere le vittime a cliccare su link dannosi o a

fornire informazioni personali. È fondamentale implementare filtri anti-*phishing* più efficaci e promuovere la formazione continua sugli attacchi via email.

Il metodo del **sito clone** (**83 casi, con un'incidenza 3%**) prevede la creazione di siti web falsi che imitano quelli legittimi per ingannare gli utenti e raccogliere le loro credenziali. È importante promuovere l'uso di certificati SSL/TLS e l'educazione degli utenti su come riconoscere i siti web falsi.

Il ***SIM swap*** (**15 casi, con un'incidenza 1%**), sebbene meno comune, rappresenta comunque una minaccia significativa. Questo metodo coinvolge la frode nelle operazioni di portabilità del numero di telefono per ottenere l'accesso agli account dell'utente. Rafforzare le procedure di verifica dell'identità nelle operazioni di portabilità può aiutare a prevenire il *SIM swap*.

Impatto dell'intelligenza artificiale sulle tecniche di ingegneria sociale

Le forze di polizia si trovano sempre più spesso a investigare reati che coinvolgono in maniera significativa l'uso dell'intelligenza artificiale (AI).
Le tecniche di ingegneria sociale utilizzate nel furto di identità possono essere amplificate negativamente da un uso distorto dell'AI. L'intelligenza artificiale può essere utilizzata per creare messaggi SMS fraudolenti altamente personalizzati, aumentando la probabilità che le vittime cadano nella trappola. Gli algoritmi di *machine learning* possono analizzare i dati personali disponibili online per generare messaggi che sembrano autentici e credibili. Le tecnologie di sintesi vocale basate sull'AI possono imitare le voci di persone reali o generare voci convincenti, rendendo le chiamate *vishing* ancora più persuasive. Inoltre, i *chatbot* AI possono automatizzare le chiamate fraudolente, aumentando il volume degli attacchi. Gli strumenti di AI possono creare email di *phishing* altamente sofisticate che imitano perfettamente le comunicazioni di istituzioni legittime e possono adattare le strategie in tempo reale per massimizzare l'efficacia.

L'intelligenza artificiale può essere utilizzata per generare siti web falsi che imitano perfettamente quelli legittimi, inclusi layout, design e contenuti. Inoltre, l'AI può aiutare a posizionare questi siti clone nei risultati dei motori di ricerca, aumentando le probabilità che le vittime vi accedano. Sebbene meno comune, l'uso dell'intelligenza artificiale può facilitare la raccolta di informazioni personali necessarie per il SIM swap attraverso la profilazione delle vittime e l'analisi dei dati disponibili online. Lo *spoofing* rappresenta una componente preoccupante del furto di identità, dove gli attaccanti possono mascherare la loro identità reale utilizzando indirizzi email, numeri

di telefono o indirizzi IP falsificati. L'AI può aumentare l'efficacia dello *spoofing* creando identità finte credibili, aumentando la difficoltà per le vittime di distinguere tra comunicazioni genuine e fraudolente.

In sintesi, l'AI può potenziare le tecniche di ingegneria sociale utilizzate nel furto di identità, aumentando l'efficacia delle truffe e la difficoltà per le vittime di riconoscere le frodi.
Di seguito, le principali attività svolte nel corso del 2024.

Oscuramento 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 Rolex
Nel mese di marzo 2024 personale del Centro Operativo per la Sicurezza Cibernetica di Perugia ha eseguito 8 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 riscontrano 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 (ex art. 415 c.p.p.), 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 per la Sicurezza Cibernetica e la collaborazione della Stazione Carabinieri di Marcianise, sono stati effettuati prevalentemente a Napoli, Caserta ed in Spagna.
L'attività illecita riscontrata nel corso delle indagini è riconducibile ai fenomeni criminali c.d. *phishing*, *hacking* e *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, 4 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.

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 e per la Sicurezza Cibernetica ed effettuata in collaborazione con l'Ufficio dell'Esperto per la Sicurezza presso l'Ambasciata d'Italia a Tirana, ha eseguito 9 decreti di perquisizione nei confronti di 21 indagati e delle sedi di 2 società energetiche e di 12 call center appaltati, 3 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 (Albania).

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 delle società energetiche e dei 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 9 milioni di euro ed ha riguardato oltre 1000 utenti truffati.

Esecuzione Mandati di Arresto Europeo

Nel mese di agosto Personale del Servizio Polizia Postale e per la Sicurezza Cibernetica, del Centro Operativo per la Sicurezza Cibernetica di Napoli e della Sezione Operativa per la Sicurezza Cibernetica di Salerno, coadiuvato da operatori della Direzione della Polizia giudiziaria della Polizia Nazionale francese, ha dato esecuzione a due Mandati di Arresto Europeo e ad un decreto di perquisizione locale e personale, emessi dalla Procura della Repubblica presso il Tribunale di Roma nei confronti di quattro soggetti stranieri[5], appartenenti ad un'associazione a delinquere finalizzata

[5] Un cittadino ucraino, un cittadino francese, un cittadino omanita e un cittadino russo.

alla commissione di reati contro il patrimonio e di criminalità informatica.
L'attività in questione scaturisce dalla cooperazione di polizia giudiziaria avviata con le omologhe autorità francesi che ha consentito di disvelare l'esistenza di un sodalizio criminale che, dopo aver attaccato il sistema informatico di una società di transazione di criptovalute, ha sottratto criptovalute per un valore di circa 14,42 milioni di dollari, effettuando una serie di trasferimenti ed operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
Gli approfondimenti investigativi, anche di tipo tecnico, hanno consentito di individuare ed arrestare gli indagati in un *resort* della provincia di Salerno, ove gli stessi si sono recati con volo privato, al fine di garantire il proprio anonimato

Operazione Taken Down
Nel mese di novembre, il Centro operativo per la sicurezza cibernetica di Catania, con il coordinamento del Servizio Polizia Postale e per la Sicurezza Cibernetica ha eseguito 88 perquisizioni sull'intero territorio nazionale e 14 perquisizioni in Gran Bretagna, Paesi Bassi, Svezia, Svizzera e Romania, nell'ambito di un'operazione volta al contrasto del fenomeno delle IPTV illegali.
L'operazione, coordinata dalla Procura della Repubblica di Catania, ha registrato il supporto degli organismi internazionali di EUROJUST ed EUROPOL, nonché della rete operativa @ON (*Operation Network*).
Nel medesimo contesto, la polizia croata ha eseguito 13 ordinanze di custodia cautelare nei confronti di altrettanti indagati.
L'attività investigativa ha consentito di smantellare una complessa infrastruttura informatica, dedita allo streaming illegale di segnali audiovisivi e contenuti multimediali ad accesso condizionato.
L'infrastruttura, gestita da un sodalizio criminale presente in Italia e con ramificazioni in diversi stati esteri, realizzava un giro illegale di affari di oltre 250 milioni di euro mensili, servendo il servizio illegalmente ad oltre 22 milioni di utenti finali.

Operazione Trade Scam
Nel mese di dicembre, la Polizia Postale ha dato esecuzione due ordinanze di custodia cautelare in carcere con estensione in campo internazionale, a carico di altrettanti cittadini albanesi, a capo di un'organizzazione criminale finalizzata alla commissione dei reati di truffa e di autoriciclaggio. Il provvedimento è stato emesso nell'ambito dell'operazione "*Trade Scam*", condotta dagli investigatori del Centro Operativo per la Sicurezza Cibernetica di Torino, sotto la direzione della locale Procura della Repubblica e con il coordinamento del Servizio Polizia Postale e per la Sicurezza Cibernetica. Alla fase esecutiva, sul territorio albanese, con il coordinamento internazionale

di EUROJUST e la collaborazione della SPAK albanese[6], gli operatori della Polizia postale, in sinergia con l'Ufficio dell'Esperto per la Sicurezza italiano in Albania, oltre a dare esecuzione all'ordinanza di custodia cautelare, hanno contestualmente sequestrato, anche per equivalente, di circa 4.000.000 di euro in ordine al delitto di truffa e di circa 500.000 euro per il delitto di autoriciclaggio.

Cyberterrorismo

Tra le attività istituzionali svolte dal Servizio Polizia Postale e per la Sicurezza Cibernetica una componente di estremo rilievo è rappresentata dalla prevenzione e contrasto dei fenomeni a carattere estremista che si esprimono sulla rete e possono determinare rischi per l'ordine e sicurezza pubblica nonché per la continuità di gestione delle infrastrutture critiche.

Gli ambiti peculiari di intervento sono rappresentati in primis dal radicalismo religioso di matrice jihadista, con particolare riguardo nel 2024 alla propaganda radicale di Hamas svolta in chiave anti – Israeliana; tale propaganda si affianca alla proliferazione mediatica jihadista realizzata ad opera di gruppi diversi quali ISIS - Daesh e Al Qaeda, i quali mantengono una forte capacità comunicativa in particolare su social network e applicazioni di messaggistica non *mainstream*.

Di rilievo sono state le attività condotte nel contrasto dell'accelerazionismo neonazista, fenomeno che aderisce sempre di più alla fascia giovanile – adolescenziale.

Ancora, attraverso i C.O.S.C. e in raccordo con le D.I.G.O.S., è stato proseguito il monitoraggio di movimenti antagonisti e anarchici, allo scopo di individuare informazioni utili circa gli eventi di protesta radicale; in particolare tra le tematiche osservate vanno segnalate l'introduzione del DDL sicurezza, il movimento della c.d. "*intifada studentesca*" nonché l'ambientalismo militante.

Nel corso del 2024 la Sezione Cyberterrorismo ha provveduto a prendere parte a vari tavoli di lavoro – in particolare presso EUROPOL – inerenti la collaborazione con gli ISP – *Internet Service Provider* e le società proprietarie dei maggiori social network. In tal senso, le riunioni hanno consentito di sottoporre questioni di rilievo quali la trattazione di segnalazioni emergenziali ex art. 18 D.S.A e art. 14 co. 5 T.C.O; sono state gestite nel corso del 2024 nr. 45 segnalazioni emergenziali originate da 10 diversi ISP – Internet Service Provider.
La I ^ Sezione Cyberterrorismo costituisce inoltre il punto di contatto nazionale della rete *EUROPOL IRU - Internet Referral Unit*, coordinata dal Centro E.C.T.C. di *EURO-*

[6] Procura Speciale deputata al contrasto della corruzione e della criminalità organizzata.

POL (European Counter Terrorism Center) – per il monitoraggio dei contenuti terroristici *online*, e partecipa insieme agli operatori di polizia di altri paesi ai cd. "*action day*" promossi in tale ambito, con notevoli risultati operativi. Durante il 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 ad account presenti sui social e applicazioni 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 preso di mira un'ampia gamma di contenuti illeciti, tra cui il c.d. *hate speech*, 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.

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 **295.000** spazi web oggetto di approfondimento investigativo; tra questi, oltre **2.300** risorse digitali sono state oscurate poiché caratterizzate da un contenuto illecito.

Estremismo religioso

Nel corso del 2024 sono state svolte numerose attività di polizia giudiziaria finalizzate all'individuazione di soggetti radicalizzati o già affiliati ad organizzazioni terroristiche strutturate; in merito, alcuni C.O.S.C. hanno fatto ricorso a tecniche avanzate quali le c.d "*operazioni undercover*", riuscendo a penetrare in modo più significativo le reti terroristiche che si esprimono sul *web*.

Le attività di polizia giudiziaria e il monitoraggio O.S.Int hanno riguardato sia canali ufficiali di produzione mediatica, sia gruppi non ufficiali dove l'ideologia jihadista violenta viene comunque divulgata tra gli aderenti.

Diversi i centri mediatici di maggiore rilievo riconducibili a ISIS – Daesh, oggetto di osservazione anche tramite mirati report di Europol che supportano gli operatori specializzati nelle ricerche informative; tra i centri si annoverano: Al-Naba, Al-Battar Foundation, Al-Dar' al-Sunni Foundation, Al-Azaim , Al-Raud and Ilam, Al Hayat media center.

Per quanto attiene le formazioni riconducibili ad Al Qaeda invece vanno citati i seguenti centri mediatici: As-Sahab Establishment for Media Production, Al-Malahem Media, Al-Andalus Establishment for Media Production, Al-Basirah Media Establishment.

Terrorismo accelerazionista

Nel corso del 2024 è stato possibile rilevare come il fenomeno sia in evoluzione e accanto alle sigle storiche quali *"AWD - AtomWaffenDivision"* e *"The Base"* se ne affiancano di nuove, i cui simboli risultano spesso inediti e di difficile individuazione attraverso i *tool* ordinari di ricerca; si è osservata peraltro, in particolare online, la sovrapposizione dell'estremismo accelerazionista con l'ideologia jihadista, in particolare in locandine e infografiche che riportano contenuti radicali misti.

Contrasto alla disinformazione

La tematica ha assunto una centralità peculiare nel corso del 2024 con particolare riguardo alle seguenti tematiche: narrazioni inerenti il conflitto Russo Ucraino; conflitto militare in Medio Oriente; elezioni presidenziali statunitensi; false narrazioni nelle elezioni presidenziali in Moldavia.

Ancora tra le narrazioni ricorrenti vanno annoverate quelle concernenti l'Unione Europea, volte a destabilizzarne le istituzioni o a darne una rappresentazione debole nel contesto internazionale.
Le tecniche adottate spaziano dall'impiego di *botnet* al ricorso al *deepfake*, sino all'utilizzo di *tool* di Intelligenza Artificiale che rendono estremamente complessa l'attività di *debunking*.

Nell'ambito della disinformazione si aggiunge che il Servizio Polizia Postale ha svolto un monitoraggio dei profili *fake* di soggetti istituzionali, segnalandoli ai social network per la conseguente chiusura in quanto ingannevoli.
Sul piano statistico, nel corso del 2024 nell'ambito del cyberterrorismo sono state svolte 56 perquisizioni, sono stati gestiti 179 SIENA in ingresso e sono stati generati 40 casi SIENA inerenti indagini dei C.O.S.C. e della Sezione presso il Servizio.

Si riepilogano di seguito le attività di maggiore rilievo.

- Il C.O.S.C. 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"*, *"The Base"*. In tale contesto si è proceduto ad eseguire nei confronti di due indagati italiani la misura cautelare dell'obbligo di permanenza domiciliare.

- Il C.O.S.C. 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 41 TULPS.
- I C.O.S.C. 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.
- Il C.O.S.C. 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 svolta 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 un software idoneo a svolgere attività di *hacking*.
- 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, D.C.P.P, Polizia Scientifica e 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.
- Il C.O.S.C. di Firenze ha dato esecuzione al decreto di perquisizione, emesso dalla Procura della Repubblica di Firenze a carico di un minore di anni 18, resosi responsabile della pubblicazione, sulla piattaforma TikTok, di un video afferente

alla strage compiuta nel 2014 da "Elliot Rodger" (strage avvenuta in un campus universitario statunitense). Il video veniva accompagnato da un messaggio testuale in cui l'usuario del profilo scriveva, in lingua inglese, di essere vittima di bullismo da parte di due coetanei e di averne abbastanza, aggiungendo poi che avrebbe invitato uno di loro a incontrarlo e che l'avrebbe picchiato e minacciato con un coltello, ribadendo la sua volontà di ottenere vendetta, entro breve, nei confronti di coloro che lo schernivano.

- Il Servizio Polizia Postale e per la sicurezza Cibernetica unitamente a personale dei C.O.S.C. di Perugia, Milano, Napoli, Torino e Firenze e delle D.I.G.O.S. di Perugia, Napoli, Brescia, Massa Carrara e Alessandria, ha dato esecuzione ai decreti di perquisizione emessi dalla Procura della Repubblica presso il Tribunale Ordinario di Perugia nei confronti di cinque soggetti indagati per i reati di cui all' art. 270 bis c.p. L'attività di indagine svolta nell'ambito del contrasto al radicalismo islamico online di matrice jihadista ha interessato alcuni gruppi *Whatsapp* in cui i soggetti si sono resi responsabili della pubblicazione di contenuti propagandistici radicali afferenti all'Islamic State.
- In data 17 dicembre 2024 personale del C.O.S.C. di Roma e della locale D.I.G.O.S ha dato esecuzione al decreto di perquisizione, personale, locale e informatica emesso dalla Procura della Repubblica presso il Tribunale per i Minorenni di Roma nei confronti di un soggetto, responsabile della pubblicazione di contenuti estremisti online afferenti l'area del suprematismo/accelerazionismo. L'attività d'indagine ha avuto origine a seguito di una segnalazione emergenziale pervenuta alla sala operativa del C.N.A.I.P.I.C. dalla società Meta inerente un utente geolocalizzato in Italia, titolare di un profilo Instagram contenente video con riferimenti a noti stragisti dell'area suprematista/accelerazionista, nonché foto di un soggetto equipaggiato con elmetto militare, un corpetto di tipo "*combat*", un pugnale ed una maschera di tipo "*skull mask*".
- In data 19 dicembre 2024 i Centri Operativi per la Sicurezza Cibernetica di Milano, Venezia, Firenze, Roma, Napoli, Bari e Roma e le locali D.I.G.O.S, hanno dato esecuzione ai decreti di perquisizione locale, personale ed informatica emessi dalla Procura della Repubblica presso il Tribunale Ordinario di Milano e dalla Procura della Repubblica presso il Tribunale per i Minorenni di Milano nei confronti di dodici soggetti, indagati per i reati di cui all'art. 604 bis c.p. Le posizioni sono emerse all'esito di un'indagine svolta dal C.O.S.C di Milano nell'ambito del contrasto dei fenomeni collegati alla propaganda estremista realizzata attraverso gruppi attivi sulla piattaforma *Telegram* e in particolare su canali e gruppi in cui sono stati divulgati contenuti di ispirazione nazi-fascista orientati all'affermazione della superiorità della razza bianca, nonché all'odio razziale nei

confronti degli ebrei e all'istigazione a commettere atti di violenza per motivi etnici e razziali, inclusi video inneggianti alla jihad.

Commissariato di P.S. online

Il Commissariato di PS online, raggiungibile attraverso la url https://www.commissariatodips.it/, è un importante strumento di interazione con i cittadini, utile per inviare segnalazioni, acquisire informazioni sulle più attuali fenomenologie criminali in rete e rivolgersi ai poliziotti della Polizia Postale e per la Sicurezza Cibernetica in qualsiasi momento e da qualunque località.

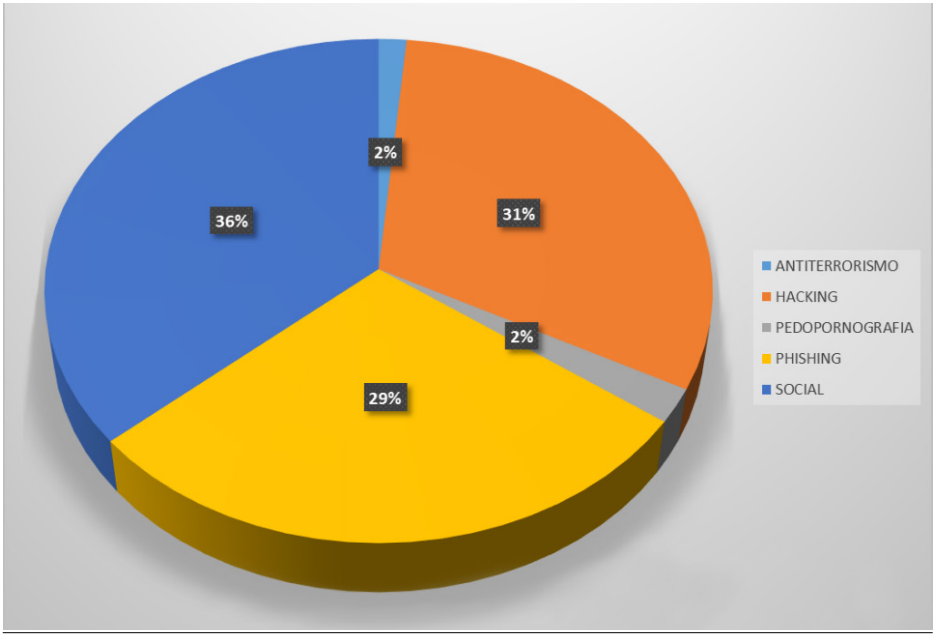
Il sito riceve quotidianamente centinaia di messaggi con richieste di informazioni riguardanti spazi virtuali con possibili contenuti illegali, condotte illecite subite e richieste di aiuto per superare difficoltà e problematiche.

L'analisi delle oltre **84.000 segnalazioni** ricevute ha evidenziato che in molti casi gli utenti non adottano quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare molti degli attacchi informatici e il perpetrarsi di attività delittuose.

Segnalazioni pervenute al Commissariato di P.S. online nel 2024	Antiterrorismo	1.232
	Hacking	26.278
	Pedopornografia	1.854
	Phishing	24.361
	Social	30.561
	TOTALE	**84.286**

Richieste di informazioni pervenute al Commissariato di P.S. online nel 2024	23.490
Visite al portale web del Commissariato di P.S. online nel 2024	2.925.314
Accessi al portale web del Commissariato di P.S. online nel 2024	53.816.209

2024 - Tipologia segnalazioni inoltrate dai cittadini attraverso il portale www.commisariatodips.it



Fonte - Mattinale Polizia Postale e per sicurezza cibernetica © 2025

Nelle sezioni *"alert"* e "approfondimenti", efficaci strumenti di prevenzione messi a disposizione del cittadino, l'utente può informarsi consultando gli aggiornamenti e i consigli della Polizia Postale.

Tra i fenomeni segnalati con maggior frequenza si riscontrano le truffe perpetrate con la 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 che informano di presunti accessi anomali su conti correnti bancari al fine di carpire i dati di accesso dei titolari; i furti di profili social e false comunicazioni di assistenza per il recupero degli account rubati.

In continua crescita il numero delle segnalazioni di estorsioni a sfondo sessuale, di truffe sugli acquisti online, che colpiscono sia acquirente che venditore e di false proposte di trading online.

L'attività più delicata ha riguardato la gestione delle segnalazioni di cittadini che manifestano situazioni di disagio e minacciano di compiere gesti estremi. Le richieste di aiuto, in alcuni casi, vengono inviate direttamente dagli utenti sul sito tramite il servizio "Segnala online"; in altri, sono ricevute dalla redazione di note trasmissioni televisive che, successivamente, le inoltrano al Commissariato di PS online. In tali circostanze, agli operatori del Commissariato è richiesto un tempestivo e coordinato intervento, che coinvolge anche altri uffici territoriali delle Forze dell'Ordine, per raggiungere nel più breve tempo possibile la persona in pericolo. Nel 2024 gli interventi dedicati al salvataggio delle vite umane sono stati 197.

La popolarità del sito è dimostrata dall'elevato numero di accessi, che sono stati nel periodo di riferimento oltre **53.800.000**

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, con l'obiettivo di far comprendere agli adolescenti le conseguenze che possono derivare dall'uso distorto del *web*.

Una coinvolgente campagna realizzata periodicamente è il format teatrale #cuoriconnessi, dedicato agli studenti delle scuole. Ogni anno, in occasione del *"Safer Internet Day - giornata mondiale per la sicurezza in rete"*, viene organizzato un evento, in cui il conduttore concentra l'attenzione del pubblico sull'importanza delle parole. Attraverso filmati, letture, musiche e testimonianze dirette, vengono fornite agli spettatori informazioni utili alla corretta navigazione in rete, per stimolare nei ragazzi una sempre maggiore consapevolezza della gravità delle azioni commesse online, in relazione all'impatto prodotto nella vita reale.

Nell'anno 2024, l'evento relativo all'ottava edizione si è svolto il 6 febbraio ed è stato seguito in diretta *streaming* da più di **225 mila** studenti.

Tra le iniziative più significative, la campagna itinerante "Una vita da Social", che negli ultimi anni ha anche travalicato i confini nazionali. A bordo del *truck,* una vera e propria aula multimediale che contraddistingue l'iniziativa, e presso gli istituti scolastici, gli operatori della Specialità incontrano scolaresche e cittadini, a cui illustrano le più attuali insidie della rete e forniscono utili strumenti per un corretto utilizzo del *web*.

L'impegno profuso dalla Polizia Postale e per la Sicurezza Cibernetica nell'azione di sensibilizzazione e informazione ha consentito, nell'anno 2024, di realizzare incontri

con **25.767** docenti, **13.403** genitori e oltre **420.000** studenti. L'attività è proseguita anche nel periodo di pausa estiva con il "*Cybersummer*", nuova iniziativa che ha permesso di incontrare bambini e ragazzi presso i centri estivi e i luoghi di aggregazione giovanile.
Le recenti attività di analisi dei fenomeni online sui minori evidenziano un costante e progressivo abbassamento dell'età di accesso ed esposizione ai contenuti e ai dispositivi digitali e il conseguente e preoccupante aumento delle denunce, relative a fatti illeciti le cui vittime hanno un'età inferiore ai 13 anni.

Nell'ottica di raggiungere anche i più piccoli, sono state attivate nuove, mirate iniziative, tra le quali assume particolare rilievo la collaborazione con la Fondazione Geronimo Stilton e Elisabetta Dami[7] – autrice e creatrice dell'omonimo personaggio di fantasia, che ha portato alla realizzazione del libro "Sulle Tracce dell'Hacker", un testo redatto con la collaborazione degli esperti della Specialità, tra i quali gli psicologi dell'Unità di Analisi del Crimine Informatico del Servizio Polizia Postale e per la Sicurezza Cibernetica, dedicato ai bambini, alunni della scuola dell'infanzia e primaria e a coloro i quali li accompagnano nella lettura.

Sempre nell'ottica del coinvolgimento della totalità del nucleo familiare, al temine del libro è inserito un "***Cyber Manuale***" con "Consigli per tutta la famiglia", con spiegazioni semplici su tutto ciò che riguarda il web, cenni sull'Intelligenza Artificiale e dieci regole da condividere con amici e familiari.
Il prodotto editoriale è stato lanciato nel mese di ottobre con diverse iniziative, tra le quali un evento promosso il giorno 7 presso l'Auditorium Parco della Musica, alla presenza di oltre **2400** bambini delle scuole primarie di Roma e provincia.
Grazie a Google, partner del progetto, sono state acquistate e donate alla Polizia Postale 12mila copie, già in parte distribuite sul territorio nazionale nel corso delle tappe della campagna itinerante "una Vita da Social". La Fondazione Geronimo Stilton donerà parte dei proventi della vendita del volume alla Fondazione "Marco Valerio", fondo di assistenza della Polizia di Stato che interviene mediante l'erogazione di contributi annuali a favore dei figli dei dipendenti in servizio ed in pensione affetti da patologie fino al diciottesimo anno di età.

In occasione delle festività natalizie, infine, dopo la positiva esperienza dello scorso anno, è stato veicolato, attraverso il portale e i canali social, il "***Calendario dell'Avvento Cyber***" del 2024, per accompagnare gli utenti al Natale con curiosità, consigli

[7] Recentemente insignita del titolo di "poliziotto ad honorem", riconoscimento assegnato a personalità della società civile che si sono distinte per la diffusione dei valori condivisi dalla Polizia di Stato, e che con la nomina divengono ambasciatori di questi ideali tra i cittadini.

e suggerimenti per navigare sicuri online, diffusi dagli operatori della Polizia Postale con dei brevi video di pillole di sicurezza digitale.

La Quinta Divisione del Servizio Polizia Postale

All'interno del Servizio Polizia Postale è incardinata la quinta divisione specializzata in Information Technology (IT) per supportare le operazioni cibernetiche e le indagini di *digital forensics*. Questa divisione svolge un ruolo fondamentale nel garantire la sicurezza informatica e nel collaborare con enti pubblici e privati per l'innovazione scientifica e tecnologica. Ecco alcuni dei principali compiti della divisione:

- garantire il supporto tecnico-operativo alle attività d'istituto della Specialità in materia di sicurezza cibernetica e *digital forensics*;
- curare i rapporti con Enti e Istituzioni, pubbliche e private, attive nel campo della ricerca e dell'innovazione scientifica, per il costante aggiornamento di metodologie e soluzioni tecnologiche nonché concorre alla definizione dei piani di formazione specialistica;
- predisporre la pianificazione delle acquisizioni IT e la programmazione triennale dei fabbisogni con la conseguente gestione dei contratti di fornitura e delle procedure di acquisto;
- coordinare, nei settori tecnici di rispettiva competenza, le articolazioni territoriali della Specialità anche in relazione all'analisi delle esigenze ed alla realizzazione di nuovi sistemi IT a supporto delle attività info-investigative;
- gestire e implementare l'infrastruttura tecnologica del Servizio attuando gli indirizzi e le politiche di sicurezza IT delineate dai competenti uffici della Polizia di Stato, secondo gli standard e le normative di settore;
- gestire tutti gli *asset* tecnologici della Specialità a livello nazionale e svolgere le funzioni di *focal point* per gli accessi alle banche dati istituzionali ed investigative in uso al Servizio.

In tema di Innovazione e Ricerca Tecnologica, presso la predetta divisione, è stato istituito **l'AiLab4Cyber**, ovvero un laboratorio di ricerca nel settore dell'intelligenza artificiale. In particolare, il predetto laboratorio provvede ad analizzare gli impatti

del Regolamento Europeo sull'Intelligenza Artificiale in relazione ai modelli e sistemi di IA idonei a supportare le investigazioni nel settore cibernetico e dell'analisi delle immagini per il contrasto alla pedopornografia.
Vengono, altresì, svolte attività di ricerca di mercato per comprendere le nuove tecnologie disponibili e in via di sviluppo. In merito, sono state consolidate collaborazioni con il mondo accademico attraverso la condivisione di progetti innovativi che vedono l'impiego dell'Intelligenza Artificiale sia nel settore delle investigazioni di pertinenza della Specialità che nella protezione delle infrastrutture critiche.

Per quanto attiene le dotazioni tecnologiche a supporto delle investigazioni, nel corso del 2024 si è provveduto a dare particolare impulso all'avvio di un rilevante programma di potenziamento, atteso il recente incremento dell'organico della Specialità. In particolare, sono state acquisite:

- tecnologie a supporto delle attività di *digital forensics* mediante la fornitura di nuove apparecchiature hardware ad elevate prestazioni nonché tecnologie software per l'acquisizione e l'analisi forense di dispositivi digitali;
- strumentazioni di ultima generazione volte all'analisi degli incidenti informatici;
- piattaforme di servizi info-investigativi volte a supportare le attività d'indagine;
- postazioni di lavoro fisse e mobili per le esigenze degli uffici territoriali e centrali.

Oltre alle predette attività di ampliamento sopra descritte, si è provveduto, altresì, a finalizzare numerose procedure amministrative volte al rinnovo dei contratti già in essere e concernenti le dotazioni strumentali in uso alla Specialità e necessarie a garantire le attività d'Istituto.

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

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

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

Inoltre, sono stati significativi gli sforzi della Divisione sia in ambito formativo, con la realizzazione, in tema di sicurezza informatica, di moduli sull'*awareness* nonché sull'uso corretto e responsabile delle tecnologie di IA relativamente ai benefici ed ai possibili rischi associati.

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

Elementi sul cybercrime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo, IBM]

Il cybercrime finanziario continua a evolversi, dominato da gruppi internazionali ben strutturati e organizzati.

Nell'analisi che segue, presento e commento i risultati di alcune rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2024, ed evidenzio alcune tendenze che potremmo osservare nel 2025. Questo lavoro è reso possibile anche grazie ai contributi dei gruppi di ricerca all'interno di IBM, i dati estratti dalla rete mondiale di IBM Security Trusteer e al lavoro quotidiano dei colleghi IBM che desidero ringraziare.

Tutte le fonti consultate sono elencate nella bibliografia al termine dell'articolo.

Attacco alle identità

Uno dei cambiamenti di maggior impatto che abbiamo osservato nel corso del 2024 è stata la crescita degli attacchi verso le identità [1]. Contestualizzato all'ambito finanziario questo si è tradotto spesso nel furto delle credenziali d'accesso e dei fattori autorizzativi dei sistemi bancari o di pagamento, per successive transazioni fraudolente (Financial Theft - tecnica MITRE ATT&CK T1657).

Da più parti si parla del fatto che gli hacker prediligono il *log-in* all' *hack-in*, a evidenziare che l'acquisizione e abuso di credenziali di account valide (Valid Accounts – tecnica T1078) ha eguagliato in frequenza il phishing in tutte le sue forme (T1566) come tecnica di accesso iniziale. Le due tecniche sono fortemente interdipendenti in quanto il phishing è quasi sempre usato per acquisire credenziali di account valide. Subito a ruota segue lo sfruttamento di debolezze nelle applicazioni esposte su Internet (Exploit Public-Facing Application - T1190), l'abuso di servizi remoti esterni (T1133), e la compromissione della Supply Chain (T1195). La frequenza e la distribuzione delle tecniche evidenziano come si preferisca attaccare i clienti, in quanto anello debole, piuttosto che la banca stessa.
Questo adattamento delle tecniche di accesso ha un legame forte con la crescita di InfoStealer, malware specializzati nel furto di informazioni, che alimentano floride attività di compravendita di credenziali nel dark web.

Un fenomeno iniziato già da tempo, X-Force riporta come gli InfoStealer erano già cresciuti del 266% nel corso del 2023 [1][1]. Misurazioni puntuali indicano che gli InfoStealer stanno gradualmente soppiantando i malware specializzati nelle frodi bancarie, già in decrescita da qualche anno.
Diminuisce la soglia di accesso alla frode finanziaria, con strumenti facilmente reperibili e un minore livello di competenze richieste agli attaccanti.

Un anno di cybercrime finanziario

Per molti anni il settore finanziario è stato il più attaccato a livello mondiale, sorpassato solo in tempi recenti dal settore manifatturiero, per la sua fragilità agli attacchi ransomware.

Limitando l'analisi all'Europa, il settore finanziario è stato vittima del 18,2% degli attacchi nel corso del 2023 [1][2], con l'Italia che ha attratto circa l'8% degli attacchi verso l'Europa, dietro Germania, Danimarca e Portogallo.

Enisa riporta che il settore finanziario/assicurativo è stato il terzo settore più attaccato in Europa, nel periodo luglio 2023 – giugno 2024[3], con il 9% di tutti gli attacchi tracciati [2]. Sempre per Enisa, la minaccia principale sono stati i Distributed Denial of Service (DDoS) che sembrano colpire tutti i settori industriali. Il 12% degli attacchi DDoS tracciati ha avuto come obiettivo il settore finanziario [2].

L'Europa ha registrato la più alta percentuale di incidenti (32%) tra le cinque regioni geografiche, con un incremento anno su anno del 31%. Il malware è stata l'azione più osservata in termini oggettivi rappresentando il 44% degli incidenti [1].

Enisa individua alcune minacce prevalenti (*prime threats*) che si sono contraddistinte per la loro importanza e persistenza nel corso degli anni. Queste sono Ransomware, Malware, Social Engineering, minacce ai dati, minacce alla disponibilità (Denial of Service), e manipolazione di informazioni [2].
Ciascuna di queste minacce può avere aspetti rilevanti per il settore finanziario. Ransomware, social engineering, e minacce ai dati possono celare una data exfiltration (tattica MITRE ATT&CK TA0010) le cui conseguenze possono essere perdite finanziarie, danni reputazionali, e sanzioni normative.

---

1 Ultimi dati disponibili.

2 Ultimi dati disponibili.

3 Ultimi dati disponibili.

Nelle pieghe del social engineering forse la minaccia più grande agli utenti finali attraverso il phishing, i cui limiti sono definiti solo dalla fantasia dei cyber criminali.
Il phishing continua a essere il vettore di accesso principale degli incidenti di sicurezza informatica.

Secondo Verizon, il phishing e il "pretesto" via e-mail (pretexting) continuano a essere il vettore iniziale di accesso più frequente, rappresentando il 73% delle violazioni. La motivazione più frequente è quella finanziaria (95% degli incidenti) e i dati compromessi con maggior frequenza sono le credenziali (50% degli incidenti) [3]. Nel "pretesto" (pretexting) si usa una storia inventata, ad esempio una carta di credito bloccata, per carpire la fiducia della vittima e manipolarla fino a farle condividere informazioni sensibili, scaricare malware, inviare denaro a criminali o arrecare danni alla propria organizzazione.

Secondo CERTFin la percentuale di clienti attivi che hanno subíto un furto di credenziali, in Italia, è stato dello 0,14% nel mercato retail (consumatore finale) con un valore dimezzato rispetto all'anno precedente e 0,08% nel mercato corporate (aziendale), quest'ultimo dato in forte aumento rispetto all'anno precedente. Delle vittime di furto di credenziali, una frazione che va dal 23% (retail) al 30% (corporate) ha poi realmente subito perdite [24 - dati 2023].

Si è notato un aumento del 71%, anno su anno[4] del volume di attacchi che utilizzano credenziali valide [1]. Per la prima volta in assoluto, l'abuso di account validi (T1078) è diventato il vettore di accesso più comune nelle reti, sistemi e applicazioni delle vittime, rappresentando il 30% di tutti gli incidenti a cui X-Force ha risposto [1], assieme al phishing (T1566) anche questo al primo posto con 30% degli incidenti gestiti. A pochissima distanza, con il 29% degli incidenti gestiti c'è lo sfruttamento delle *public-facing applications* (T1190), che racchiude lo sfruttamento malevolo di tutte le applicazioni, su qualsiasi protocollo, accessibili tramite rete.

Altra osservazione di notevole importanza è la crescita del 266% nell'uso InfoStealer generici. Gruppi che in precedenza si erano specializzati in ransomware mostrano un crescente interesse per gli InfoStealer [1]. Alcuni nuovi InfoStealer, come Rhadamanthys, LummaC2 e Strela Stealer hanno debuttato, dimostrando subito un'attività molto prolifica.
Anche in Italia il phishing continua a essere una delle minacce principali. La Polizia Postale ha ricevuto circa 24000 segnalazioni nel corso del 2024, pari al 28.9% di tutte le segnalazioni ricevute attraverso il portale Commissariato di P.S. online [4].

4 2023 vs 2022, ultimi dati disponibili.

L'analisi delle principali campagne di attacco del 2024 mostra che la frode verso il settore finanziario avviene prevalentemente attraverso i seguenti meccanismi, spesso combinati tra di loro:

- Phishing, in tutte le sue forme (SMishing/SMSishing, Quishing/QRishing), per il furto iniziale di credenziali di accesso (credential theft) oppure di altri dati personali (telefono, codice fiscale, e-mail) sempre combinata con una successiva interazione con un finto operatore per la sottrazione dei fattori di autenticazione forte o dispositivi mancanti;
- InfoStealer e malware specializzati nel furto di credenziali e fattori addizionali di autenticazione, o manipolazione di una transazione;
- Manipolazione del pagatore, inducendolo a emettere un ordine di pagamento online, oppure convincendolo a recarsi allo sportello e fare un'operazione dispositiva;
- Finte App e aggiornamenti di App, all'apparenza sia di banking che no;
- E infine, ma in misura inferiore, con l'attacco diretto all'infrastruttura dell'istituzione bancaria sfruttando vulnerabilità spesso note ma ancora non fissate.

Il regolamento AGCOM sull'utilizzo dei caratteri alfanumerici per identificare il mittente degli SMS[5], con il blocco degli SMS con Alias provenienti dall'estero, ha contribuito a contrastare una porzione rilevante di messaggi SMS usati per realizzare tentativi di frode. Nell'SMS Alias il mittente di un SMS viene specificato come stringa alfanumerica (esempio il nome di una banca) piuttosto che il numero di telefono. L'SMS Alias è stato sfruttato nel recente passato per attribuire autorevolezza al mittente, traendo in inganno il destinatario del messaggio. Entrato in vigore in più fasi, tra novembre 2023 e maggio 2024, gli impatti reali della delibera AGCOM si potranno misurare solo nei prossimi mesi.

Con l'irrobustimento delle soluzioni di difesa tecnologiche e con sistemi di autenticazione e algoritmi antifrode più efficaci, i *threat actor* (attori cybercriminali) stanno sfruttando anche innovative quanto fantasiose ragioni per indurre la vittima a recarsi alla sua filiale e fare operazioni dispositive allo sportello, scavalcando così molti dei controlli effettuati invece nelle operazioni on-line.

In generale, sia nel mercato retail che in quello corporate, prosegue la diminuzione di attacchi meramente tecnologici, con un parallelo incremento di azioni di coercizione della vittima.

[5] Delibera 12/23/CIR - Regolamento sull'utilizzo dei caratteri alfanumerici che identificano il soggetto mittente nei servizi di messaggistica aziendale (SMS ALIAS)

Phishing verso il settore finanziario italiano

Nel corso del 2024 è continuata la graduale decrescita nel numero di pagine phishing attivate. Questo segue una tendenza mondiale osservata anche da altri operatori [5]. Altre fonti confermano lo stesso andamento al livello italiano [6].

Il picco del phishing si era avuto nel corso del 2022 [5]. Lo stesso anno Akamai aveva stimato che il 20.1% di tutti i domini registrati erano stati a supporto di attività malevole [7], per un totale di circa 13 milioni di nuovi domini malevoli al mese, a livello globale.

In ambito finanziario, uno dei fattori determinanti di decrescita è stato l'entrata in vigore della direttiva europea PSD2 (second Payment Service Directive) [18], a partire dal settembre 2019 ma con alcune deroghe fino al dicembre 2020. La PSD2 impone alcuni meccanismi tecnici ai pagamenti (definiti nei Regulatory Technical Standards o RTS) il più rilevante dei quali ai fini del contrasto del phishing è stato quello sull'autenticazione forte del cliente, o Strong Customer Authentication (SCA). Questo ha imposto una complessità maggiore negli attacchi e necessariamente cambiato il modus operandi degli attaccanti. Prima della PSD2, nella maggior parte dei casi, bastava soltanto codice utente e PIN per fare login in un sito bancario e disporre un'operazione. Una buona campagna di phishing era in grado di catturare contemporaneamente username e password e permettere la transazione fraudolenta. Con la PSD2 questo non è più possibile, in quanto gli attaccanti ora devono impossessarsi anche dei fattori addizionali di autenticazione, generati al momento della transazione.

La SCA non è obbligatoria in tutte le transazioni, ma permette alcuni criteri di esenzione basati su livello di rischio, importo, ricorrenza e canale di pagamento. Questo ci consente di confrontare il tasso di frode su transazioni che hanno coinvolto la SCA, verso quelle senza, e trarre delle conclusioni sulla sua efficacia. Per le carte di pagamento emesse in Unione Europea, tra il 55% e 78% delle transazioni elettroniche hanno coinvolto Strong Customer Authentication, con differenze in base al tipo di transazione. Un risultato comune è che il tasso di frode per le transazioni con carta autenticate tramite SCA è stato inferiore al tasso di frode per le transazioni senza SCA [8].

Vale la pena anche ricordare che il prestatore di servizi di pagamento (intermediario finanziario nei pagamenti effettuati tramite il canale internet) deve assicurare il rimborso quando l'operazione di pagamento disconosciuta non è stata autorizzata con autenticazione forte[6].

[6] Artt. 10 e 12 del D.lgs. 11/2010.

È in corso una revisione del quadro normativo alla luce dei progressi tecnologici che ci sta guidando verso la nuova direttiva PSD3 e la PSR – Payment Service Regulation, la cui finalizzazione è prevista nel 2025. Uno degli obiettivi dell'iniziativa regolamentare è proprio rafforzare la protezione degli utenti e la fiducia nei pagamenti.

Il settore finanziario, anche in Italia, è da sempre obiettivo privilegiato dalle campagne di phishing per il furto di credenziali, siano esse di autenticazione a un sistema di banking online, oppure elementi distintivi di una carta di credito (PAN, CVV/CV2 e altri). Il furto di questi elementi è solo il primo passo per portare a termine una transazione fraudolenta all'insaputa del possessore del conto.

Lo studio che segue si basa sull'analisi di un campione di *oltre 510 campagne* di furto di credenziali per servizi bancari e sistemi di pagamento italiani tra il 1° gennaio e il 31 dicembre 2024, verificate individualmente e monitorate fino a completa disattivazione.
Questo insieme non rappresenta la totalità delle campagne di phishing che hanno colpito il nostro Paese, ma un campione così numeroso permette di fare analisi e trarre alcune conclusioni.
Limitandosi al settore finanziario italiano, in tutto il 2024 è stata osservata una media di circa 1,4 nuove pagine di phishing al giorno attivate e perfettamente funzionanti. L'Italia segue la tendenza mondiale di diminuzione di campagne di phishing, e questo è osservato anche da altri operatori [5] [6].

Le campagne analizzate hanno coinvolto 30 istituzioni finanziarie italiane. Ai primi 3 posti permangono esattamente le stesse istituzioni dell'anno precedente, che da sole hanno attratto il 52% di tutto il phishing dell'anno.

Dal punto di vista stagionale l'attività è decresciuta nel corso del primo semestre per raggiungere il picco minimo nel mese di agosto, che conferma una costante da quando facciamo rilevazioni su campagne italiane (**Figura 1**). L'attività è poi ripresa nella parte finale dell'anno. Anche se con una valenza statistica limitata, i primi giorni del 2025, fino alla data di scrittura di questo testo, sono state osservata una media di 2,1 nuove pagine di phishing al giorno, superiore rispetto alla media del 2024.
Il 38% di questi siti di phishing è stato ospitato negli Stati Uniti, un valore leggermente inferiore a quello dell'anno precedente, il 16% in Russia e solo il 2% in Italia. Il valore italiano era stato del 6% nel corso del 2023, e 11% nel 2022, a conferma di una tendenza in costante decrescita anno su anno.

Una delle novità emersa a partire dal 2023 è l'hosting su risorse Amazon (ospitate principalmente in Germania e Stati Uniti) che nel corso del 2024 ha contato per il 26%, in crescita rispetto all'anno scorso.

Queste analisi non prendono in considerazione i numerosissimi domini che lasciano immaginare banche o prodotti finanziari (domain squatting), oppure nomi che richiamano ad aggiornamenti o necessità di azione ma che non arrivano fino a completa attivazione. Questi domini sono almeno il doppio rispetto a quelli poi effettivamente attivati. In quest'ultima area è sempre vigile l'operazione di monitoraggio e proactive takedown (disattivazione) prima ancora che la campagna fraudolenta abbia inizio.

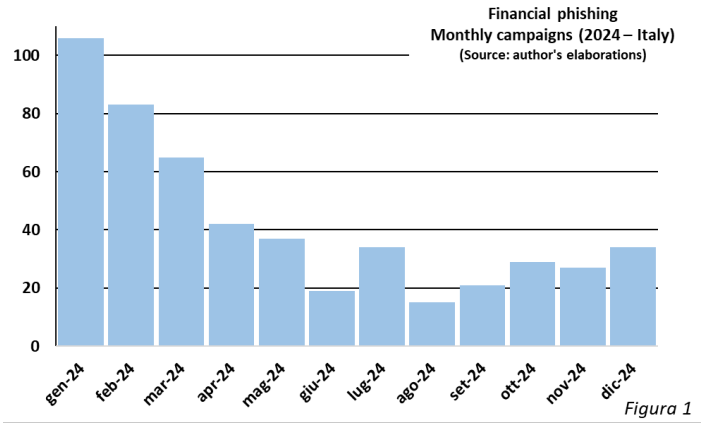


Figura 1

Uso del protocollo HTTPs

Il 98,6% delle URL di phishing attivate nel corso del 2024 ha usato il protocollo HTTPS, il cosiddetto HTTP "sicuro" che quindi, da ribadire in tutte le campagne di educazione alla sicurezza informatica, non è più un'indicazione sull'affidabilità o meno del sito. Un valore così alto, prossimo al 99%, è stabile dal 2022.

Tecnologie come HTTPS e l'SSL/TLS sono progettate per proteggere le comunicazioni tra client e server. L'icona del lucchetto nella barra indirizzi del browser può però creare la falsa illusione che un sito web sia attendibile. Questo interferisce molto con il giudizio che i visitatori danno del sito internet, e deve indubbiamente guidare le indicazioni che le organizzazioni forniscono ai propri clienti relativamente alla presenza di un lucchetto chiuso e dalla dicitura "https://" nella barra degli indirizzi come elementi per distinguere una pagina sicura da una non sicura. Se l'uso di una connessione HTTP di tipo semplice (http://) sicuramente *non* fornisce nessuna garanzia sulla controparte, l'uso del protocollo HTTPS, senza successive verifiche sul *tipo di certificato, chi lo ha emesso e per quali scopi*, parimenti non può darci nessuna indicazione di sicurezza.

Proprio per questa ragione Google Chrome, a partire dall'aggiornamento di settembre 2023, ha rimosso l'icona del lucchetto dalla barra dell'indirizzo per sostituirla con un'icona più neutrale [9].

La decisione sulla veridicità di una connessione HTTPS dovrebbe essere legata alla effettiva *validazione* del dominio. Nella totalità dei casi, i phisher usano domini con certificati di tipo Domain Validation (DV), la forma più semplice di validazione e quella proposta dai siti di web hosting per qualche euro o addirittura gratuitamente. I certificati di tipo Domain Validation, anche se in grado di garantire comunicazioni criptate e sicure attraverso connessioni HTTPS, poco o nulla dicono sulla autenticità di chi possiede il sito web al quale siamo collegati. Questa ambiguità viene sfruttata dai threat actor quando usano comunicazioni HTTPS. Non esiste nessuna forma di controllo sull'entità o sulla persona che richiede un certificato SSL/TLS per abilitare un sito al protocollo HTTPS, ma si controlla in automatico solo che chi richiede il certificato abbia il controllo del dominio in questione, cosa spesso ovvia.

I siti reali di banking italiani usano certificati di tipo Organization Validated (OV), o meglio ancora, Extended Validation (EV). Quest'ultimo tipo di validazione del certificato, il cui rilascio è articolato e subordinato a numerosi controlli anche di natura legale sull'entità che lo richiede, fornisce le maggiori garanzie sul reale titolare del sito web. Per evitare il phishing, il controllo non dovrebbe essere sull'utilizzo del protocollo HTTPS, ma sul tipo di validazione del certificato usato, limitando la connessione solo a siti che usano certificati di tipo Organization Validated (OV) o Extended Validation (EV). Una differenza di non facile comprensione per l'utenza media di Internet. Tutti i browser forniscono un'indicazione visiva sul tipo di validazione del certificato, purtroppo però non sempre di facile interpretazione, ed è su questo che gli utenti dei servizi di banking andrebbero informati e istruiti con indicazioni chiare. Nel dubbio, non considerare un dominio HTTPS più attendibile di uno HTTP.

Altre caratteristiche delle pagine di phishing

Le pagine di furto di credenziali vengono attivate prevalentemente verso la fine della settimana lavorativa, dal giovedì al sabato (**Figura 2**), pronte per attacchi che si sviluppano durante il week-end, quando la vittima è più vulnerabile con gli sportelli bancari chiusi e gli help-desk a orario ridotto, a cui è più difficile rivolgersi tempestivamente.

La maggior parte delle pagine è rimasta attiva per meno di 48 ore.

Questa media soffre di una grande varianza. Ci sono pagine rimaste attive solo qualche ora, e altre pagine rimaste perfettamente attive e che hanno continuato a "pescare" preziose credenziali per oltre un mese.

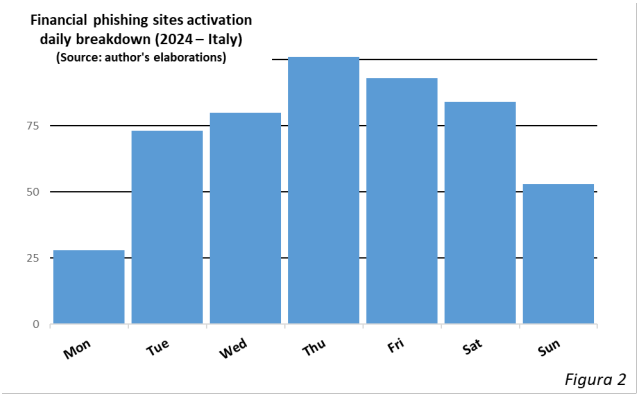


Figura 2

Molti phishing kit espongono in chiaro, tramite URL accessibili a chi ne conosce il path esatto (Direct Object Reference), i dati delle vittime della campagna di phishing (Sensitive Data Exposure). Questa situazione piuttosto frequente è al limite tra un errore di chi ha scritto il phishing kit e la scelta deliberata dei *threat actor* per attingere ai dati "pescati" senza la necessità di alcuna forma di login al sito di phishing, rendendo più difficile il tracciamento e un'eventuale analisi forense. Il fenomeno è di particolare gravità e pericolo per la vittima, in quanto i suoi dati rimangono visibili e potrebbero cadere in mano, non solo degli attaccanti (cosa di per sé già estremamente pericolosa), ma anche di altri threat actors "parassiti" che possono semplicemente seguire gli attacchi senza orchestrarli, catturando le credenziali di accesso per poi costruirci nuove campagne di attacco, oppure ancora provare a rivenderli nel dark web anche all'interno di combo list.

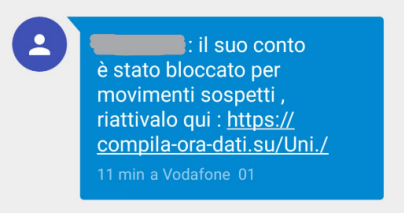
Frequente il fenomeno delle *phishing factory*, vere e proprie fabbriche di phishing con i cyber criminali che registrano e attivano una grande quantità di domini di phishing anche verso target diversi, nel giro di poche ore.

Il phishing verso il settore finanziario italiano ha come tecniche di accesso iniziale prevalentemente e-mail e SMS, ma con una veloce crescita in termini percentuali della Posta Elettronica Certificata (PEC) [33]. In generale il phishing finanziario mira al furto delle credenziali di accesso, come il codice cliente in tutte le sue denominazioni, la password o PIN, e la OTP di accesso e tutti i suoi equivalenti, ma anche altre informazioni utili a rendere più facile un accesso fraudolento, come numero di telefono dell'utente, il codice fiscale e l'indirizzo e-mail. Ogni informazione, anche quella apparentemente meno sensibile, può essere utile quando combinata con altre. La frode è normalmente realizzata attraverso una sequenza di passi successivi,

non necessariamente tutti nella stessa sessione, in ciascuno dei quali vengono rubate solo alcune credenziali, o altre informazioni, per poi ricomporre tutto assieme per perpetrare l'accesso fraudolento.

2023-02-04	0 / 87	VirusTotal	www.accessogruppobperweb.com
2023-02-04	18 / 88	VirusTotal	accessogruppobperweb.com
2023-02-03	16 / 88	VirusTotal	credenzialiappincomplete.com
2023-02-03	16 / 88	VirusTotal	www.credenzialiappincomplete.com
2023-02-03	0 / 87	VirusTotal	www.revocacredenzialiapp.com
2023-02-03	12 / 88	VirusTotal	revocacredenzialiapp.com
2023-02-03	0 / 87	VirusTotal	www.accessoportalebancabper.com
2023-02-03	16 / 88	VirusTotal	accessoportalebancabper.com
2023-02-03	0 / 87	VirusTotal	www.revocatransazioni.com
2023-02-03	17 / 88	VirusTotal	revocatransazioni.com
2023-02-03	0 / 87	VirusTotal	www.ripristinacredenzialiweb.com
2023-02-03	16 / 88	VirusTotal	ripristinacredenzialiweb.com
2023-02-03	0 / 87	VirusTotal	linguainternazionale.it
2023-02-03	0 / 87	VirusTotal	www.linguainternazionale.it
2023-02-03	0 / 87	VirusTotal	www.completaverificadati.com
2023-02-03	0 / 88	VirusTotal	completaverificadati.com

Già dal 2020 abbiamo osservato campagne che usano falsi operatori bancari e chat live di assistenza. I falsi operatori bancari richiamano il numero di telefono che spesso viene chiesto nella pagina di phishing, presentandosi come addetti della banca che hanno notato movimenti sospetti o che richiedono urgenti aggiornamenti dell'App bancaria. In alcuni casi si sono anche presentati come addetti delle forze di polizia che avevano intercettato un accesso fraudolento al nostro conto.

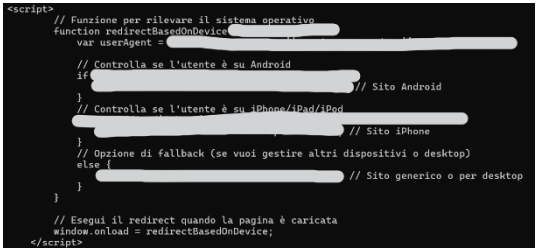


Nel corso del 2024 molte campagne sono iniziate con un SMS che segnala un'operazione anomala sul conto o sulla carta di credito e indica di chiamare un call center (fraudolento) per disconoscere la somma. Dipendentemente da quanto la vittima ha già eventualmente inserito nella prima fase del phishing, i finti operatori chiedono tutti gli altri elementi di autenticazione, oppure solo quelli mancanti. Questa tecnica di interlocuzione telefonica è usata per convincere la vittima a fornire i codici one-time di autenticazione forte del cliente (Strong Customer Authentication) che sotto diverse denominazioni ciascuna banca invia o chiede all'utente di generare in virtù della PSD2.

Si può ipotizzare che, mentre è al telefono con noi, il finto addetto faccia login sul sito vero della banca e per questo ha bisogno dei codici one-time che proprio in quel mo-

mento la banca invia al nostro cellulare o alla App installata sul nostro smartphone, e che lui non può avere senza il nostro aiuto. Oltretutto i codici hanno una validità limitata nel tempo, quindi devono essere usati necessariamente entro qualche minuto.

C'è da notare che molti sistemi VOIP consentono la configurazione del numero chiamante in uscita. Non c'è da sorprendersi se alcune delle chiamate dai finti operatori arrivano da un numero di telefono che è proprio quello della banca. Questa tecnica è chiamata frode "alias" [25]. Approccio simile si ha nelle finestre di chat live che sono presenti su alcune pagine di furto di credenziali. In questo caso, l'operatore via chat ha lo stesso ruolo dell'operatore telefonico nel caso descritto precedentemente e mira a carpire gli elementi di autenticazione ancora mancanti e l'elemento di autenticazione forte, necessario per alcune operazioni dispositive, e a più alto rischio.
Vista la semplicità realizzativa e il basso livello di rischio di chi la perpetra, si prevede una crescita di questa tecnica.



Analizzando i phishing kit usati nelle campagne italiane, si può concludere che il phishing finanziario italiano sia per lo più controllato da operatori italiani. Le campagne hanno una perfetta localizzazione in lingua italiana, il codice presenta commenti in italiano, nelle chat live e ancora di più nelle conversazioni con i finti operatori telefonici si capisce che la controparte è italiana, anzi spesso se ne individuano forti inflessioni dialettali.

Il phishing finanziario italiano è quindi un fenomeno nazionale e operato da attori cyber criminali italiani. Le uniche appendici estere sono relative al transito delle somme su conti esteri e money mule stranieri [26] per renderne più difficile il tracciamento e il recupero.

L'era del low cost phishing

Una frazione molto rilevante del 53% di campagne di phishing finanziario è stata ospitata direttamente sulla piattaforma cPanel, diffusissimo pannello di controllo per la gestione e l'amministrazione di siti internet e web hosting. Il fenomeno è stato predominante nelle campagne di inizio anno, per poi decrescere durante l'anno. Queste pagine, per la loro breve durata (a volte solo qualche ora), sono raramente catturate dai sistemi automatici di analisi.

Le campagne su cPanel, cresciute in maniera importante nel 2023, hanno colpito due terzi delle istituzioni finanziarie analizzate in questa analisi, rappresentando un fenomeno generalizzato.

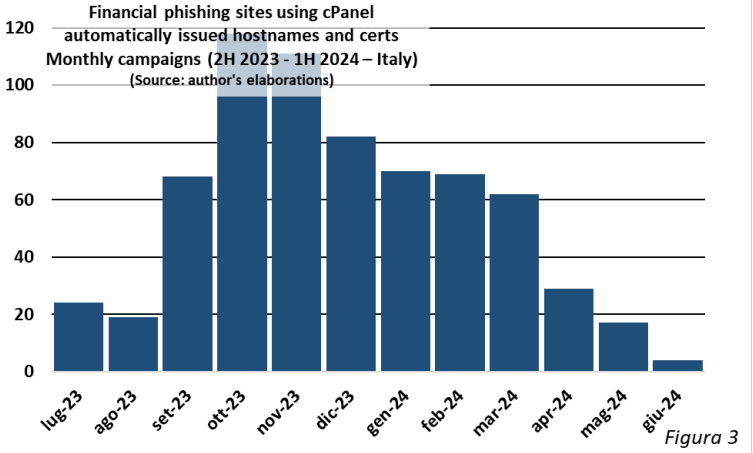


Figura 3

Questo modo di operare ha indubbiamente velocizzato, reso più economica e meno rischiosa la creazione di siti di phishing. Una congiuntura troppo ghiotta per essere ignorata dagli attaccanti. Al momento dell'installazione, se l'interfaccia WebHost Manager (WHM) di cPanel non dispone di un hostname, le viene automaticamente assegnato un hostname all'interno del dominio cprapid.com generato sulla base dell'IP. Inoltre, la Certification Authority di cPanel genera un certificato SSL/TLS per il server web e questo consente connessioni HTTPS senza generare messaggi di errore nei browser client.

Questo meccanismo consente in maniera estremamente semplice ed economica di attivare in autonomia siti web di phishing senza poggiarsi su provider Internet, il che semplifica e rende meno rischiosa l'attività dei cyber criminali.

Financial malware

L'Europa ha registrato la più alta percentuale di incidenti (32%) tra le regioni geografiche, con un incremento anno su anno del 31%. Il malware è stata l'azione più osservata in termini oggettivi rappresentando il 44% degli incidenti [1].

Notevole la crescita anno su anno, del 266%, nell'uso di InfoStealer generici. Gruppi che in precedenza si erano specializzati in ransomware mostrano ora un crescente interesse per gli InfoStealer [1].

In questa sede ci occupiamo solo del sottoinsieme di tutti i malware usati nelle frodi finanziarie. L'obiettivo finale di questi malware è portare a termine un furto o frode finanziaria (T1657), ad esempio catturare credenziali, effettuare un bonifico dal conto della vittima, oppure una transazione fraudolenta con una carta di credito, e questo può accadere in diversi modi. Un attacco prevede molte fasi e per questo è necessario combinare più TTP (Tecnica, Tattica, Procedura). Esiste almeno una tattica di Initial Access (accesso iniziale) per guadagnare l'accesso al sistema o all'account della vittima, e poi altre tattiche e tecniche per finalizzare la frode ed eventualmente occultarne le tracce. Dopo aver effettuato la frode c'è poi la fase di monetizzazione della somma, cioè convertire una transazione elettronica in denaro senza lasciare tracce che consentono l'identificazione del frodatore.

Con l'aumentata efficacia dei sistemi antifrode, e l'intelligenza artificiale per individuare le transazioni sospette, i frodatori si muovono verso la manipolazione della vittima per indurla a effettuare l'operazione allo sportello, dove l'operazione in presenza è soggetta a meno controlli rispetto alle operazioni online da remoto.

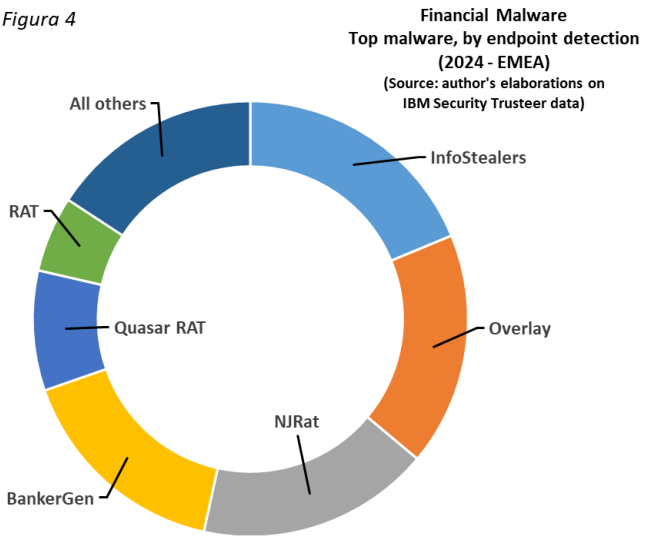
Attività dei principali financial malware nel corso dell'anno

Uno dei fenomeni più significativi dell'anno è la sostituzione di malware specializzati, con InfoStealer, remote overlay generici e Remote Access Tool (RAT) [1]. Si tratta di malware semplici, molto usati in passato, che ora godono di nuova vita per la loro versatilità.
Nelle osservazioni di IBM Security Trusteer nell'area geografica EMEA (Europa, Medio Oriente e Africa) sull'intero anno 2024, queste tre tipologie di malware assommano a oltre il 53% di tutto il malware usato nelle frodi finanziare (T1657).

Il diagramma in **Figura 4** descrive la distribuzione dei malware così come sono stati rilevati sui dispositivi utente (endpoint) infetti, e misura anche la capacità del malware di infettare il computer o smartphone della vittima, malgrado la presenza dei sistemi di protezione.

Dopo alcuni anni in cui avevamo osservato sempre gli stessi malware contendersi il mercato, già dal 2023 abbiamo notato che i threat actors hanno preferito usare software malevoli generici, come gli InfoStealers o i Remote Access Tools, in alcuni casi disponibili sul dark web, piuttosto che malware specializzati per frodi finanziarie. Con la crescita degli InfoStealer generici, gruppi che in precedenza si erano specializzati in ransomware mostrano un crescente interesse per gli InfoStealer [1]. Alcuni nuovi InfoStealer di spicco hanno recentemente debuttato e dimostrato subito un'importante attività, come Rhadamanthys, LummaC2 e Strela Stealer.

Figura 4



Attorno a Rhadamanthys (InfoStealer) sono state costruite molte campagne in Italia nel corso del 2024, in particolare negli ultimi mesi, e si ipotizza che questo malware continuerà la sua attività anche nel corso del 2025.

A novembre 2024 IBM X-Force ha monitorato le campagne che distribuivano Strela Stealer a vittime in tutta Europa, principalmente Italia, Spagna, Germania and Ucraina [27]. Le e-mail di phishing utilizzate in queste campagne sono vere notifiche di fatture, rubate tramite credenziali e-mail precedentemente esfiltrate. Strela Stealer è progettato per estrarre le credenziali utente archiviate in Microsoft Outlook e Mozilla Thunderbird, aprendo la strada ad attacchi Business E-mail Compromise (BEC) e perpetuare così la propria diffusione.
Anche per CERT-AGID i malware più diffusi in Italia nel 2024 sono stati degli InfoStealer e Remote Access Tools (AgentTesla, FormBook, Remcos) [10].
Gozi/Ursnif, un malware per sistemi Windows, è stato usato in alcune campagne verso istituzioni bancarie italiane. Nelle campagne è stato configurato per operare uno "swap account" con una sostituzione dell'IBAN nella fase di esecuzione di un bonifico, e dirottare così le somme verso conti sotto il controllo dei cyber criminali.

Questo cambiamento segna una svolta importante in quanto abbassa il livello di competenza necessario a costruire un attacco. Il ricco mercato del cybercrime si apre a nuovi threat actors senza la necessità di grosse competenze di programmazione e

conoscenza dei sistemi operativi. Piuttosto i gruppi cyber criminali si stanno specializzando nel sovvertire psicologicamente la vittima e trarre vantaggio delle debolezze dei processi di autenticazione e autorizzazione della transazione.
È ragionevole ipotizzare che questi cambiamenti aprano spazio all'ingresso di un numero sempre maggiore di cyber criminali con un conseguente aumento complessivo degli attacchi.

Lo smishing, SMS contenenti phishing che arrivano sul telefono e invitano a visitare un link o installare una app o aggiornamento di app, è stato uno dei metodi più usati per infettare i dispositivi mobili. L'SMS, ormai poco usato nelle comunicazioni interpersonali, continua invece a essere molto usato nelle frodi in quanto mima alcune comunicazioni bancarie ancora veicolate via SMS. Fornisce una percezione di maggiore affidabilità agli occhi della vittima.
SpyNote, malware Android molto diffuso in Italia nel corso del 2023 e del 2024 [10], [11] ha tra le funzionalità standard proprio quella di intercettare SMS, ancora usati come fattore di autenticazione per operazioni bancarie. SpyNote si è diffuso con false campagne che inducevano a installare App per IT-Alert sull'ondata del lancio di questo servizio in tutta Italia [12].
Su Android si è abusato molto dei servizi di accessibilità, progettati per rendere più semplice l'utilizzo del telefono da parte di utenti con visibilità o manualità ridotta e che per questo forniscono un insieme di accessi e di interazioni addizionali, sfruttati in maniera malevola dai creatori di malware.

Finora scrivere malware per dispositivi iOS ha richiesto uno sforzo, competenze e costi più elevati rispetto ai dispositivi Android. Inoltre, i dispositivi iOS sono stati anche protetti dal fatto che le applicazioni da installare potevano provenire soltanto dallo store ufficiale Apple. Quest'ultimo meccanismo è venuto meno nel corso del 2024, per gli utenti nell'Unione Europea, da quando Apple ha dovuto consentire il sideloading [13], installazione di App anche da store non ufficiali, su pressione dell'Unione Europea attraverso la Digital Markets Act. Le app disponibili sugli store alternativi sono sottoposte a controllo (Notarization) da parte di Apple, con una combinazione di controlli per garantire che le app siano prive di malware, virus o altre minacce note, funzionino come promesso e non espongano gli utenti a frodi. Questo processo è tuttavia diverso da quello a cui sono soggette le app scaricate dall'App Store ufficiale. Le ricadute in termini CyberSecurity di questo cambiamento saranno meglio misurabili nei prossimi mesi.

La crescita degli attacchi Living off the Land/Living Off Trusted Sites

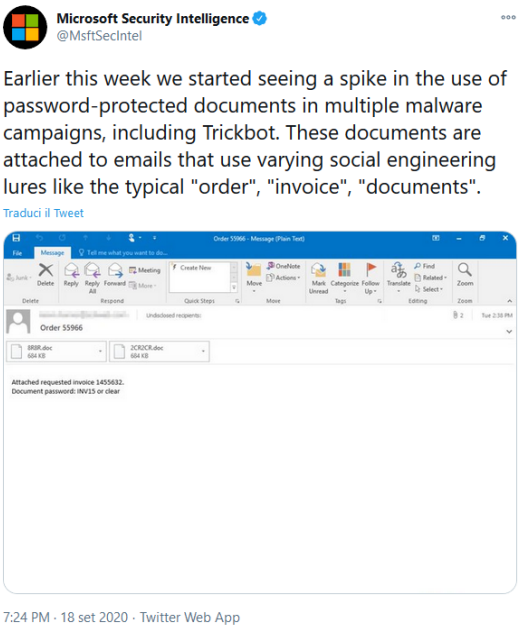
L'espressione *living off the land* significa, in lingua inglese, vivere dei prodotti della propria terra. Similmente, gli attacchi *Living Off The Land* (LOTL) si basano su strumenti nativi preinstallati nel sistema operativo, come ad esempio la PowerShell o la Windows Management Instrumentation (WMI) per i sistemi Windows. Quindi attacchi sono autosufficienti nel senso che trovano sul sistema da attaccare già tutti gli strumenti di cui necessitano.
Gli attaccanti hanno anche ulteriormente esteso l'uso di Telegram e altri servizi cloud, come infrastruttura di Comando e Controllo (C2) ed esfiltrazione di dati [14]. Queste scelte, oltre che rendere più difficile l'individuazione e il filtraggio delle comunicazioni tra agent e server, abbattono drasticamente i tempi di sviluppo e i costi dell'infrastruttura necessaria a controllare tutte le comunicazioni con gli agent malevoli. L'espressione Living Off Trusted Sites (LOTS) [2] racchiude tutte queste tecniche.

Oltre 30 campagne di phishing nel corso del 2024 hanno sfruttato i servizi Cloudflare. L'ottima reputazione di questa azienda è evidentemente sfruttata per aumentare l'impressione di legittimità della pagina fraudolenta. Decisione questa abbastanza controversa da parte dei cyber criminali in quanto i servizi di segnalazione abusi di Cloudflare sono molto efficaci, e quindi non appena individuata la non legittimità della pagina risulta facile e veloce segnalarla per una pronta disattivazione.
Il successo di queste tecniche a supporto degli attacchi è dovuto al fatto che richiedono un investimento davvero minimo e sono più difficilmente individuabili dagli strumenti di protezione dell'Endpoint tradizionali, che basano il loro funzionamento sulla ricerca di malware o script conosciute. Questi attacchi, quindi, tendono a essere più efficaci, permettendo all'attaccante di prolungare la durata dell'attacco a lungo prima di essere individuato. Enisa ha inserito le tecniche Living Off The Land (LOTL) e Living Off Trusted Sites (LOTS) nei Key Trends 2024 [2].

Con la crescita delle tecniche LOLT/LOTS assistiamo a una trasformazione nel panorama del codice malware. Sicuramente c'è da aspettarsi una sempre minore presenza dei dropper (Emotet il più famoso), sostituiti da script/macro all'interno di documenti Office, PDF o e-mail.

Il ruolo delle macro all'interno di documenti Office

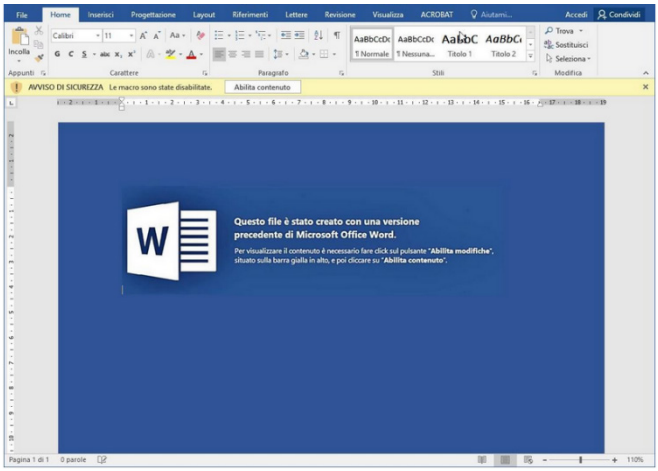
Nel corso dell'anno i malware sono stati veicolati nella maggioranza dei casi attraverso file compressi contenenti documenti Office, allegati a e-mail e protetti da password.



Nel caso dei documenti Office, una volta aperti, l'utente viene invitato ad abilitare l'esecuzione di macro, o altri contenuti attivi. Questa operazione apparentemente innocua fornisce al documento i privilegi necessari per scaricare il resto del malware da una *drop URL* sfruttando prevalentemente strumenti nativi del sistema operativo, come la Powershell di Windows e il protocollo HTTP/HTTPS, tipicamente non filtrato.

Nel corso del 2019 avevamo osservato molti documenti malevoli sfruttare la CVE-2017-0199 e la CVE-2017-11882, due Remote Execution Vulnerability per Windows molto insidiose. Era sufficiente aprire il documento, e in talune circostanze fare la sola preview, per eseguire la componente malevola che scaricava il codice malware. Il meccanismo, su macchine non aggiornate, era particolarmente potente in quanto richiedeva un'interazione minima da parte della vittima.

Dal 2020 in poi gli attaccanti si sono mossi invece su un terreno decisamente più facile, sfruttando prevalentemente la debolezza umana con documenti Office contenenti macro malevole.



La differenziazione tra una campagna e l'altra sta principalmente nel messaggio (pretext) usato per invitare la vittima ad aprire il documento e abilitare l'esecuzione delle macro, anche se l'obiettivo finale rimane lo stesso. Gli inviti più frequenti sono di abilitare le macro in quanto necessario per un aggiornamento di Word, oppure perché il documento è protetto, oppure molto più frequentemente in quanto il documento è creato con una versione più recente di Word. Tutte motivazioni false, il cui unico obiettivo è di far eseguire la macro nascosta e non visibile all'interno del documento, che scarica e infine attiva il malware. Dopo l'attivazione, il malware comunica con la sua infrastruttura di controllo e con il gruppo cyber criminale attraverso una rete di nodi di Command-and-Control (C2C o C2), dai quali riceve ulteriori elementi di configurazione, watchlist, comandi remoti da eseguire sul sistema infetto, o attraverso i quali esfiltra i dati della macchina infetta, come username, password o URL visitate.

Microsoft ha operato, con diversi roll-out tra il 2022 e il 2023, un importante cambiamento nell'apertura di macro in documenti Office provenienti da Internet [15]. Con questa modifica, quando gli utenti aprono un file Office proveniente da Internet o da una porzione della Intranet considerata come non affidabile per le policy del computer o dominio, viene visualizzato un messaggio che spiega che le macro sono state bloccare per sicurezza. Il pulsante "Ulteriori informazioni" porta l'utente a un articolo con informazioni sui rischi legati all'attivazione delle macro, pratiche sicure per prevenire phishing e malware, e infine istruzioni su come abilitare le macro se assolutamente necessarie. Il messaggio era presente anche prima, ora è stato ulteriormente chiarito.

L'artificio di inserire un file compresso, ad esempio .zip, protetto da password ma con una password molto semplice e inclusa in chiaro nel testo della mail, serve a evadere i meccanismi antivirus sulla e-mail e il sandboxing degli allegati. In questo modo la vittima è in grado di aprire il file compresso e poi il documento malevolo contenuto all'interno e "detonarlo" (termine che indica l'esecuzione di un file potenzialmente malevolo) direttamente sul sistema endpoint. La catena degli incapsulamenti, con un file compresso e protetto da password ma con la password disponibile, serve esclusivamente a eludere alcuni sistemi di scansione e analisi automatica della e-mail che non riescono a espandere o eseguire archivi protetti da password.

Caselle PEC sempre più usate

Alcune campagne fraudolente, specie nella seconda parte dell'anno, hanno sfruttato messaggi di Posta Elettronica Certificata (PEC), sia per campagne di phishing [28] [33] che per la diffusione di malware e in particolare in Italia il malware Vidar [16] [17], un InfoStealer per Windows che cattura ed esfiltra dati sensibili dal browser.

Nella maggior parte dei casi si è trattato di caselle PEC compromesse in precedenti campagne.

L'uso della PEC ha lo scopo di attribuire maggiore autorevolezza al messaggio e indurre la vittima a cadere più facilmente nell'inganno.

Furto di credenziali e resistenza al phishing

Il semplice furto delle credenziali di accesso, intese come nome utente e password, da solo non basta a portare a termine una frode finanziaria. La direttiva europea PSD2 [18] ha introdotto dal 2019 l'utilizzo di un ulteriore fattore di autenticazione forte del cliente (SCA – Strong Customer Authentication), spesso nella forma di una OTP (One Time Password – Password valida solo 1 volta) inviata via SMS o generati da una App, da reinserire in un form per verificare l'utente e completare l'autenticazione. Questi meccanismi sono noti più in generale come MFA – Multi-Factor Authentication, o autenticazione a più fattori [19]. La cattiva notizia è che ben presto la Multi-Factor Authentication è diventata a sua volta vittima di phishing o social engineering.

All'atto pratico, lo strumento messo a punto per scongiurare il furto delle credenziali, si è dimostrato vulnerabile allo stesso tipo di attacco. Anzi, molte frodi che hanno successo, sono riuscite a raggirare la protezione introdotta dalla Multi-Factor Authentication. Laddove la credenziale aggiuntiva preveda qualcosa (PIN, codice monouso) da reinserire in un form-online, quel tipo di meccanismo, a priori, *non è resistente al phishing*. Per quanto articolato o dipendente dal tempo, i cyber criminali possono sempre creare form verosimili o coinvolgere finti operatori telefonici o chat online per indurre la vittima a fornire i fattori di autenticazione.

One-time password (OTP), SMS, notifiche push con un numero o codice da reinserire in un form, alcuni usi delle App di autenticazione, sono tutti sistemi vulnerabili al phishing.

Sempre più spesso si stanno diffondendo sistemi *Phishing-Resistant Multi-Factor Authentication*, intesi come meccanismi di autenticazione progettati per rilevare e impedire la divulgazione di credenziali di autenticazione verso un'applicazione o sito web mascherato da sistema legittimo.
In una minaccia phishing così pervasiva, tutti i sistemi ad alto valore di un'organizzazione dovrebbero implementare o pianificare quanto prima la loro migrazione a meccanismi MFA resistenti al phishing.

Al momento i due sistemi più efficaci sono quelli basati su autenticazione FIDO/WebAuthn (conosciuta anche come standard FIDO2) [20], oppure basati su Public key infrastructure (PKI), anche attraverso le più recenti implementazioni delle App di autenticazione.

La FIDO Alliance ha originariamente sviluppato il protocollo WebAuthn come parte degli standard pubblicati FIDO2. Il supporto WebAuthn è già incluso nei principali browser, sistemi operativi e smartphone. Gli autenticatori WebAuthn sono tipicamente dei piccoli token fisici di basso costo chiamati autenticatori "roaming" da collegare al computer o smartphone tramite USB o NFC.

Cosa si può prevedere per il 2025

Le osservazioni degli ultimi mesi descrivono un contesto in costante evoluzione e un contemporaneo abbassamento della soglia di difficoltà nel realizzare gli attacchi. La disponibilità di malware sui marketplace nel dark web, a volte anche gratuiti, le credenziali in vendita, i dump di dati e l'utilizzo dell'intelligenza artificiale generativa non possono che incrementare il numero e la complessità degli attacchi.
La soluzione è in realtà più vicina di quanto si pensi. In molti attacchi analizzati sarebbe bastato applicare alcune best practice consolidate, come il rafforzamento delle

credenziali, il principio del privilegio minimo, e attivare autenticazione a più fattori resistente al phishing per limitare l'impatto di alcuni vettori di accesso usati negli attacchi.
È fondamentale accelerare il percorso di sostituzione delle soluzioni di autenticazione a più fattori non resistenti al phishing, come le One-Time Password (OTP) via SMS. Per quanto supportato anche dai cellulari di più vecchia generazione, il rischio che le OTP vengano catturate e riutilizzare in maniera fraudolenta è davvero alto.
Bisogna essere pronti a nuove forme di phishing, come l'aumento di inserzioni malevole sui social network, con annunci che usando il marchio e l'identità visiva di note aziende bancarie, inducono a investire somme di denaro su piattaforme false. Attenzione anche ai nuovi canali, come ad esempio phishing e malware veicolati attraverso messaggi di PEC.

Il phishing continua la sua evoluzione anche attraverso tattiche più articolate, come codice offuscato, filtri contro l'analisi, pagine phishing attivate e disattivate on-demand in tempi brevi per impedire l'analisi e il blocco. Nel corso del 2024 si è assistito a un numero minore di pagine, ma con codice di complessità maggiore. Questo presumibilmente continuerà nel corso 2025.
Un business così profittevole favorisce la proliferazione di piattaforme di Phishing-as-a-Service [21] e Malware-as-a-Service. Con queste piattaforme, pubblicizzate su canali Telegram e altri social, il cybercrime diventa facilmente accessibile a una platea più ampia.

Indubbio sarà il ruolo della education, sia quella generalista, che quella indirizzata a determinate categorie di utenza, come ad esempio gli utenti di un particolare servizio o ai dipendenti d'azienda. Per la protezione dei dati aziendali questo è quantomai attuale. Il Cost of a Data Breach Report 2024 [22] mostra ormai da qualche anno come l'*employee training* (formazione del dipendente) sia il fattore che da solo contribuisca maggiormente alla riduzione dei costi nel caso in cui una azienda sia vittima di un data breach. L'offerta in Italia è ricchissima. Il Clusit, con il progetto *SicuraMente Clusit*, è impegnato da oltre 20 anni nelle scuole per diffondere la cultura della sicurezza informatica. Appositamente dedicata all'utenza bancaria è la web serie *I Navigati – Informati e sicuri* del CERTFin che spiega in maniera molto chiara come riconoscere le più comuni truffe bancarie.

La formazione è sicuramente importante per prevenire molte forme di attacco, ma purtroppo da sola non basta. Alcuni attacchi particolarmente insidiosi hanno successo anche laddove l'utente opera con cautela e prevenzione. Servono delle contromisure di natura tecnica, che intervengano laddove la minaccia riesca a scavalcare le protezioni della vittima.

Sul mercato si osserva una virtuosa convergenza di soluzioni verso l'adozione di feed di Cyber Threat Intelligence [23]. I feed veicolano, in tempo reale o quasi, descrizioni di minacce e attacchi e questi aggiornano costantemente le soluzioni di sicurezza con nuove definizioni, proprio come abbiamo imparato per gli antivirus. Queste integrazioni, un tempo appannaggio delle soluzioni SIEM e dei dispositivi di rete, sono ora possibili per tante altre soluzioni di sicurezza come la SOAR (Security Orchestration, Automation and Response), le soluzioni di Threat Investigation e quelle di Identity e Access Governance, come ad esempio le innovative soluzioni di Identity Threat Detection and Response (ITDR). Nell'Identity Threat Detection and Response troviamo un connubio virtuoso nel quale strumenti e processi di sicurezza sono orientati a indentificare, bloccare e rispondere agli attacchi incentrati sull'identità. Le soluzioni ITDR attraggono grande interesse dal mercato e si può attendere una crescita legata all'impennata delle minacce a identità e accessi.

La Cyber Threat Intelligence è fondamentale per prevenire le minacce. La sua adozione da parte delle soluzioni IT e delle organizzazioni continuerà senza dubbio a crescere. Più in generale c'è forte interesse, oltre che obblighi normativi, verso il tema dell'InfoSharing o condivisione di informazioni. Esistono molti servizi generalisti open, e crescono le reti di InfoSharing di settore, come ad esempio quella che in Italia si opera nel settore finanziario (CERTFin) o nella Pubblica Amministrazione (CERT-AGID). Per i gestori dei servizi di pagamento, oltre ai più tradizionali Indicators of Compromise (IoC) tipicamente forniti e fruiti dai dipartimenti legati alla Cyber-Security, sono di grande valore gli Indicators of Fraud (IoF) appannaggio dei dipartimenti antifrodi. Ciascuna organizzazione può, al tempo stesso, fruire di indicatori forniti da terzi, e individuare indicatori da condividere con altri.

La PSR - Payment Service Regulation, ancora in iter approvativo, prevede meccanismi di fraud data sharing in base ai quali i fornitori di servizi di pagamento (Payment Service Providers o PSP) possono scambiarsi informazioni su transazioni di pagamento fraudolente, anche mediante l'uso di piattaforme IT dedicate.

L'intelligenza artificiale, in particolare quella di tipo generativo, sta facendo un ingresso prorompente in tutti i settori. Se da una parte questo fornisce nuovi strumenti di difesa oltre a quelli già forniti dal Machine Learning, forte è la preoccupazione per le nuove potenti armi che fornirà agli attaccanti.
Al momento sono pochi i casi in cui un attacco è stato certamente ricondotto all'uso di intelligenza artificiale generativa, e quasi tutti legati a deepfake usati per accreditarsi verso la vittima. Esiste una indubbia difficoltà nell'attribuire un attacco a intelligenza artificiale, e l'impatto della AI nelle campagne malevole rischia di rimanere sottostimato.

Abbiamo già parlato della crescente complessità delle campagne di phishing. Tra gli usi attesi della AI generativa nelle campagne di phishing e malware, c'è la generazione di script PowerShell (o altri strumenti Living off the Land) malevole [2], e l'offuscamento del codice malevolo. Alcuni Large Language Models potranno essere usati per individuare in maniera automatica vulnerabilità di codice, e generare codice per sfruttarle.
I cyber criminali, oltre che usare modelli di AI generativa per la creazione di campagne di attacco, potrebbero decidere di attaccare i dati e i modelli su cui si poggiano i Large Language Models, al momento poco o nulla protetti.
Per le organizzazioni, è imperativo da subito individuare e classificare tutti i modelli usati, i dati e le applicazioni che usano i modelli. Questo ci permetterà di proteggere i dati, e con essi i modelli. È poi importante individuare vulnerabilità ad attacchi ai modelli, e monitorare sia le fasi di training che di utilizzo dei modelli per individuare usi anomali.

In ambito finanziario occorrerà prestare crescente attenzione verso gli attacchi deepfake, in particolare relativi alle fasi di onboarding di nuovi clienti, con il rischio che nelle nuove App bancarie questo avvenga con file vocali, immagini o video generati artificialmente.

Il *cloud computing* e l'*intelligenza artificiale* sono due fenomeni inarrestabili che caratterizzano il panorama informatico di questi anni e continueranno a farlo negli anni a venire. Continua incessante, anche in Italia, lo spostamento di applicazioni, workload e dati verso il cloud. Questo indipendentemente dal settore e dalla dimensione dell'organizzazione. L'annosa diatriba della scelta tra cloud e on-premises che ha caratterizzato il dibattito negli anni passati, ha trovato una naturale soluzione nel cloud ibrido (hybrid cloud) con il quale è possibile integrare i dati e le applicazioni dei propri data center con dati e applicazioni in cloud privati, oppure nei cloud pubblici dei provider di mercato anche in modalità multi-cloud, senza vincolarsi a nessuno di questi (vendor lock-in) e a nessuna scelta architetturale di lungo termine. Il cloud ibrido deve il suo successo all'ampia flessibilità che lascia all'organizzazione, in quanto questa può decidere di far risiedere i dati e le applicazioni dove ritiene più appropriato, o dove è economicamente più conveniente (FinOps), integrando ambienti eterogenei. Una soluzione di sicurezza, qualunque essa sia, deve essere capace di gestire tale livello di complessità, adattandosi alle scelte architetturali dell'organizzazione e gestendo le minacce e i rischi a cui sono costantemente esposte tutte le componenti IT, indipendente da dove queste siano collocate.

Da diversi anni ormai il Cost of a Data Breach Report [22] mostra come intelligenza artificiale e automazione nella individuazione e risposta agli incidenti, sono tra i fattori

che maggiormente contribuiscono all'abbassamento dell'impatto economico di un data breach.

Gli attacchi diventano sempre più veloci, anche a causa dei meccanismi di automazione usati dagli attaccanti. La prevenzione, individuazione e risposta agli attacchi deve pertanto poggiarsi su strumenti che consentano una pari rapidità di azione.

Bibliografia

[1] *X-Force Threat Intelligence Index* 2024 IBM X-Force, February 2024
[2] *ENISA Threat Landscape 2024* European Union Agency for Cybersecurity (ENISA), settembre 2024
[3] *Verizon 2024 Data Breach Investigations Report* Verizon, 2024
[4] *Polizia Postale - Report annuale 2024 - Aggiornamento 21/12/2024*
[5] *PhishStats - Dashboard 1 - New Phishing websites by year* PhishStats (Consultato gennaio 2025)
[6] *Un anno di Phishing. L'evoluzione delle Truffe Online in Italia nel 2024* D3Lab, 19 dicembre 2024
[7] *Flagging 13 Million Malicious Domains in 1 Month with Newly Observed Domains* Akamai Security Research, September 2022
[8] *2024 Report on Payment Fraud* European Central Bank (ECB) and the European Banking Authority (EBA), 1 August 2024
[9] D. Adrian, S. Chen, J. DeBlasio, E. Stark, and E. von Zezschwitz *An Update on the Lock Icon* Chromium Blog, May 2023
[10] *Rapporto di riepilogo – Anno 2024* CERT-AGID, gennaio 2025
[11] Report riepilogativo sull'andamento delle campagne malevole che hanno interessato l'Italia nel 2023 CERT-AGID, gennaio 2024
[12] A. Draghetti *Malware veicolato tramite falso sito di IT-Alert* D3Lab, 16 ottobre 2023
[13] *Installing apps through alternative app distribution in the European Union* Apple, 11 December 2024
[14] *Campagna di phishing PEC: Credenziali inoltrate a un bot Telegram* CERT-AGID, 10/04/2024
[15] *Macros from the internet are blocked by default in Office* Microsoft, December 2023
[16] *Ritorna Vidar in Italia con una campagna di malspam tramite PEC* CERT-AGID, 06 agosto 2024
[17] *Vidar torna a colpire in Italia attraverso PEC compromesse* CERT-AGID, 04 novembre 2024

[18] *Directive (EU) 2015/2366 of the European Parliament and of the Council* Official Journal of the European Union, November 2015
[19] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019 https://securityintelligence.com/multifactor-authentication-delivers-the-convenience-and-security-online-shoppers-demand/
[20] S. Weeden *What makes FIDO and WebAuthn phishing resistant?* IBM Security Community, December 2021
[21] P. Paganini *Phishing-as-a-Service Rockstar 2FA continues to be prevalent* securityaffairs, 29 november 2024
[22] *Cost of a Data Breach Report 2024* IBM and Ponemon Institute, July 2024
[23] Pier Luigi Rotondo *Soluzioni di sicurezza più efficaci con la threat intelligence di IBM X-Force Exchange* IBM Italia Newsroom, dicembre 2023 https://it.newsroom.ibm.com/xforceexchange
[24] *Report CERTFin - SICUREZZA E FRODI INFORMATICHE IN BANCA - Come prevenire e contrastare attacchi informatici e frodi sui canali digitali* CERTFin, maggio 2024
[25] *Contrasto alla criminalità finanziaria - Attività della Polizia Postale contro le frodi "Alias"* Commissariato di P.S. online, novembre 2020
[26] S. Foffo *Operazione "Emma 9" contro i muli del cybercrime* Polizia di Stato, dicembre 2023
[27] G. Mühr, J. Fasulo, C. Hammond *Strela Stealer: Today's invoice is tomorrow's phish* SecurityIntelligence.com, 12 November 2024
[28] *Caselle PEC sempre più usate nel phishing per le frodi bancarie* CERT-AGID, 25 novembre 2024
[29] Webinar IoC e Hashr - Rafforzare la sicurezza informatica delle PA CERT-AGID, 18 dicembre 2024
[30] *Rilevata campagna malware SpyNote mascherata come app INPS Mobile* CERT-AGID, 09 aprile 2024
[31] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019 https://securityintelligence.com/posts/how-will-strong-customer-authentication-impact-the-security-of-electronic-payments/
[32] G. Badalucco *Identity security, la sicurezza basata sull'identità* Data Manager, settembre 2022
[33] P. Paganini *Anche le PEC possono essere vettori di attacco* Repubblica, 14 ottobre 2024

Proteggere il data center ibrido nell'era dell'intelligenza artificiale

(A cura di Andrea Verri e Luciano Pomelli, Cisco)

L'intelligenza artificiale (IA) sta trasformando la sicurezza dei data center ibridi, richiedendo soluzioni più scalabili e automatizzate per proteggere le infrastrutture moderne. L'articolo esplora come l'IA e tecnologie come eBPF migliorino la sicurezza dei cluster Kubernetes, offrendo protezione avanzata contro le minacce in tempo reale. Cisco crede che lo sviluppo di sistemi evoluti basata su IA per automatizzare la gestione della sicurezza nei cloud ibridi, possano aumentare la resilienza e la protezione delle applicazioni. Il futuro della cybersecurity è sempre più orientato a modelli AI-driven per ecosistemi più sicuri e dinamici.

Oggi tutti parlano di intelligenza artificiale (IA) non solo per il suo fascino tecnologico, ma per il suo impatto trasformativo e i notevoli guadagni in termini di produttività. Il motore di questa rivoluzione, il data center, è destinato a crescere in modo esponenziale nei prossimi anni.

Il cambiamento del settore IT

In passato, aziende come Amazon, Google e Microsoft hanno affrontato una crescita tale da rendere obsoleti i tradizionali sistemi di data center aziendali. Per rispondere a questa sfida, hanno sviluppato software infrastrutturale e adottato un modello di scalabilità orizzontale, dando vita al cloud pubblico. Oggi, tutte le aziende devono pensare a come adattarsi a un "data center su scala IA" e le tradizionali appliance di sicurezza non saranno sufficienti.

La preparazione delle Aziende all'IA e alla Cybersecurity

Secondo l' "AI Readiness Index 2024[1]" , il report di Cisco che valuta la preparazione delle aziende per l'integrazione dell'IA attraverso sei pilastri: Strategia, Infrastruttura, Dati, Governance, Talento e Cultura, molte organizzazioni stanno investendo nell'IA, ma non si sentono ancora pronte ad adottarla pienamente. Sebbene gli investimenti in IA e sicurezza informatica siano in crescita, i leader aziendali ritengono di non aver ancora raggiunto i livelli desiderati di preparazione.

Nonostante gli investimenti continui, l'indice mostra un declino nella prontezza all'IA a livello globale, con infrastruttura e sicurezza informatica che emergono come preoccupazioni critiche. In particolare il report evidenzia le seguenti problematiche:

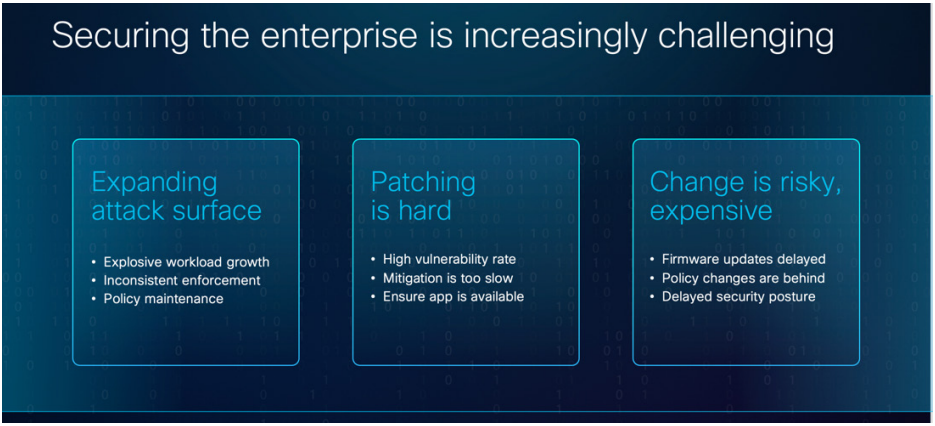
- **sfide dell'Infrastruttura:** la prontezza dell'infrastruttura per supportare le iniziative di IA è diminuita, con solo il 46% delle aziende che si sente almeno moderatamente preparato. Questa inadeguatezza è evidente in aree come potenza di calcolo, prestazioni di rete e scalabilità, componenti essenziali per un'efficace implementazione dell'IA;
- **aumento dei Carichi di Lavoro dell'Infrastruttura:** una cifra sorprendente del 93% delle organizzazioni prevede un aumento dei carichi di lavoro dell'infrastruttura con il dispiegamento dell'IA. Tuttavia, i sistemi esistenti spesso non riescono a gestire queste richieste, sottolineando la necessità di un'infrastruttura robusta e scalabile;
- **rischi di Sicurezza Informatica in intensificazione:** con l'integrazione delle tecnologie IA, la sicurezza informatica è diventata una preoccupazione fondamentale. Molte organizzazioni (67%) segnalano una comprensione limitata delle minacce specifiche per l'IA e l'apprendimento automatico. Questa mancanza di consapevolezza può portare a vulnerabilità, poiché i sistemi IA sono sempre più presi di mira da minacce informatiche sofisticate;
- **controllo degli Accessi e Sicurezza dei Dati:** la gestione del controllo degli accessi ai sistemi e ai dataset IA è un'altra area in cui le organizzazioni stanno lottando. Quasi il 72% degli intervistati indica che l'attuale posizione nella gestione del controllo degli accessi è insufficiente, rispetto al 68% dell'anno scorso. Questo divario evidenzia la necessità di misure di sicurezza potenziate per proteggere i processi e i dati sensibili dell'IA.

In parallelo, il Cisco Cybersecurity Readiness Index 20242 conferma che la maggior parte delle organizzazioni non è adeguatamente preparata per difendersi da queste minacce in evoluzione, nonostante gli sforzi per rafforzare la sicurezza delle reti e del cloud.

- L'importanza della resilienza della rete è sottolineata dalla necessità di strategie di protezione flessibili negli ambienti di lavoro ibridi. La microsegmentazione è una tattica chiave, che consente alle organizzazioni di isolare segmenti di rete e limitare la diffusione delle minacce bloccando il movimento laterale non autorizzato.
- Il rafforzamento del cloud è altrettanto critico poiché le operazioni si spostano verso infrastrutture gestite da terzi. I firewall "host-based" forniscono un livello di difesa cruciale proteggendo carichi di lavoro virtuali ed eterogenei da accessi non autorizzati.

- Il patching dinamico delle vulnerabilità è un'altra misura essenziale, che consente alle organizzazioni di affrontare rapidamente le vulnerabilità del software e proteggere le applicazioni cloud. L'applicazione delle patch con i metodi e i processi attuali richiede oggi troppo tempo e numerose e accurate verifiche per garantire la funzionalita' dei carichi di lavoro sui quali vengono installate.

Riconoscendo le crescenti minacce, le organizzazioni stanno rispondendo pianificando significativi aggiornamenti delle infrastrutture IT, con oltre la metà (52%) intenzionata a migliorare i propri sistemi nei prossimi 12-24 mesi. Molte mirano ad aggiornare le soluzioni esistenti (66%), implementarne di nuove (57%) e investire in tecnologie guidate dall'intelligenza artificiale (55%) per migliorare l'identificazione, l'analisi e il rilevamento delle minacce e ridurre la superficie di attacco sfruttando l'automazione ("machine scale").



Kubernetes: il cuore dell'infrastruttura IT moderna

Nel frenetico panorama digitale odierno, la capacità di sviluppare, distribuire e scalare applicazioni senza problemi è diventata una pietra miliare dell'innovazione.

Kubernetes, solida piattaforma di orchestrazione dei containers, è emersa come lo standard de facto per la gestione delle moderne architetture applicative. La sua flessibilità e scalabilità consentono alle organizzazioni di creare applicazioni resilienti e native per il cloud (pubblico e privato) in grado di soddisfare le esigenze di un mercato in rapida evoluzione. Kubernetes offre anche la possibilità di eseguire carichi di lavoro di macchine virtuali (VM) legacy accanto ad applicazioni containerizzate, permettendo alle aziende di modernizzare la propria infrastruttura senza interruzioni.

Inoltre, Kubernetes si propone sempre più come piattaforma ideale per applicazioni che sfruttano l'intelligenza artificiale, fornendo un ambiente scalabile e dinamico per il deployment di modelli di IA e carichi di lavoro complessi.

Kubernetes e la Sicurezza Informatica

Nonostante i numerosi vantaggi, un'architettura iper-distribuita come Kubernetes presenta complesse sfide di sicurezza. La dinamicità degli ambienti Kubernetes, sia su cloud pubblico che privato, richiede un livello di protezione difficilmente raggiungibile con tecnologie tradizionali, che spesso mostrano limiti di scalabilità nella protezione dei container durante l'esecuzione.

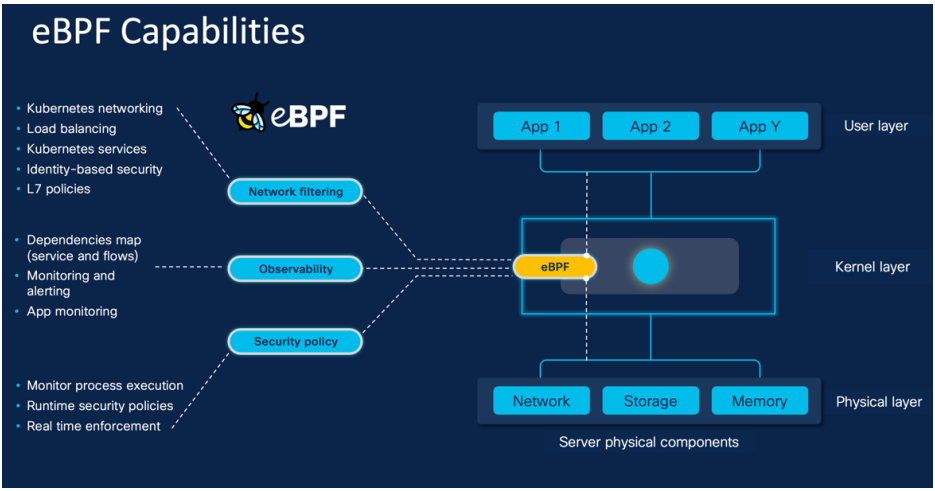
Principali strategie di sicurezza per Kubernetes:

- monitoraggio continuo: Sorveglia costantemente i container per individuare attività sospette o anomalie;
- controllo degli accessi: Restringe l'interazione con i container, definendo permessi rigorosi;
- rilevamento delle intrusioni: Identifica e risponde ai tentativi di accesso non autorizzato o compromissione;
- gestione delle vulnerabilità: Aggiorna e risolve regolarmente le vulnerabilità nel software dei container;
- isolamento: Mantiene i container separati per prevenire la diffusione delle minacce;
- log e auditing: Registra eventi e attività per analisi e conformità.

L'integrazione di sistemi di sicurezza basati sull'intelligenza artificiale può rafforzare significativamente la protezione, automatizzando il rilevamento e la mitigazione delle minacce in tempo reale e adattandosi rapidamente ai cambiamenti infrastrutturali e ai nuovi scenari di attacco. **In questo contesto, la sinergia tra la tecnologia eBPF (Extended Berkeley Packet Filter) e l'IA può elevare la cybersecurity a un livello superiore di sofisticazione.**

eBPF e l'Intelligenza Artificiale nella Sicurezza

Uno degli strumenti più efficaci per garantire la sicurezza negli ambienti Kubernetes è eBPF una tecnologia avanzata, integrata nel kernel di Linux e prossimamente anche in quelli Windows, che consente di monitorare e filtrare il traffico di rete in tempo reale senza impattare negativamente sulle prestazioni.



Operando direttamente nel kernel del sistema operativo, eBPF offre un livello di protezione granulare e adattivo, capace di rispondere automaticamente ai cambiamenti dell'infrastruttura.

Oltre alla protezione della rete, eBPF permette di:

- rilevare anomalie nel comportamento delle applicazioni;
- identificare attività sospette in tempo reale;
- applicare misure di mitigazione automatizzate senza necessità di aggiornamenti manuali delle policy di sicurezza.

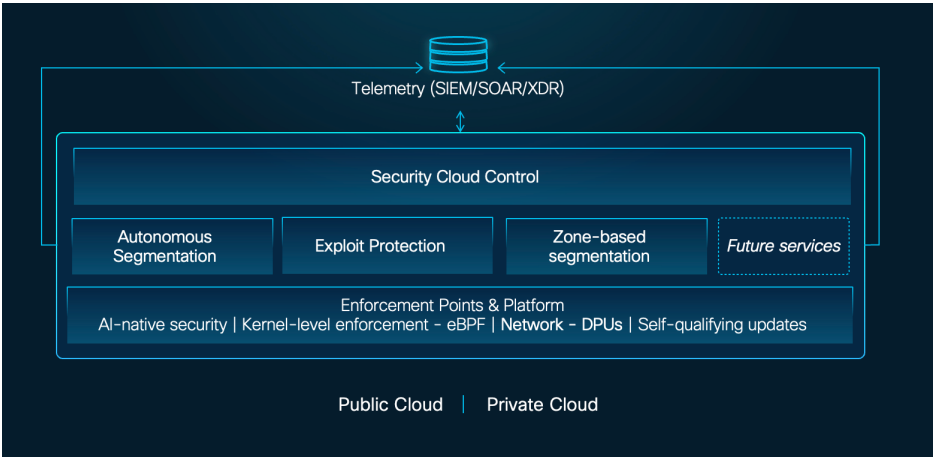
L'integrazione di eBPF con l'intelligenza artificiale porta la cybersecurity a un livello avanzato. L'IA analizza in tempo reale i dati generati da eBPF, individuando pattern e anomalie con maggiore precisione. Grazie all'apprendimento continuo, il sistema migliora progressivamente la capacità di prevenire attacchi sofisticati, la protezione diventa cosi proattiva, anticipando le minacce prima che possano compromettere il Sistema.

L'adozione di tecnologie avanzate come eBPF e aI permette di proteggere i cluster Kubernetes e le applicazioni:

- monitorando e controllando i processi in esecuzione e le comunicazioni tra i carichi di lavoro;
- applicando patch di sicurezza in modo automatico e senza interruzioni;
- automatizzando i processi di protezione, riducendo la necessità di intervento manuale.

In un panorama di minacce in continua evoluzione, affidarsi a un approccio AI-driven e a tecnologie come eBPF significa costruire un ecosistema Kubernetes più sicuro, resiliente e pronto per il futuro.

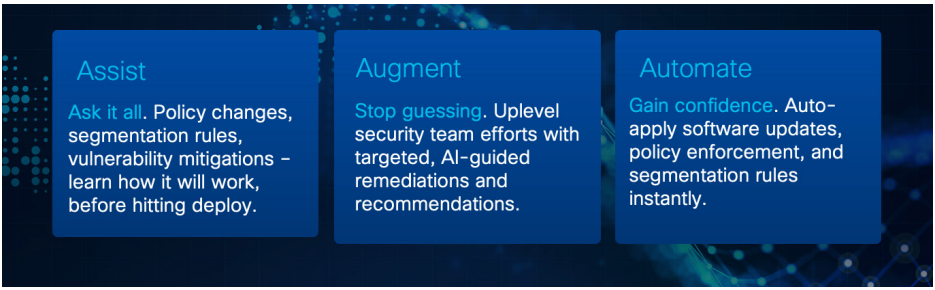
Diventa pertanto necessario reinventare la sicurezza negli ambienti cloud pubblici e privati e progettare nuove soluzioni per la Container security che grazie a una architettura distribuita e all'integrazione nativa dell'intelligenza artificiale raggiungano visibilita' estramente approfondita e un autonomia di molto maggiore rispetto alle soluzioni tradizionali.



Si tratta di sistemi software progettati per un modello di policy basato sugli intenti, con gestione centralizzata (cloud-based), enforcement distribuito e indipendente dal fattore di forma e orientati ai seguenti casi d'uso.

1. Segmentazione autonoma per controllare il movimento laterale tra i carichi di lavoro nei cloud pubblici e privati;
2. Protezione dagli exploit distribuiti per accelerare la protezione dagli exploit di vulnerabilità, mantenendo le applicazioni attive e funzionanti.

Per garantire la resilienza e la continuità operativa richiesta dalle applicazioni critiche questi sistemi devono avere capacità intrinsiche di "self-upgrading" e "self-updating" e integrare un motore IA addestrato per assistere, aumentare e automatizzare i workflow di sicurezza.



Assistere

Il motore di analisi AI nativo individua una vulnerabilità sfruttata attivamente "in the wild" e ne conferma la presenza su un asset di alto valore. Genera immediatamente raccomandazioni di correzione per mitigare l'attacco. Gli analisti della sicurezza ricevono il supporto necessario per stabilire le priorità, migliorando l'efficacia nei loro ruoli.

Aumentare

È risaputo che non sempre è possibile applicare patch alle applicazioni vulnerabili: a volte non esiste una patch disponibile, altre volte può causare effetti indesiderati. Per questo motivo, è essenziale eseguire molteplici test in ambienti non produttivi prima di implementarle in quelli di produzione.

Questi sistemi propongono automaticamente diverse opzioni personalizzate per l'ambiente specifico del cliente. Inoltre, verifica se altri clienti hanno già implementato queste soluzioni e quali risultati hanno ottenuto, con l'obiettivo di aumentare la fiducia nei risultati raggiunti grazie all'uso dell'IA.

Automatizzare

Il sistema automatizza il test degli aggiornamenti delle policy o delle patch sul traffico di produzione in tempo reale, senza influire sull'applicazione in esecuzione. È progettato per consentire all'amministratore di determinare il livello di autonomia con cui si sente a proprio agio, utilizzando funzionalità di test, registrazione e report per aumentarne la confidenza

Si può immaginare una soluzione di sicurezza di rete capace di scrivere le proprie regole, testarle, distribuirle e gestirne il ciclo di vita.

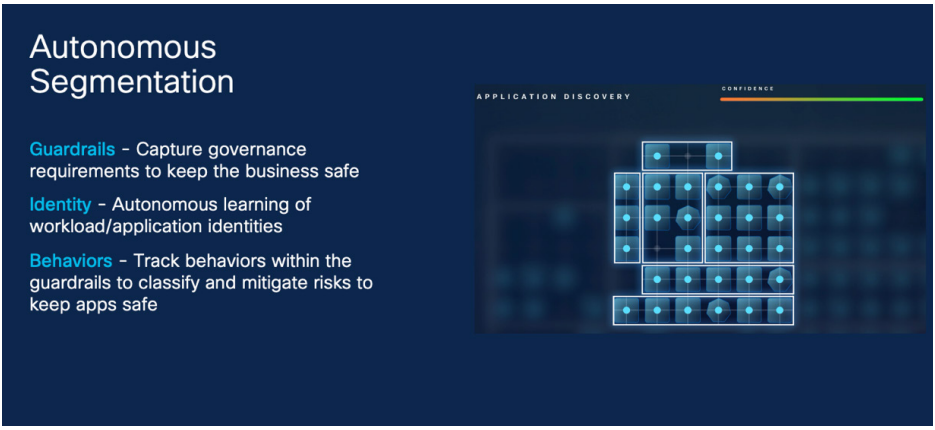
Segmentazione autonoma

La segmentazione della rete è stata a lungo una necessità obbligatoria nelle reti aziendali per diminuire e controllare il cosiddetto "blast radius" (raggio di esplosione) in caso di attacco.

Nonostante decenni di investimenti, molte reti restano ancora piatte o sottosegmentate. Gli amministratori della sicurezza trovano il processo di segmentazione complesso e lento. I clienti riferiscono che possono essere necessari 40 giorni o più per definire le regole di segmentazione per una singola applicazione, un tempo decisamente troppo lungo.

I sistemi di sicurezza basati su AI forniscono una soluzione efficiente ed elegante a questi problemi. Informati da quanto accade in tutti gli ambienti che proteggono e guidati dall'intelligenza artificiale estendono la visibilità dei tradizionali flussi di rete ed esaminano, avvalendosi di informazioni di threat intelligence, un'ampia gamma di comportamenti identificando quelli riconducibili a vulnerabilità e tecniche/tattiche di attacco. Inoltre, apprendono dalle best practices, suggeriscono e guidano la modifica delle regole di segmentazione e modella le azioni eseguite durante un attacco.

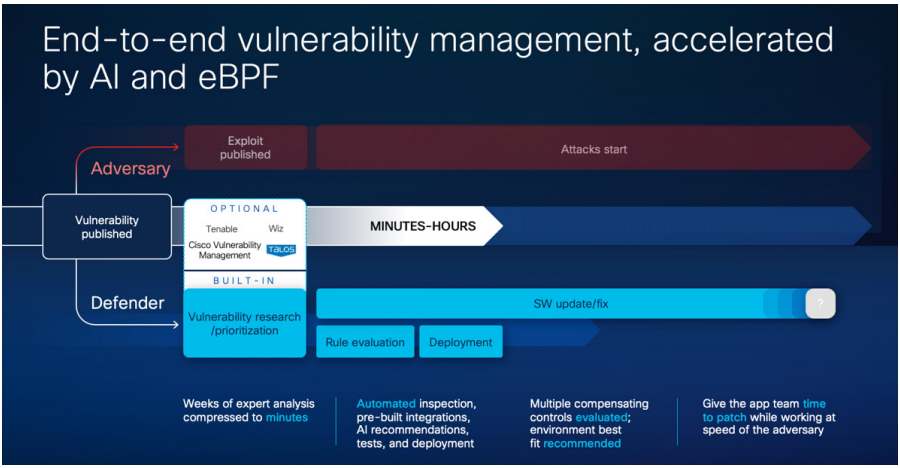
Il risultato è una rete segmentata in modo autonomo con raccomandazioni supportate da dati in tempo reale e gestite sotto la supervisione dell'amministratore della sicurezza.



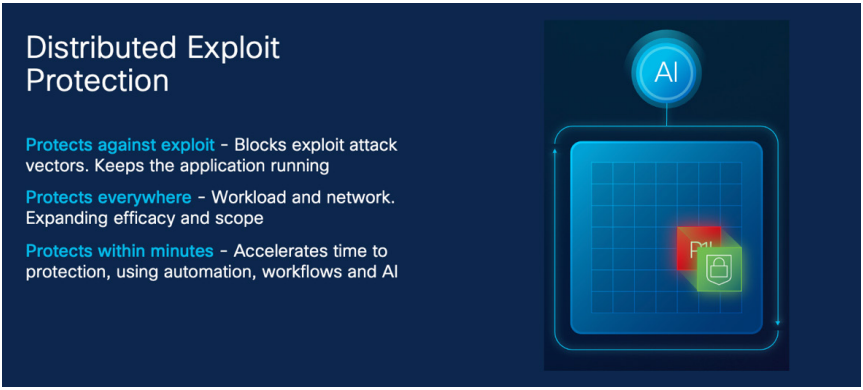
Protezione dagli exploit distribuiti

L'applicazione di patch per le vulnerabilità note è un problema complesso a causa della rete di eventi necessari, come la disponibilità e compatibilità delle patch, finestre di manutenzione e cicli di test, che devono allinearsi per eliminare la vulnerabilità. Nel frattempo, la situazione peggiora con la continua scoperta di nuove vulnerabilità. Ad esempio, la threat intelligence di Cisco, Talos, identifica centinaia di nuove vulnerabilità ogni anno, e circa 80 nuovi CVE vengono segnalati quotidianamente. Gli aggressori riducono costantemente il tempo tra il rilascio pubblico di nuove informazioni su una vulnerabilità e il primo exploit, aumentando così le loro possibilità di successo con il passare del tempo.

Un moderno sistema di protezione offre una soluzione completa per l'applicazione di patch alle vulnerabilità. Oltre alle funzionalità integrate per la gestione delle vulnerabilità, deve integrarsi con gli strumenti di gestione delle vulnerabilità di terze parti e sfruttare un modello di apprendimento continuativo in grado di verificare la presenza di vulnerabilità in rete, valutarne il rischio in base alla disponibilità di un eventuale exploit e alla criticità dei carichi di lavoro esposti.



L'intelligenza artificiale analizza tutte le potenziali minacce nell'ambiente e assegna loro la priorità in modo che ciascuna possa essere affrontata in modo appropriato con controlli di compensazione, fornendo protezione e dando ai team di sicurezza il tempo di indagare e mitigare. Questi controlli di compensazione sono applicati con modalita' chirurgica e vanno a bloccare la catena di attacco della vulnerabilità senza interferire con le funzionalità dell'applicazione.



Aggiornamenti continui

Come descritto in precedenza, la continuità operativa delle applicazioni critiche è fondamentale per garantire la resilienza di un business moderno e digitale.

Un sistema di protezione avanzato è progettato per sfruttare l'intelligenza artificiale, permettendo aggiornamenti automatici e manuali.

L'integrazione nativa dell'IA consente al sistema di apprendere progressivamente le specificità del contesto operativo, migliorando l'affidabilità delle raccomandazioni. Questo permette agli utenti di valutare l'aumentata affidabilità del sistema e, di conseguenza, concedere gradualmente al sistema un maggiore livello di autonomia garantendo un livello di protezione accurato con sforzi operativi più contenuti.

Conclusioni

Nel frenetico panorama digitale odierno, la capacità di sviluppare, distribuire e scalare applicazioni senza problemi è diventata una pietra miliare dell'innovazione. Kubernetes, una solida piattaforma di orchestrazione dei containers, è emersa come lo standard de facto per la gestione delle moderne architetture applicative. La sua flessibilità e scalabilità consentono alle organizzazioni di creare applicazioni resilienti e native per il cloud, in grado di soddisfare le esigenze di un mercato in rapida evoluzione. Tuttavia, con questa evoluzione emergono anche nuove sfide di sicurezza, in particolare per le architetture iper-distribuite come Kubernetes.

Nonostante i numerosi vantaggi offerti, la dinamicità degli ambienti Kubernetes richiede strategie di sicurezza avanzate per proteggere efficacemente le applicazioni. Tra queste strategie, il monitoraggio continuo dei container per individuare attività sospette, il controllo rigoroso degli accessi e il rilevamento delle intrusioni sono fondamentali. Inoltre, la gestione delle vulnerabilità e l'isolamento dei container sono essenziali per prevenire la diffusione delle minacce e garantire la protezione delle applicazioni.

Incorporare Kubernetes nelle infrastrutture IT non solo supporta la modernizzazione e la scalabilità, ma anche la protezione delle applicazioni in un contesto sempre più complesso. Investire in tecnologie di sicurezza adeguate e strategie proattive è quindi cruciale per sfruttare appieno i benefici di Kubernetes, senza compromettere la sicurezza dell'intera infrastruttura. Solo attraverso un approccio integrato e consapevole, le organizzazioni possono garantire un ambiente digitale sicuro e resiliente, pronto ad affrontare le sfide del futuro.

Riferimenti

[1] Cisco AI Readiness Index 2024 - https://www.cisco.com/c/m/en_us/solutions/ai/readiness-index.html
[2] Cisco Cybersecurity Readiness Index 2024 - https://transform.cisco.com/opsadmin/2024cybersecurityreadinessindex?xs=605654

Intelligenza Artificiale nella Cybersecurity: opportunità e minacce

(A cura di Umberto Pirovano, Palo Alto Networks)

Quale ruolo l'AI debba svolgere nella cybersecurity rappresenta uno dei temi più dibattuti e articolati degli ultimi anni.

Il motivo di tale interesse per una tecnologia teorizzata già a metà degli anni 50 è strettamente legato all'avvento della AI generativa, che introduce una sorta di "salto quantico" rispetto a ciò che poteva essere fatto finora.

Quando valutiamo i benefici derivanti dalla rivoluzione nel modo di rapportarci alle macchine che l'AI generativa introduce non possiamo trascurare gli impatti sulla sicurezza derivanti dall'utilizzo di applicazioni Gen AI da parte degli utenti. Allo stesso tempo dobbiamo ragionare sulla sicurezza intrinseca delle applicazioni AI che espandono ulteriormente la superficie di attacco aziendale.

Le tecnologie predittive (ML) fanno parte del bagaglio di risorse a disposizione della cybersecurity da molti anni e i casi di uso si sono evoluti con l'evoluzione della tecnologia.

Se, per esempio, analizziamo la protezione del traffico inline, ci accorgiamo che una tecnologia capace di identificare e bloccare quanto già noto non è più sufficiente da lungo tempo. Prendiamo in esame una semplice funzione di URL filtering: la velocità e l'automazione con cui chi attacca è in grado di realizzare e pubblicare nuovi siti e nuovi vettori non consentono una protezione adeguata fino al riconoscimento e alla classificazione del sito come malevolo. La finestra di scopertura per ciascun nuovo sito potenzialmente malevolo aumenta al crescere della frequenza di "pubblicazione" di nuovi siti.

L'URL filtering classico quindi rimane utile come sistema di controllo dell'accesso a determinate categorie di siti, ma non ha alcuna valenza come sistema di protezione cyber.

Introducendo però, ad esempio, un sistema a due livelli di ML in line e DL in near real time, posso realizzare ciò che è definibile Advanced Url Filtering in grado di identificare velocemente la natura di un sito mai visto in precedenza, fornendo un verdetto immediato che permette di prendere una decisione di sicurezza immediata.

Estendendo il concetto a motori di threat prevention, DNS security, IoT security e behavioral analysis, diventa evidente il motivo per cui negli ultimi 10 anni sia diventato imprescindibile l'utilizzo di tecnologie predittive nella cybersecurity.

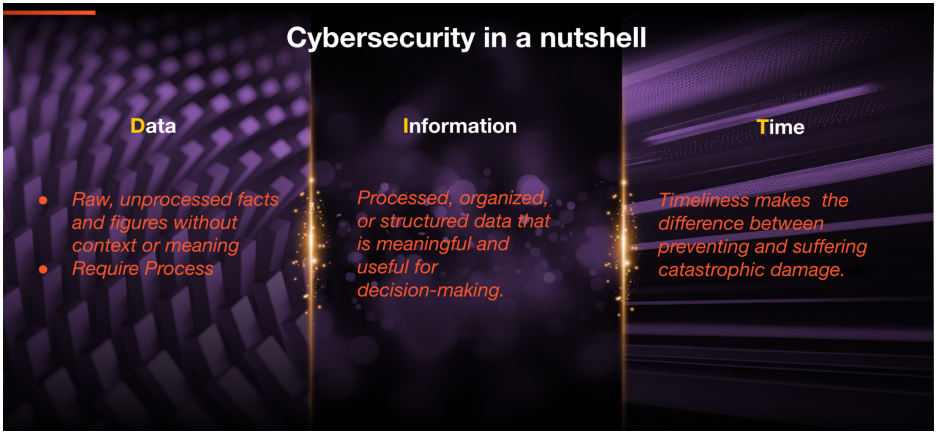
Ipersemplificando e rimanendo nell'ambito tecnico, la cybersecurity è una questione di informazioni e di tempo. Su una qualunque collezione di dati devo estrarre l'informazione per ottenere un verdetto su un evento, quindi compiere un'azione nel minor tempo possibile, idealmente in real time.

La "qualità" dei dati gioca un ruolo importante oltre alla quantità: non a caso si è passati gradualmente dai log a dati telemetrici e dal raccogliere dati di flow o log di firewall, al consolidamento in datalake di dati provenienti da network, host, cloud, utenti. IoT/OT, etc.

Il paradosso dei SIEM per i quali l'ingestion di dati era limitata a causa dei costi o di limitazioni nella scalabilita' mal si coniuga con l'esigenza di avere più dati e con più contesto.

Molte delle strategie IT o di security adottate dalle aziende hanno portato all'esplosione dei dati: si pensi, ad esempio, a un approccio Zero Trust o ai temi della cloud transformation.

L'importanza di poter disporre di dati pronti per la manipolazione è evidente quando consideriamo che le analisi forensiche post incidenti hanno una probabilità altissima (oltre il 90%) di identificare l'intera catena di occorrenze che ha portato a un breach di successo. Ciò dimostra che le informazioni erano presenti, ma che non si è avuta la capacità di utilizzarle in tempo reale.



Non c'è nulla di meglio di una macchina per estrarre informazioni dai dati molto rapidamente, anche petabyte di dati al giorno.

La criticità del fattore tempo è evidente: quanto prima riesco a convertire un dato in informazione tanto prima posso iniziare una qualsiasi azione, che sia di blocco o di remediation.

Il tempo è un fattore chiave per i **clienti**: se identifico in anticipo un artefatto o una URL malevola sono protetto, se mi accorgo dei prodromi di un attacco o di una esposizione prima che l'attacco inizi posso sulla carta intervenire, e se infine il disastro è avvenuto, prima rispondo con mitigazione e risoluzione e analisi post mortem, prima riparto.

Il tempo è un fattore chiave per i **normatori**: tutte le norme recenti hanno richiesto di ridurre i tempi nell'identificazione e nell'azione in caso di breach. Un aspetto assolutamente ovvio, poiché resilienza significa anche tornare a erogare i servizi vitali o a produrre col minore impatto possibile.

Il tempo è infine un fattore chiave **per il SOC**, dove la valutazione dell'efficienza può essere quantificata dal tempo medio di detection e remediation (MTTR/MTTD): abbiamo quindi una misura oggettiva di quanto il SOC sia performante e quanto sia critico questo elemento considerando i due punti precedenti. Ridurre questi tempi da ore, o addirittura giorni, a minuti è uno degli aspetti più interessanti derivanti dall'utilizzo di AI predittiva e generativa.

Tralasciamo per un attimo i benefici legati all'utilizzo della generativa nelle operation e nella gestione del ciclo della cybersecurity, rimandando per questo a un qualunque articolo su Copilot, e cerchiamo di illustrare invece il lato oscuro della medaglia.

Anche nella condizione in cui la AI sia impiegata per dare risposte (ad esempio il verdetto su un artefatto o query in linguaggio naturale sullo stato di sicurezza), il considerarla fonte di verità assoluta può condurre a una risposta errata sulle operazioni seguenti, con un impatto assai rilevante. Per quanto riguarda il real time, ad esempio, un verdetto errato potrebbe consentire il passaggio di un ransomware, una risposta sbagliata sull'automazione nella gestione di un incidente potrebbe portare all'adozione di strategie di remediation controproducenti.

La precisione, sia nel caso di predittiva sia della generativa, è quindi un fattore fondamentale.

Ci sono poi i rischi derivanti dall'utilizzo di AI. Come già accennato, le aziende dovrebbero considerare assolutamente funzioni di sicurezza in grado di visualizzare e normare l'utilizzo di strumenti Gen AI in SaaS: ci sono, infatti, aspetti legati all'esposizione di dati e proprietà intellettuale (ad esempio codice sorgente nel caso degli assistenti allo sviluppo) con impatti potenzialmente rilevanti in termini di security posture e gestione del rischio.

L'assenza di chiare politiche di utilizzo di GenAI può portare a problemi nel rapporto con i dipendenti, tra cui insoddisfazione, riduzione della produttività e la possibilità per essi di eludere divieti o restrizioni sull'utilizzo delle app GenAI.
La diffusa disponibilità di strumenti GenAI pubblici, in generale, crea nuovi vettori di attacco per i criminali informatici, che vanno opportunamente trattati.

Tornando al tema dell'impatto sulla superficie d'attacco portato dall'implementazione delle tecnologie AI nelle infrastrutture dei clienti, la situazione attuale e' dominata da applicazioni tipo chat-bot, ma e' necessario che le organizzazioni siano pronte per lo step successivo, ovvero il passaggio agli AI Agents per realizzare infrastrutture sicure.

Un recente studio pubblicato da Langchain (https://www.langchain.com/stateofaiagents) mostra che il 78% delle aziende ha un piano per l'introduzione di AI Agents in ambienti di produzione, prevedendo un passaggio piuttosto repentino a questo tipo di approccio.

Dal punto di vista della cybersecurity gli AI Agents introdurranno un ulteriore aumento dei potenziali vettori di attacco e nuovi livelli di rischio, in una traiettoria evolutiva iniziata dall'adozione e dallo sviluppo di applicazioni Gen AI interne.

Secondo la nostra visione, l'adozione e lo sviluppo di applicazioni Gen AI interne, richiedono un approccio di sicurezza by design sin dalle prime fasi di stesura codice, così come la necessità di assicurare la postura di sicurezza e la protezione dell'intera farm AI in termini di runtime protection. Quest'ultimo tipo di tecnologia è concepita per proteggere le applicazioni IA, siano esse realizzate su piattaforme low-code/no-code, come Microsoft Copilot Studio o VoiceFlow, sia per agenti AI sviluppati con workflow personalizzati. Essa offre una solida protezione per gli AI Agents difendendoli da una varietà di potenziali minacce, tra cui:

- **prompt injections:** gli hacker manipolano i sistemi di intelligenza artificiale generativa fornendo loro input dannosi mascherati da prompt utente legittimi;
- **perdite di dati sensibili:** rendono i dati di addestramento suscettibili a leak nelle risposte dell'applicazione;

- **URL dannosi:** un modello di intelligenza artificiale può essere indotto con l'inganno a compilare un URL contenente un dominio di proprietà dell'aggressore con dati sensibili incorporati nei parametri URL. L'app o l'utente finale potrebbero quindi tentare di recuperare l'URL, che invia i dati al server dell'aggressore.

L'interesse per gli AI Agents è notevole in diversi ambiti, incluso quello delle operations in cybersecurity, considerato come step successivo alle attuali automazioni nei processi dei SOC (ad esempio data stitching automatico o identificazione automatica delle evoluzioni dei playbooks).

Ad alto livello, gli agenti IA sono molto più avanzati dei tipici chatbot di risposta alle domande a cui siamo abituati. Vanno oltre le semplici query: sono sistemi sofisticati e autonomi che agiscono per conto degli utenti. Invece di limitarsi a rispondere, pensano, decidono e si adattano attivamente.

Fondamentalmente, un agente AI è un sistema software intelligente che può:

- percepire il suo ambiente: gli agenti AI percepiscono il loro ambiente per raccogliere informazioni rilevanti. Queste informazioni potrebbero provenire da flussi di dati, input di sistema o altre fonti esterne, inclusi altri agenti. Assorbono costantemente informazioni per comprendere il mondo che li circonda;
- "ragionare" su ciò che sta accadendo: una volta che l'agente dispone di tutti questi dati, deve elaborare e dare un senso alle informazioni. È qui che l'agente applica algoritmi e logica per analizzare le informazioni, in modo simile a come gli esseri umani ragionano sui problemi;
- prendere decisioni basate su quel ragionamento: sulla base delle intuizioni del ragionamento, l'agente deve scegliere la migliore azione possibile per raggiungere i suoi obiettivi. Che si tratti di risolvere un problema complesso o di ottimizzare un processo, l'obiettivo è sempre quello di selezionare il percorso più efficace da seguire;
- agire in modo autonomo: gli agenti IA sono progettati per operare in modo indipendente e non richiedono l'intervento umano per ogni decisione. Possono adattarsi alle nuove informazioni e agli ambienti in evoluzione, dirigendosi continuamente verso i propri obiettivi senza essere guidati manualmente.

Poiché sono intelligenti, adattabili e spinti ad agire in modo indipendente, gli agenti IA possono essere strumenti incredibilmente potenti per le aziende, incluso l'ambito della cybersecurity: possono, ad esempio, spingere a un livello finora mai raggiunto l'evoluzione verso un SOC autonomo.

Tuttavia, come vedremo, queste stessa autonomia e capacità decisionali indipendenti introducono anche nuove sfide alla sicurezza.

Diamo un'occhiata più da vicino al loro funzionamento interno e all'architettura che rende questi agenti così potenti.

- **Memoria a breve termine:** aiuta l'agente a ricordare dettagli immediati e importanti, come l'attività corrente o eventuali obiettivi su cui sta lavorando.
- **Memoria a lungo termine:** immagazzina esperienze e conoscenze passate. È qui che l'agente impara dalle sue azioni e si adatta. Va considerata come la capacità dell'agente di migliorare nel tempo in base alla sua storia e alle sue esperienze.
- **Modulo di pianificazione:** il centro strategico dell'agente determina come raggiungere gli obiettivi e svolgere le attività.
- **I tool sono risorse o funzioni esterne** che l'agente può utilizzare per facilitare le attività. L'agente utilizza questi strumenti secondo necessità e li integra nei processi di pianificazione e decisione per raggiungere gli obiettivi in modo più efficace.

Un agente AI è un sistema ben organizzato con memoria, pianificazione e strumenti che lavorano di concerto per aiutarlo a pensare, apprendere e agire in modo autonomo. È un sistema dinamico e in evoluzione in grado di risolvere problemi e migliorare nel tempo, in totale autonomia. Alcuni agenti operano in un sistema multi-agente AI, in cui più agenti AI collaborano per affrontare compiti complessi, aumentando il loro potere e, nel contempo, la loro vulnerabilità.

In che modo gli aggressori possono sfruttare gli agenti AI?

Per quanto potenti siano gli agenti AI, essi comportano una serie di sfide per la sicurezza. Queste sfide si basano sulla capacità dell'agente di modificare il proprio comportamento e di agire nell'interesse degli aggressori anziché dell'organizzazione. Questi exploit includono, tra gli altri, quanto segue:

- **manipolazione dei dati contestuali:** manipolando i sistemi di memoria, gli aggressori possono corrompere le informazioni archiviate sulle interazioni passate e sui dati contestuali. Una volta inserite informazioni false o modificato il contenuto della memoria esistente, gli aggressori possono costringere gli agenti a prendere decisioni errate, ignorare i protocolli di sicurezza o agire contro gli interessi degli utenti, mentre sembrano funzionare normalmente. La persistenza di questo attacco lo rende particolarmente pericoloso, poiché la memoria danneggiata può influenzare il comportamento dell'agente in più sessioni e interazioni;

- **attacco di sfruttamento degli strumenti:** attraverso richieste attentamente elaborate, gli aggressori possono indurre gli agenti di intelligenza artificiale a utilizzare involontariamente strumenti legittimi e autorizzazioni di accesso. Questo sfruttamento può consentire l'accesso non autorizzato a dati sensibili o risorse di sistema senza attivare avvisi di sicurezza standard;
- **distorsione dell'output fabbricata:** gli aggressori possono generare intenzionalmente output falsi o inaffidabili sfruttando la tendenza degli agenti di intelligenza artificiale a fare supposizioni di fronte a informazioni incomplete o ambigue. Questa vulnerabilità è particolarmente pericolosa nei sistemi autonomi, dove gli agenti agiscono su questi output generati senza verifica umana. Ciò potrebbe portare ad azioni non autorizzate o a un processo decisionale errato, compromettendo la sicurezza e l'affidabilità del sistema.

Cybersecurity in sanità: incidenti in crescita e nuove misure di protezione e sanzioni con NIS2

(A cura di Sonia Montegiove, Manuela Santini, Sofia Scozzari e Anna Vaccarelli - Women For Security)

Lo scenario

Il settore sanitario risulta uno di quelli maggiormente colpiti e con un andamento degli incidenti in crescita. Le ragioni sono diverse e concomitanti. Prima di tutto c'è da sottolineare il fatto che i dati sanitari sono facilmente rivendibili nel dark web con ampi guadagni. Inoltre, non è infrequente che nei sistemi siano presenti vulnerabilità note e non sistemate, che consentono un facile accesso agli attaccanti.

I rischi ai quali è maggiormente sottoposto l'ambiente sanitario sono:

1. **Violazione dei dati**: le violazioni dei dati possono portare alla perdita o al furto di informazioni personali dei pazienti, come i dettagli delle assicurazioni sanitarie, i numeri di previdenza sociale, i risultati dei test medici e altre informazioni sensibili.
2. **Ransomware**[1]: gli attacchi ransomware sono diventati sempre più comuni nel settore sanitario. I cybercriminali criptano i dati dei pazienti chiedendo un riscatto per sbloccarli, causando interruzioni nei servizi sanitari e mettendo a rischio la sicurezza delle persone malate.
3. **Accesso non autorizzato**: gli hacker possono tentare di ottenere accesso non autorizzato ai sistemi informatici della sanità per rubare informazioni.
4. **Dispositivi medici connessi**: con l'aumento dei dispositivi medici connessi alla rete, come monitor cardiaci e pompe per insulina, cresce il rischio di attacchi informatici che potrebbero compromettere la sicurezza dei pazienti.

Spesso gli attacchi vanno a buon fine (come, d'altra parte, nella maggior parte dei casi anche in altri settori, a causa di errori umani dovuti a **mancanza di formazione in materia di sicurezza**: il personale sanitario risulta spesso non adeguatamente formato per riconoscere le minacce alla sicurezza informatica e adottare contromisure adeguate per prevenirle.

[1] https://it.wikipedia.org/wiki/Ransomware

Uno dei danni maggiori è la violazione dell'integrità dei dati medici, modificando i risultati dei test o i dettagli dei trattamenti, con gravi danni alla salute delle persone. L'altro è il blocco delle prestazioni sanitarie che può essere causato da un attacco, con il rischio per molti pazienti di non poter ricevere tempestivamente cure adeguate o programmate. Un aspetto positivo che potrebbe mitigare i rischi nel settore sanitario è l'obbligo di sottostare a numerose normative e regolamenti in materia di sicurezza dei dati tra cui GDPR e NIS2. Essendo previste delle sanzioni, è possibile che questa prospettiva funzioni da deterrente e si dedichi maggiore attenzione ai problemi di sicurezza informatica, come è successo e sta succedendo in altri settori.

I cyber attacchi verso il settore Healthcare nel 2024

L'Healthcare è un ambito sempre più preso di mira dai cyber criminali. Il settore sanitario a livello globale ha infatti registrato **810 cyber incidenti divenuti di pubblico dominio nel 2024**[2], il 30% in più rispetto all'anno precedente e il quadruplo rispetto al 2020 e 2021, con un trend in forte crescita che non accenna a diminuire.

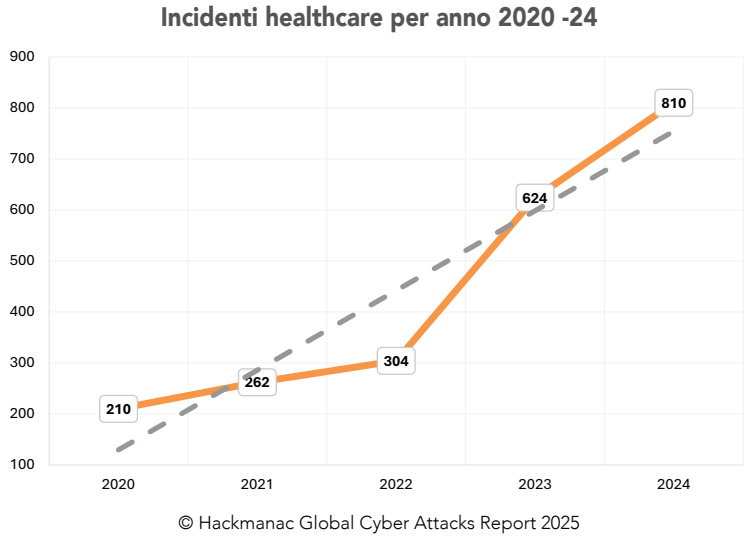


Fig. 1 - Trend dei cyber incidenti nel settore sanitario nel periodo 2020 - 2024

La media arriva a **68 incidenti al mese** (contro i 52 del 2023), mentre gennaio, febbraio e maggio risultano i mesi più attivi, a differenza dei mesi estivi e di dicembre dove le attività malevole sono inferiori.

[2] Fonte: Hackmanac Global Cyber Attacks Report 2025

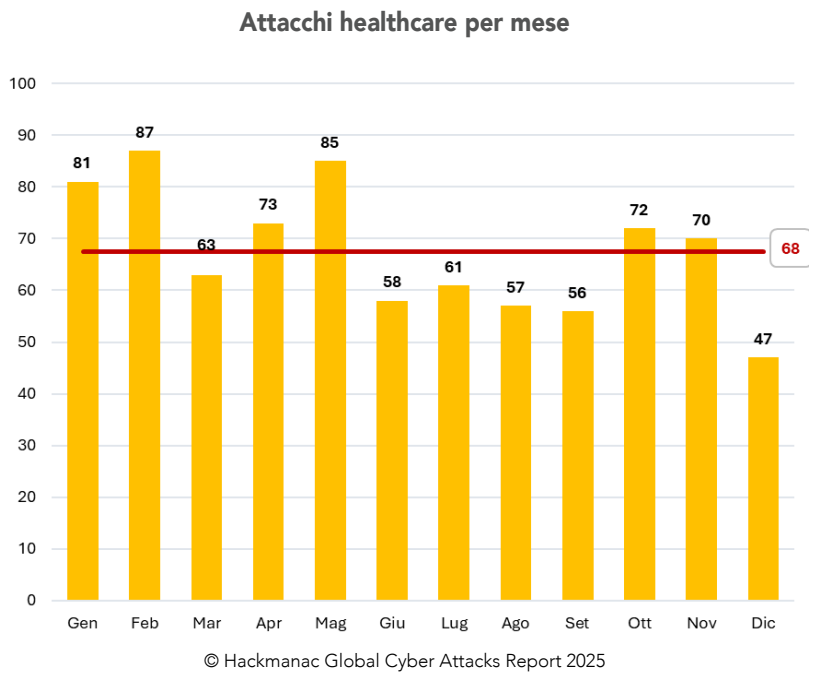


Fig. 2 - Andamento mensile degli incidenti globali verso il settore sanitario nel 2024

Sostanzialmente il 100% degli incidenti (806 incidenti complessivi) ha avuto una motivazione di stampo cybercriminale, mentre solo una manciata (4 in totale) deriva da attività di *hacktivism*[3] e di *cyber espionage*[4].

Il settore sanitario è maggiormente colpito nel continente americano (78% in lieve diminuzione rispetto all'80% del 2023), mentre aumentano le vittime in Europa (14% dal 12%) e in Asia (5% dal 4%). Oceania (2%) e Africa (1%) vengono interessate in misura minore e restano stabili (**Fig. 3**).

[3] https://it.wikipedia.org/wiki/Hacktivism

[4] https://www.cybersecurity360.it/nuove-minacce/cyber-espionage-una-seria-minaccia-per-le-aziende-attori-criminali-e-misure-di-contrasto

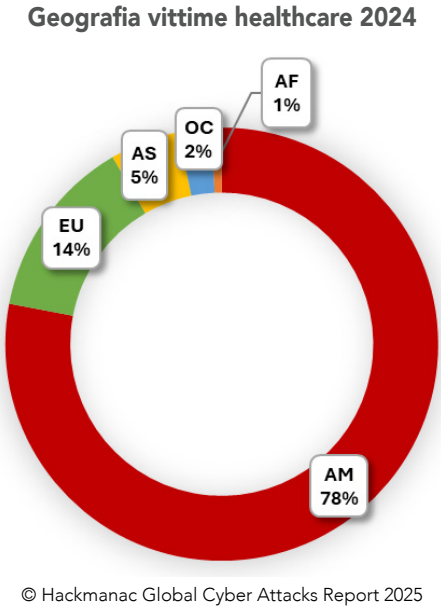


Fig. 3 - Geografia delle vittime dei cyber incidenti in ambito sanitario nel 2024

Assente, invece, anche quest'anno la quota di incidenti verso località multiple, a fronte del fatto che nel 2024, come nell'anno precedente, gli attacchi tendono a essere maggiormente mirati (**Fig. 4**).

I Malware, e in particolare i ransomware, rappresentano nuovamente la tecnica di attacco prediletta dai cyber criminali nelle loro operazioni malevole che colpiscono il settore, con una quota di adozione in crescita rispetto al 2023 (60%, +3pp) e doppia rispetto al 2022 (**Fig. 5**).

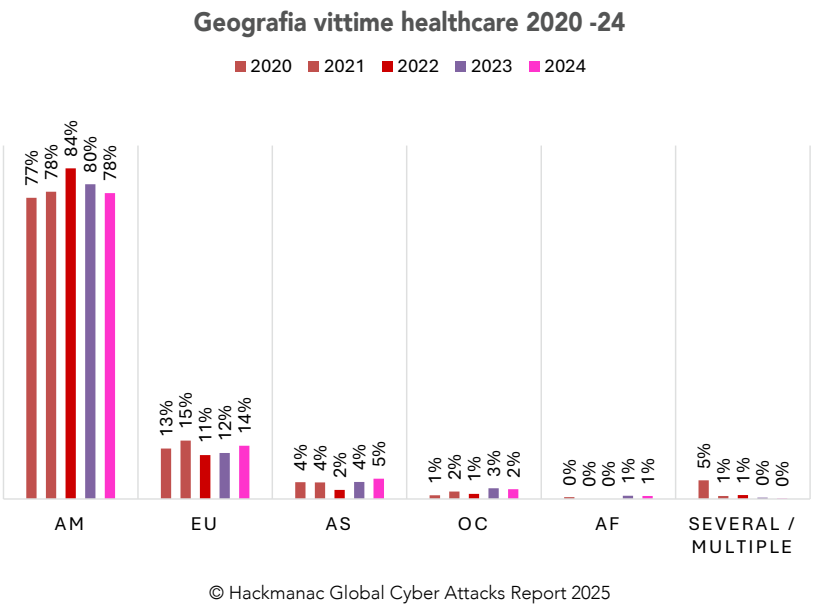


Fig. 4 - Distribuzione geografica delle vittime nel settore Healthcare nel periodo 2020-24

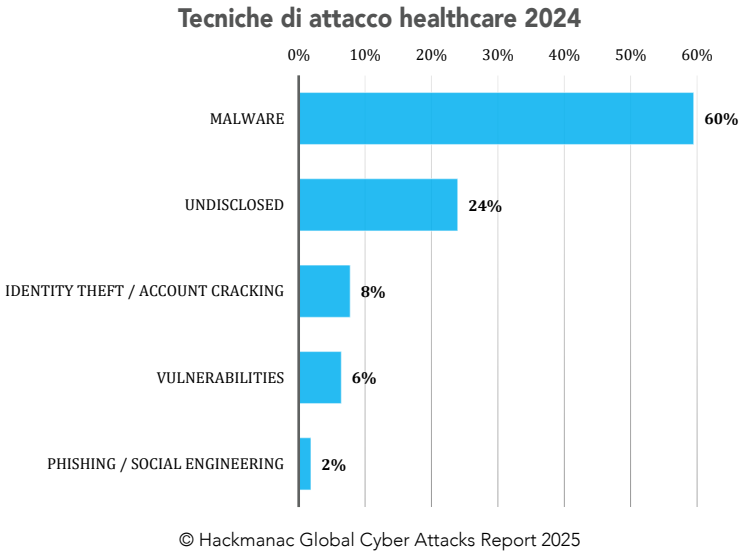
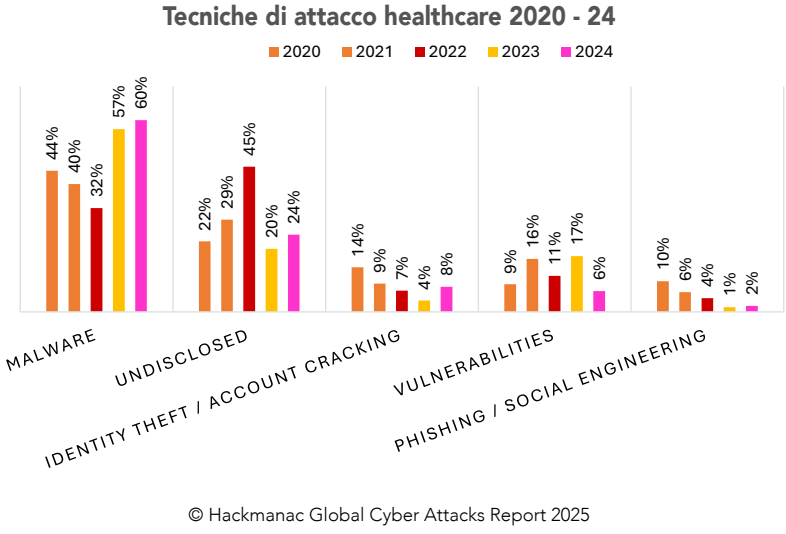


Fig. 5 - Tecniche di attacco verso il settore Healthcare nel 2024

Aumenta anche il ricorso a "tecniche non classificate" (undisclosed) (perlopiù data breach[5], 24%) e a furti di identità e violazioni di account (8%), in entrambi i casi con una crescita di 4 punti percentuali rispetto all'anno precedente. Inoltre, sebbene con un'adozione minore, raddoppia di fatto il ricorso a phishing[6] e ingegneria sociale[7] passando da 1% a 2%.



© Hackmanac Global Cyber Attacks Report 2025

Fig. 6 - Distribuzione delle tecniche di attacco verso il settore sanitario nel periodo 2020 - 2024

Diminuisce sensibilmente invece il ricorso allo sfruttamento delle vulnerabilità, incluse quelle pericolosissime non ancora note come gli 0-day[8], che perdono globalmente ben 11 punti percentuali, indice del fatto che nel 2024 i cybercriminali preferiscono affidarsi a tecniche più rodate e "affidabili" come i ransomware.

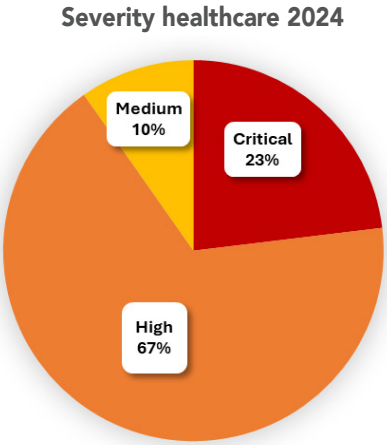
Per quanto riguarda, infine, le ripercussioni degli attacchi che colpiscono il settore sanitario, nel 2024 la quota di incidenti con impatti importanti gravi (67%) o gravissimi (23%) resta il 90% del totale, esattamente come nell'anno precedente, un chiaro sintomo di quanto il settore continui a essere pesantemente preso di mira.

5 https://it.wikipedia.org/wiki/Data_breach

6 https://it.wikipedia.org/wiki/Phishing

7 https://it.wikipedia.org/wiki/Ingegneria_sociale

8 https://it.wikipedia.org/wiki/0-day



© Hackmanac Global Cyber Attacks Report 2025

Fig. 7 - Severity cyber incidenti verso il settore sanitario nel 2024

La situazione italiana

In Italia le attività malevole verso il settore sanitario mostrano un andamento in leggera diminuzione rispetto all'anno precedente, passando da 15 a **13 cyber incidenti di successo e di pubblico dominio**, che totalizzano il 3% del degli incidenti registrati nel nostro paese (Fig. 8).

A differenza di quanto avvenuto nel 2023, le motivazioni degli attacchi vedono il Cybercrime come unico protagonista, mentre spariscono altre tipologie come *hacktivism* ed *espionage/sabotage* riscontrate invece nel campione globale (Fig. 9).

Le tecniche di attacco confermano il ricorso al Malware (54% dei cyber incidenti dell'anno), nello specifico ransomware, che si dimostra ormai lo strumento prediletto e maggiormente affidabile (dal punto di vista cybercriminale) per arrecare danni alle strutture sanitarie nazionali (Fig: 10).

Il ricorso a questa tecnica continua a essere al primo posto, pur perdendo diversi punti percentuali rispetto al 2023 a favore dello sfruttamento delle vulnerabilità. In questo caso parliamo di attacchi tramite la supply chain, che in Italia, a differenza di quanto avvenuto nel campione globale, quest'anno trovano terreno fertile mostrando, per la prima volta un'esorbitante crescita del 31%. Questo dimostra quanto la supply chain, in particolare nel settore sanitario, rappresenti una minaccia crescente (Fig. 11).

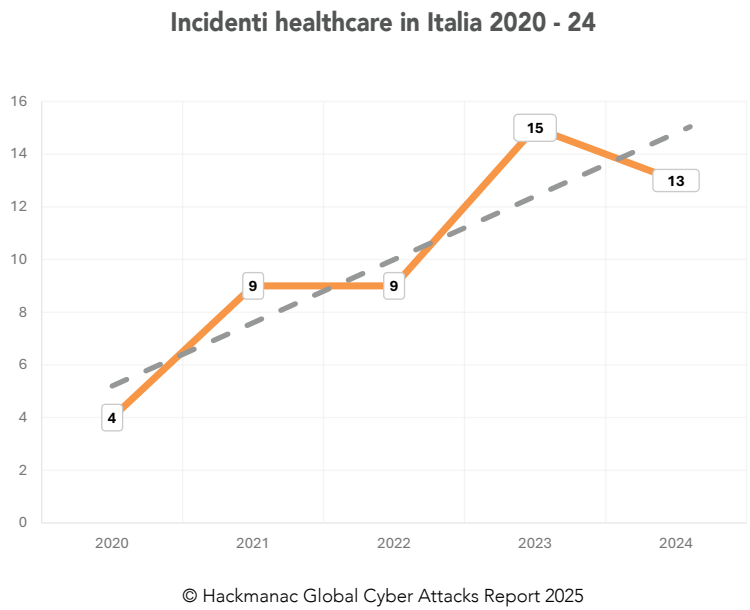


Fig. 8 - Andamento dei cyber incidenti verso il settore sanitario in Italia nel periodo 2020 - 2024

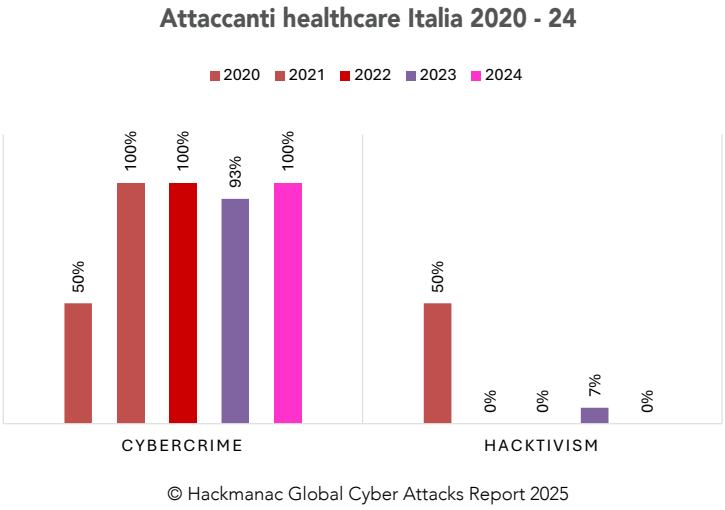


Fig. 9 - Distribuzione degli attaccanti verso il settore sanitario in Italia nel periodo 2020 - 24

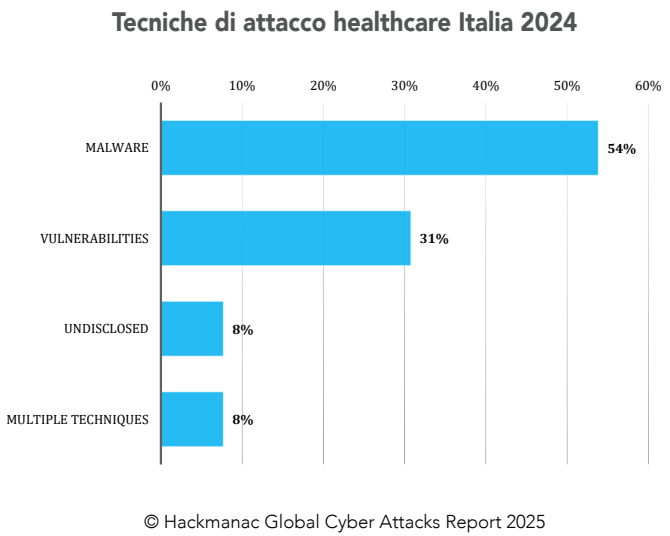


Fig. 10 - Tecniche di attacco verso il settore sanitario in Italia nel 2024

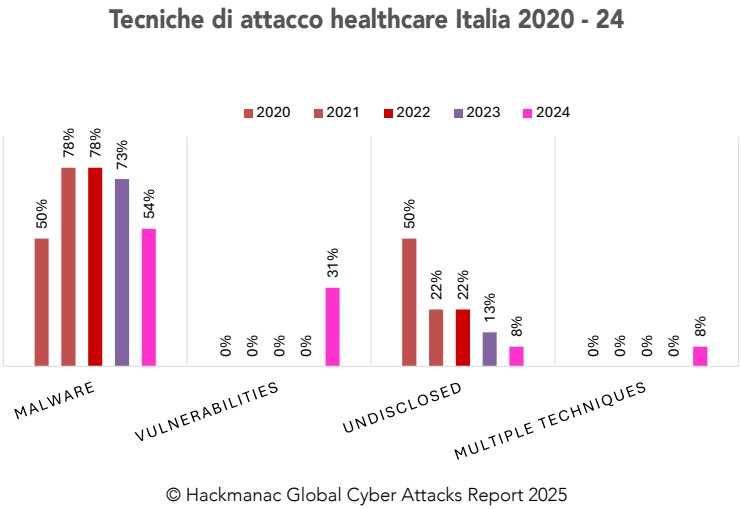
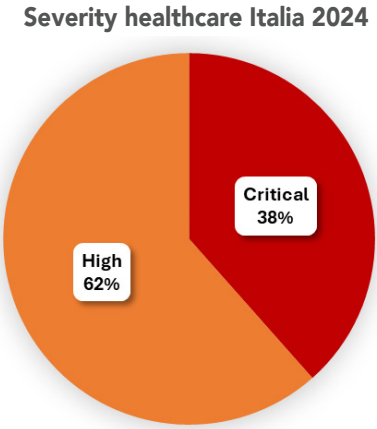


Fig. 11 - Distribuzione delle tecniche di attacco verso il settore sanitario in Italia nel periodo 2020 - 2024

Aumenta per la prima volta anche il ricorso alle "tecniche multiple" (8% degli incidenti), di solito utilizzate in operazioni malevole particolarmente complesse e pericolose.

In discesa invece le tecniche non classificate (-5 punti percentuali), indice del fatto che la precisione dell'informazione sugli incidenti che colpiscono il settore in Italia sta migliorando.

La severity degli incidenti resta il fattore più preoccupante: nel 2024, infatti, il 100% degli incidenti subiti dal settore sanitario nazionale ha avuto impatti gravi (62%) o gravissimi (38%), mentre l'anno precedente la stessa quota si attestava sul 93%.



© Hackmanac Global Cyber Attacks Report 2025

Fig. 12 - Severity degli incidenti verso il settore sanitario in Italia nel 2024

Spariscono invece del tutto gli impatti medi, che in passato avevano fatto registrare qualche eccezione (7% degli incidenti nel 2023) (**Fig. 13**).

È evidente che l'healthcare italiana viene colpita dal cybercrime in maniera consistente e con una gravità crescente, un dato di particolare rilevanza considerando l'importanza primaria del servizio.

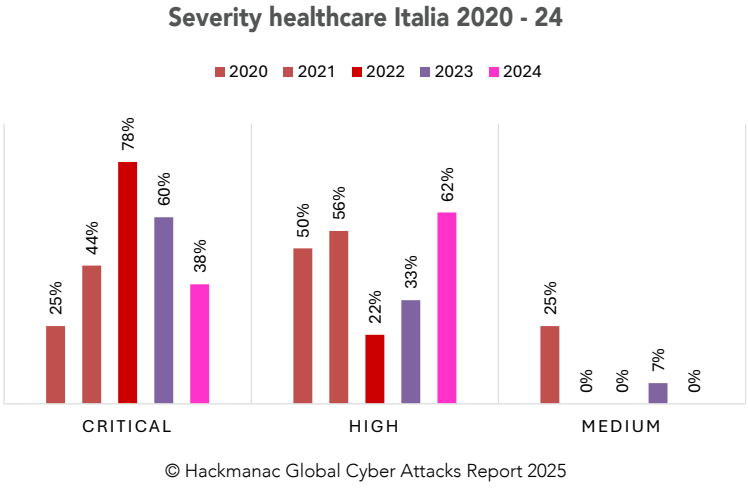


Fig. 13 - Distribuzione della severity degli incidenti verso il settore sanitario in Italia nel periodo 2020 - 24

I principali incidenti italiani

"A seguito dell'accidentale e imprevedibile evento informatico - reso noto già nei giorni scorsi - è possibile una violazione di dati personali di utenti, dipendenti e, più in generale, delle persone delle quali l'Azienda Sanitaria Locale di Potenza tratta dati personali". Recita così, a inizio 2024, uno dei primi comunicati ufficiali[9] di attacco cyber alla sanità italiana, ovvero all'**Azienda Sanitaria Locale di Potenza** che, insieme ad altri ospedali e alla stessa Regione, è vittima di un importante incidente legato alla supply chain. "La violazione - si spiega nel comunicato - è avvenuta tramite intrusione illecita in un computer di differente Azienda Sanitaria Regionale e si è diffusa verso altri Enti del SSR, le cui reti informatiche sono necessariamente comunicanti per la gestione di alcuni applicativi. Al momento non possono essere definiti con precisione i dettagli di quanto accaduto in termini di tipo di violazione o numero di persone interessate: tra le evenienze possibili si indicano la copia, l'alterazione o la cancellazione di dati, che gli uffici competenti stanno verificando e accertando. Allo stato, pertanto, non può precisarsi la tipologia di dati personali coinvolti, che potrebbero essere 'amministrativi' (es. nominativi, indirizzi…) o anche 'particolari' (dati sanitari)".

[9] https://www.aspbasilicata.it/2024/02/01/comunicazione-di-violazione-dei-dati-personali-ai-sensi-dellart-34-del-regolamento-ue-2016-679/

L'attacco alla sanità lucana, avvenuto nella notte del 28 gennaio, colpisce diversi ospedali e strutture sanitarie, tra cui l'**Azienda Ospedaliera Regionale "San Carlo" di Potenza, l'Azienda Sanitaria di Potenza, l'IRCCS CROB e l'Azienda sanitaria di Matera**. Oltre a **Regione Basilicata** che, qualche giorno dopo, informa gli utenti con altro comunicato in cui si specificano meglio i tipi di dati potenzialmente sottratti e si parla della loro pubblicazione nel dark web[10]. A rivendicare l'azione - che blocca diversi servizi sanitari per l'impossibilità ad accedere a Internet e alla posta aziendale da parte delle strutture - la cybergang Rhysida, già responsabile in passato degli attacchi al Comune di Ferrara, all'Azienda Ospedaliera Universitaria Integrata di Verona e all'Università di Salento. In questo - come in altri casi di attacchi italiani - a intervenire al fine di ripristinare i servizi in tempi rapidi anche l'Agenzia per la Cybersicurezza Nazionale che, in una nota, informa del fatto che *"il proprio pool operativo (CSIRT Italia), che ha seguito l'evento fin dai primi istanti, è attualmente sul posto per dare supporto alle operazioni di ripristino dei servizi*".

Ancora prima della Basilicata a essere vittima di un attacco hacker, il 18 gennaio, è **Croce Rossa Italiana** che comunica[11] - a giugno del 2024 - la "*pubblicazione illecita di circa 29 gigabyte dei dati di cui al suddetto attacco, resi altresì scaricabili nel web attraverso un link presente su un sito di file-hosting neozelandese"*. Oltre a esprimere rammarico per *"la diffusione impropria dei dati"*, Croce Rossa afferma che "*i documenti di cui i responsabili dell'attacco hanno preso visione attraverso la violazione delle misure di sicurezza informatiche potrebbero aver consentito l'accesso a dati personali trattati dall'Associazione nello svolgimento delle proprie attività istituzionali; inoltre, dalle dettagliate verifiche ancora in corso, i dati diffusi attraverso il suddetto link, oggi non più disponibile all'utenza, sembrerebbero essere riconducibili per la maggior parte alle informazioni raccolte dall'Associazione nell'ambito del proprio operato umanitario"*.

Il 4 maggio a essere sotto attacco è il fornitore di servizi di diagnostica sanitaria **Synlab Italia** che deve interrompere l'erogazione dei propri servizi. Il fatto, attribuito in un momento iniziale a "generici problemi tecnici", si rivela un attacco di tipo ransomware del gruppo criminale Blackbasta, rilevato dalla piattaforma Ransomfeed.it.

A giugno 2024 è la volta dell'**ASST Rhodense**[12] con i suoi ospedali di **ospedali di Garbagnate, Bollate e Rho**. In questo caso interventi chirurgici sospesi, servizi

[10] https://www.aspbasilicata.it/2024/02/01/comunicazione-di-violazione-dei-dati-personali-ai-sensi-dellart-34-del-regolamento-ue-2016-679/

[11] https://cri.it/2024/06/17/aggiornamento-attacco-hacker-2024/

[12] https://www.cybersecurity360.it/nuove-minacce/attacco-a-ospedali-milanesi-chirurgie-e-servizi-bloccati-e-mistero-sulle-cause/

sanitari in tilt e, dopo qualche giorno, la rivendicazione da parte del gruppo ransomware Cicada3301, che ha annunciato la pubblicazione di oltre 1 Tb di dati di pazienti - inclusi documenti medici, prescrizioni, e informazioni di identificazione personale - nel dark web. Ci sono voluti oltre 15 giorni e il lavoro di un team di esperti per riprendere le attività di prenotazione presso le strutture sanitarie e la riattivazione dei punti prelievo ospedalieri di Bollate, Garbagnate, Passirana e Rho.

A novembre 2024 è il Cup della regione Marche[13] a essere inutilizzabile. A dare la notizia Regione Marche che in un primo momento esclude problemi di sicurezza in una nota in cui vengono riferite "anomalie di funzionamento agli apparati di rete del datacenter regionale con conseguenti interruzioni della connettività degli applicativi regionali. È stata esclusa la possibilità di attacco hacker, in quanto le piattaforme sono regolarmente funzionanti anche se non raggiungibili".

Tra gli ultimi attacchi del 2024 quello che ha colpito l'**Avis Intercomunale Arnaldo Colombo**, con la pubblicazione online di circa 420.000 record contenenti informazioni personali, tra cui nome, codice fiscale, indirizzo e gruppo sanguigno. L'esfiltrazione di dati, a opera del collettivo ransomware **Argonauts,** è stata anche riportata nel bollettino si sintesi delle campagne malevole curato da Cert-AgID[14].

In sintesi, come evidenziato dal report "La minaccia cibernetica al settore sanitario - Analisi e raccomandazioni - gennaio 22-dicembre 24"[15], pubblicato dall'Agenzia per la Cybersicurezza Nazionale, tra le conseguenze più significative ci sono i blocchi dei servizi digitali sanitari, con impatti sulla gestione degli ospedali e quindi dei pazienti, l'esfiltrazione e, in alcuni casi, la vendita del dati sensibili oltre ai danni reputazionali, la perdita di integrità delle informazioni a seguito di modifiche di dati e conseguente impossibilità per gli operatori sanitari di utilizzare alcuni macchinari, la cancellazione di file e gli inevitabili costi di ripristino che aziende sanitarie e Regioni hanno dovuto sostenere a fronte degli attacchi subiti.

Tra le ragioni individuate dallo stesso report ACN dell'aumento degli incidenti informatici al settore health care ci sono:

1. **gestione decentralizzata dei sistemi IT**, con reparti che adottano soluzioni differenti senza una politica di sicurezza comune;

---

[13] https://www.anconatoday.it/cronaca/problemi-a-data-center-il-cup-va-ko-escluso-attacco-hacker.html

[14] https://cert-agid.gov.it/news/sintesi-riepilogativa-delle-campagne-malevole-nella-settimana-del-7-13-dicembre/

[15] https://www.acn.gov.it/portale/documents/20119/551838/acn_la+minaccia+cyber+al+settore+sanitario_clear.pdf/0f72c9c8-58e0-fcb0-7367-0999dced74e8?t=1735893649917

2. **obsolescenza delle tecnologie**, con dispositivi medicali non aggiornabili che rimangono vulnerabili;
3. **carenza di personale specializzato**, con la sicurezza informatica spesso affidata a personale IT non dedicato.

Soluzioni semplici non sono possibili, ma una riflessione circa la necessità di affrontare in modo strategico e urgente il tema Cybersicurezza è sicuramente necessaria, in particolare per la sanità pubblica.

Verso una Cybersicurezza rafforzata: NIS2 e AI nella Sanità per sicurezza, compliance e sostenibilità

La direttiva NIS2 segna un punto di svolta fondamentale per la sicurezza informatica delle infrastrutture critiche, tra cui il settore sanitario. Con l'aumento delle minacce cyber, le strutture sanitarie devono adottare misure rafforzate per la gestione del rischio, la continuità operativa e la resilienza dei sistemi IT. I requisiti posti dalla norma evidenziano la necessità di un approccio proattivo alla cybersecurity, che includa valutazioni continue delle vulnerabilità, il rafforzamento delle capacità di threat intelligence e una maggiore cooperazione tra attori pubblici e privati nella condivisione di informazioni per arrivare a una maggiore "situational awareness" e capacità di risposta agli incidenti. In questo contesto, il rispetto di standard come la ISO/IEC 27001 diventa cruciale per garantire una gestione efficace della sicurezza delle informazioni e dare evidenza della conformità alla norma. Infatti, la Direttiva NIS2 è fortemente allineata allo standard ISO/IEC 27001, tanto che un adeguamento NIS2 può rappresentare buona parte del percorso di certificazione. In diversi paesi europei (non l'Italia) è richiesto un audit annuale di una terza parte per dare evidenza dello stato di conformità. La diffusione di certificazioni ISO/IEC 27001 potrebbe diventare un vantaggio competitivo nella supply chain.

L'Intelligenza Artificiale (AI) può supportare le organizzazioni sanitarie nel raggiungimento degli obiettivi di sicurezza imposti dalla NIS2. Gli strumenti di AI avanzata, applicati alla threat intelligence, consentono di identificare e neutralizzare minacce in tempo reale, riducendo i tempi di risposta agli attacchi e migliorando la capacità di prevenzione. Tuttavia, il crescente utilizzo dell'AI introduce anche nuove sfide, tra cui la necessità di garantire la trasparenza e l'affidabilità degli algoritmi, evitando decisioni errate o discriminazioni nei sistemi automatizzati di cybersecurity. L'AI Act dell'Unione Europea interviene proprio su questi aspetti, imponendo requisiti rigorosi sulla governance dei modelli AI, sulla loro spiegabilità e sulla gestione del rischio, per evitare impatti negativi di natura sistemica.

Un aspetto cruciale è lo sviluppo sicuro delle soluzioni AI nel settore sanitario. Adottare un approccio basato sull'AI Life Cycle permette di integrare misure di sicurezza fin dalle prime fasi di progettazione, garantendo la conformità normativa e riducendo i rischi di esposizione a minacce informatiche. Il Secure Software Development Life Cycle (SSDLC) rappresenta una metodologia essenziale per sviluppare applicazioni AI sicure, minimizzando vulnerabilità e potenziali exploit.
Allo stesso tempo, la sostenibilità delle infrastrutture IT diventa un fattore sempre più rilevante: pratiche di green coding AI, orientate alla riduzione del consumo energetico dei data center, non solo aiutano a mitigare l'impatto ambientale, ma contribuiscono anche alla sicurezza, riducendo il rischio di inefficienze o errori derivanti da un carico eccessivo di lavoro sui sistemi. Un approccio che concilia performance con sostenibilità è quindi fondamentale.

Inoltre, l'importanza dei test del software diventa ancora più evidente. Test rigorosi e continui permettono di identificare vulnerabilità e anomalie in fase di sviluppo, evitando che potenziali exploit compromettano la sicurezza delle applicazioni AI in produzione. Solo con un'accurata fase di testing, che comprenda test di sicurezza e validazione dei modelli, è possibile garantire che i sistemi siano davvero resilienti e pronti a fronteggiare minacce in continua evoluzione.

Recentemente, i casi di vulnerabilità in sistemi AI avanzati, come DeepSeek, hanno evidenziato i rischi connessi all'uso di tecnologie AI non adeguatamente controllate. Le falle di sicurezza scoperte in questi sistemi dimostrano quanto sia fondamentale integrare controlli rigorosi e strategie di mitigazione per evitare che l'AI diventi essa stessa un vettore di attacco. Inoltre, il rischio di model collapse, in cui il modello AI smette di funzionare come previsto, è una minaccia concreta che può derivare da training non adeguati o da dati compromessi, accentuando la necessità di monitoraggio continuo. L'adozione di framework di AI security, insieme a una governance chiara e a processi di valutazione del rischio continui, è essenziale per garantire che l'AI sia uno strumento di protezione e non una minaccia aggiuntiva.

In un panorama normativo e tecnologico in rapida evoluzione, le strutture sanitarie devono adottare un approccio integrato alla sicurezza IT, coniugando le richieste della NIS2 con le esigenze di conformità all'AI Act e agli standard internazionali come la ISO/IEC 27001. L'implementazione di sistemi di gestione multicompliance e di strumenti di compliance automation può facilitare questo percorso, riducendo i costi operativi e rafforzando la sicurezza dell'intero ecosistema digitale sanitario. Investire in cybersecurity, sviluppo AI responsabile, sostenibilità e test approfonditi non è solo una necessità normativa, ma un'opportunità per costruire un futuro digitale più sicuro, efficiente e resiliente per la sanità.

Tuttavia, è fondamentale affrontare le sfide associate all'uso responsabile e sostenibile di queste tecnologie. Da un lato, l'AI può ottimizzare i processi clinici e amministrativi, migliorando la capacità di diagnosi, riducendo i consumi energetici e migliorando la gestione delle risorse. Dall'altro, l'implementazione di modelli AI comporta un elevato consumo energetico, con conseguenti impatti ambientali significativi. Inoltre, l'uso di algoritmi complessi solleva interrogativi etici riguardo alla trasparenza e alla gestione dei dati sensibili.

In parallelo, la direttiva NIS2 introduce nuove normative per la sicurezza informatica, imponendo requisiti più stringenti in termini di resilienza IT, gestione del rischio e conformità. Se da un lato questo può rappresentare una sfida per le aziende in termini di compliance e investimenti tecnologici, dall'altro rafforza l'idea che una cybersecurity efficace sia un pilastro della sostenibilità digitale: una maggiore sicurezza previene impatti economici, ambientali e reputazionali dovuti a cyberattacchi e perdite di dati.

Integrare AI e criteri di sicurezza in modo responsabile significa adottare modelli energeticamente efficienti, garantire una governance etica dei dati e sviluppare infrastrutture IT resilienti. La sostenibilità nell'uso delle nuove tecnologie non è solo una questione ambientale, ma anche una strategia per costruire un futuro digitale sicuro, innovativo e in linea con gli obiettivi ESG nel settore sanitario.

I rischi legati alla supply chain in sanità

Secondo questo rapporto l'Healthcare è il terzo settore più colpito al mondo da incidenti informatici e Gartner prevede che, nel 2025, il 45% delle organizzazioni a livello mondiale subirà attacchi attraverso le vulnerabilità del software dei loro fornitori, un valore triplicato rispetto al 2021.
Nel 2023, le aziende sanitarie hanno registrato costi medi di un data breach pari a 10,93 milioni di dollari (2023 IBM Security Cost of a Data Breach Report), con criticità legate alla supply chain tra le principali responsabili. Secondo il Ponemon-Sullivan Report 2024, il 60% delle organizzazioni sanitarie sono altamente vulnerabili a causa degli attacchi alla supply chain. Il 60% degli intervistati nel report riferisce di aver subito in media 4 attacchi all'anno provenienti dalla supply chain negli ultimi due anni.

Come si vede lo scenario è abbastanza preoccupante e i motivi per cui la sanità è così esposta sono diversi: soprattutto in Italia, da un lato c'è una generale obsolescenza di hardware e software, che non vengono rinnovati o aggiornati con regolarità; dall'altro di dati sanitari sono particolarmente appetibili per gli hacker perché nel dark web ogni record di dati di un paziente vale più dei dati di una carta credito.

Inoltre, gli hacker hanno capito che se riescono a colpire un piccolo fornitore che sia l'unico in una determinata regione, possono causare un impatto significativo sul settore sanitario nel suo complesso e massimizzare i loro guadagni.
Nel 2024 ci sono stati alcuni attacchi alla supply chain che hanno avuto particolare risonanza:

- a febbraio 2024 Change Healthcare è stata attaccata da un ransomware e sono stati rubati i dati personali e medici di oltre 100 milioni di persone, causando una grave interruzione al sistema sanitario americano;
- nell'aprile 2024, il gruppo ransomware BlackSuit ha preso di mira Octapharma, un fornitore di plasma, provocando la chiusura di oltre 190 centri di donazione del plasma negli Stati Uniti e interruzioni nell'Unione Europea;
- nel giugno 2024, la gang ransomware QiLin ha attaccato il fornitore di analisi e diagnosi Synnovis, costringendo diversi ospedali di Londra a riprogrammare interventi chirurgici e annullare migliaia di appuntamenti nelle settimane successive all'attacc;
- nel luglio 2024, il fornitore di sangue OneBlood, con sede in Florida, ha subito un attacco ransomware che ha causato un'interruzione del software, rendendo impossibile avere la disponibilità di magazzino e costringendo gli ospedali ad attivare protocolli di emergenza per la carenza di sangue.

Le interruzioni dei servizi o fisiche della supply chain, causate da questi attacchi, evidenziano il potenziale effetto a cascata sull'assistenza ai pazienti.
Le aziende sanitarie si appoggiano molto spesso a servizi esterni, molti dei quali non dispongono di adeguate misure di sicurezza per la protezione dei sistemi e dei dati sensibili. Inoltre, lo scenario degli attacchi informatici, in continua evoluzione, impone aggiornamenti e frequenti delle pratiche di sicurezza, che richiedono tempo e risorse, spesso insufficienti e della cui necessità non si ha piena consapevolezza.

I fornitori fanno parte a pieno titolo della "superficie di attacco" di una organizzazione e spesso il livello loro di sicurezza è insufficiente e più basso di quello dell'organizzazione sanitaria "committente"; perciò, diventano la via preferita dagli hacker per violare i sistemi e entrare nell'organizzazione sanitaria attraverso le loro vulnerabilità. Spesso ai fornitori viene concesso dal committente l'accesso ai sistemi e, se le credenziali non sono adeguatamente protette, diventa facile introdursi nel sistema sanitario attraverso le credenziali del fornitore.
I rischi per le organizzazioni sanitarie sono, quindi, molto alti perché, a seconda del sistema o dei dispositivi attaccati, può essere a rischio la salute dei pazienti.
Questo scenario potrebbe risultare attenuato dall'adozione della NIS2 che include la sanità nelle misure da adottare e impone controlli sui livelli di sicurezza dei fornitori.

Mitigare gli attacchi alla supply chain richiede che le organizzazioni sanitarie stabiliscano precise regole ai loro fornitori, ben costruite e orientate alla sicurezza, a partire dalla fase contrattuale.

Per comunicare le regole ai fornitori è indispensabile che le stesse organizzazioni sanitarie le costruiscano in maniera coerente con i principi della cybersecurity, preparando piani di sicurezza accurati, che prevedano vari scenari e coinvolgano i loro fornitori.
Per ridurre il rischio della supply chain è opportuno adottare alcune delle contromisure che fanno parte (o dovrebbero far parte) dei piani di sicurezza "standard" delle aziende:

- operare in modo che sia garantita la continuità operativa durante un attacco, individuando i punti critici che potrebbero generare impatti a cascata;
- includere la sicurezza dei fornitori terzi nelle analisi del rischio aziendale e nelle esercitazioni pratiche;
- avere fornitori alternativi, in modo da non dipendere da una sola fonte per forniture salvavita in caso di attacco informatico contro un fornitore critico;
- monitorare adeguatamente la sicurezza dei fornitori tramite attraverso audit periodici e controllare la eventuale catena dei subappalti;
- attivare forme di monitoraggio proattive, per esempio basate su AI o utilizzare la Threat Intelligence per identificare e prevenire attacchi noti.

La gestione degli accessi e delle identità è un punto critico nella catena dei fornitori. Sarebbe necessario stabilire:

- autenticazione a più fattori (MFA), obbligatoria per l'accesso ai sistemi critici;
- implementare politiche di accesso basate sul principio del minimo privilegio;
- garantire la disattivazione rapida degli account di dipendenti o fornitori che lasciano l'organizzazione;
- approccio Zero Trust nei confronti di qualunque partner o soggetto esterno, eliminando la fiducia implicita.

Infine, bisogna lavorare molto sulla formazione del personale per ridurre il rischio derivante da un errore umano, come per esempio non riconoscere una e-mail di phishing (il modo più classico ma ancora molto efficace per rubare le credenziali) o come comportarsi e reagire in caso di attacco.

La consapevolezza del costo che un attacco ha sull'organizzazione, oltre che in relazione a un eventuale riscatto per lo sblocco dei sistemi o la restituzione di dati, anche per il ripristino del funzionamento, aiuterebbe i singoli utenti a considerare con il giusto peso le azioni da compiere per salvaguardare l'integrità dei sistemi e dei dati.

Cybersecurity nelle mPMI: un quadro aggiornato dall'analisi dei dati del PID Cyber Check delle Camere di Commercio

(A cura di Georgia Cesarone, Paola Girdinio, Giovanni Manigrasso e Alessio Misuri)

Tra fine 2022 e inizio 2023, DINTEC - Consorzio per l'innovazione tecnologica - società in house di Unioncamere, dell'ENEA e delle Camere di commercio italiane, partendo da un modello predisposto dall'istituto di informatica e telematica (IIT) del CNR, assieme al Centro di Competenza START 4.0, ha sviluppato un modello di cyber assessment dedicato alle mPMI chiamato PID Cyber Check.

Il PID Cyber Check è uno strumento dei PID – Punti Impresa Digitale- le strutture delle Camere di commercio finalizzate a favorire i processi di digitalizzazione delle imprese italiane. Il servizio si avvale di un questionario che può essere svolto online autonomamente dalle imprese e che guida le mPMI in un'analisi sistematica della loro esposizione e vulnerabilità alle minacce cyber. La struttura si sviluppa in sezioni che raccolgono informazioni fondamentali sull'azienda, sulla rete IT, sui dati gestiti, sui processi aziendali e sulle misure di protezione già implementate.

Attraverso domande che spaziano dalla presenza di politiche di sicurezza formali alla gestione di dispositivi mobili e sistemi IT critici, lo strumento permette di mappare con precisione i punti di forza e le aree di rischio, riportando una prima indicazione di alto livello sulla postura cyber aziendale. Vengono analizzati aspetti tecnici, come la crittografia e l'aggiornamento dei sistemi, ma anche le risorse umane con la formazione del personale e la consapevolezza sulle minacce, per fornire una analisi sui tre pilastri di tecnologie, processi e persone. Le domande finali si focalizzano sugli attacchi subiti e sulle procedure di risposta, offrendo un primo quadro della resilienza cyber dell'organizzazione.

L'obiettivo ultimo è di consentire alle mPMI di diventare più consapevoli nell'adottare misure mirate per rafforzare la sicurezza informatica, prevenire attacchi e garantire la continuità operativa. Questo approccio pratico e modulare lo rende un primo strumento essenziale per valutare e cominciare a pianificare interventi in ambito cyber.

La **prima sezione** raccoglie informazioni generali sull'organizzazione, come il settore di appartenenza, il numero di dipendenti e il fatturato, dati che sappiamo fondamentali per contestualizzare il livello di rischio informatico in base alle dimensioni e alla tipologia di attività dell'azienda.

La **seconda sezione** esplora le caratteristiche della rete IT aziendale, chiedendo di descrivere il numero e la tipologia di dispositivi connessi (computer, server, dispositivi mobili, stampanti, ecc.), la presenza e l'uso di servizi cloud nonché il livello di complessità dell'infrastruttura IT. Queste domande servono a valutare l'ampiezza del perimetro tecnologico e i potenziali punti d'accesso alle minacce.

Una **terza sezione** si concentra sulle risorse dati gestite dall'azienda, come informazioni personali identificabili (PII), dati finanziari, know-how, audit e log e dati operativi. La finalità è individuare quali tipi di dati critici siano archiviati, comprendendo così il livello di sensibilità delle informazioni che potrebbero essere esposte a rischi e minacce.

Il questionario esamina poi l'importanza dell'IT nei processi aziendali, chiedendo quale sia l'impatto di un'interruzione IT sulle operazioni quotidiane. Le risposte variano da "nessun impatto rilevante" fino a "l'azienda sarebbe completamente paralizzata". Viene indagata anche l'importanza del sito web aziendale, distinguendo tra siti informativi, siti che gestiscono dati sensibili e quelli che risultano cruciali per il business.

La sezione relativa alla protezione informatica e al management è dedicata alle politiche di sicurezza formali, chiedendo se esistano regole definite per la gestione della rete, dei dispositivi mobili e della sicurezza IT in generale. Si indaga inoltre se l'azienda disponga di figure dedicate alla sicurezza informatica, come responsabili interni o organizzazioni esterne.

Un'area fondamentale analizza il livello di consapevolezza dei dipendenti in materia di cybersecurity, verificando se siano o siano stati previsti momenti di formazione specifici, corsi organizzati da aziende esterne o semplici linee guida firmate dal personale. È qui che emerge il ruolo chiave delle risorse umane come prima linea di difesa contro le minacce.

La parte tecnica include domande sul controllo degli accessi, la gestione delle password e l'utilizzo di meccanismi di protezione della rete, come firewall, sistemi di rilevamento delle intrusioni o segmentazione della rete. Vengono inoltre richieste informazioni sulla frequenza degli aggiornamenti software, sulla crittografia dei dati sensibili, sui backup regolari e sull'utilizzo di sistemi di logging.

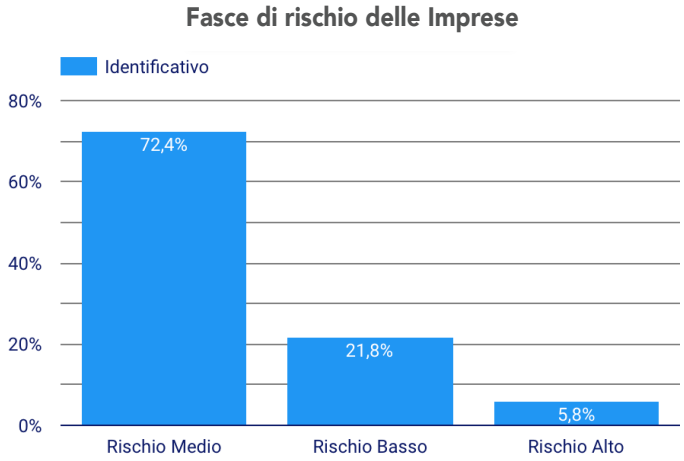
Infine, il questionario affronta il tema degli incidenti informatici avvenuti negli ultimi tre anni, distinguendo tra diverse tipologie di attacchi come malware, ransomware, phishing o comportamenti scorretti dei dipendenti. Si verifica anche se l'azienda dispone di procedure di risposta agli incidenti, includendo contatti con esperti di sicurezza informatica.

Attraverso queste domande, il PID Cyber Check non si limita a fornire un quadro delle vulnerabilità esistenti, ma permette di identificare le prime aree di intervento e di costruire un piano di indicazioni di alto livello ma mirato sui bisogni aziendali. Questo strumento è particolarmente adatto per le mPMI, che spesso hanno risorse limitate, offrendo un approccio sistematico per rafforzare la loro resilienza contro le minacce cyber, grazie alle sua gratuità, semplicità e ripetibilità.

Addentriamoci nell'analisi dei dati forniti raccolti grazie al PID Cyber Check nell'ultimo anno e mezzo (da giugno 2023 a dicembre 2024) che evidenziano i livelli di rischio, i settori più colpiti e la distribuzione degli attacchi in Italia:

Partecipazione al PID Cyber Check

Le 2.487 PMI che hanno compilato il test rappresentano un campione significativo del panorama italiano, offrendo una visione ampia dello stato della sicurezza informatica tra le piccole e medie imprese. Con una media complessiva del rischio di 40 su 100 (dove con il 100 si indica il valore di rischio massimo), la maggior parte delle aziende si colloca in una fascia di rischio medio (72,4%), seguita da una quota minore in rischio basso (21,7%) e una frazione più contenuta in rischio alto (5,8%).



Questa distribuzione evidenzia una situazione preoccupante: mentre solo una piccola percentuale è in condizioni critiche, oltre il 70% delle aziende non ha un livello di sicurezza ottimale, risultando esposta a potenziali minacce e vulnerabilità. Questa situazione richiede interventi strategici per ridurre il rischio medio e migliorare la resilienza complessiva.

Frequenza e tipologia degli attacchi

Un dato rilevante è che il 37,8% delle PMI dichiara di aver subito attacchi informatici, confermando che oltre un terzo delle imprese è stato vittima di cybercriminali. La distribuzione degli attacchi evidenzia che:

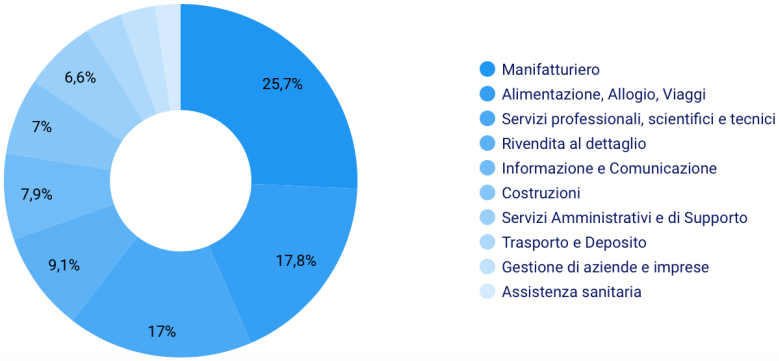
- Il phishing è la minaccia principale, rappresentando il 31% degli attacchi. Questo conferma che i dipendenti e gli utenti finali restano l'anello debole della catena di sicurezza, sfruttando tecniche di ingegneria sociale per sottrarre dati sensibili.
- Il malware segue con il 24%, indicando che software dannosi, come virus e trojan, continuano a essere una problematica rilevante.
- Gli attacchi alle web application (13%) sottolineano l'importanza di proteggere le piattaforme online, un problema critico per le aziende che utilizzano siti web e applicazioni per gestire il proprio business.
- Ransomware e comportamenti scorretti (entrambi al 10%) mettono in luce il crescente rischio legato a richieste di riscatto per dati criptati e alla mancanza di consapevolezza o formazione interna.

- Infine, l'11% rappresenta altre tipologie di attacco, a dimostrazione della varietà delle minacce cui le PMI sono esposte.

Quali sono i settori maggiormente colpiti?

I dati mostrano che i settori più colpiti dagli attacchi sono:

1. Manifatturiero
2. Alimentazione, Alloggio, Viaggi
3. Servizi professionali, scientifici e tecnici



Questi settori condividono caratteristiche specifiche che li rendono particolarmente vulnerabili agli attacchi informatici. Il manifatturiero, ad esempio, si basa spesso su infrastrutture tecnologiche obsolete e su dispositivi IoT industriali che rappresentano punti deboli facilmente sfruttabili dai cybercriminali.

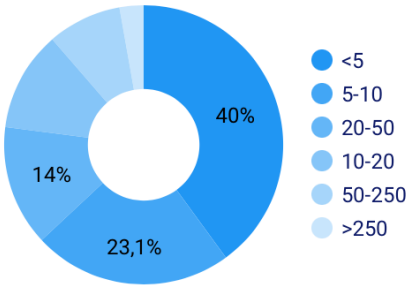
Il settore dell'alimentazione, dell'alloggio e dei viaggi, invece, si distinguono per la gestione di grandi volumi di dati sensibili appartenenti ai clienti, come informazioni personali e dettagli di pagamento, che lo rendono un bersaglio privilegiato per il furto di dati. Allo stesso modo, i servizi professionali e tecnici risultano esposti a causa della natura riservata dei dati gestiti, tra cui progetti, proprietà intellettuale e informazioni finanziarie, tutti elementi di grande valore per eventuali attacchi.

Distribuzione per dimensione aziendale e fatturato

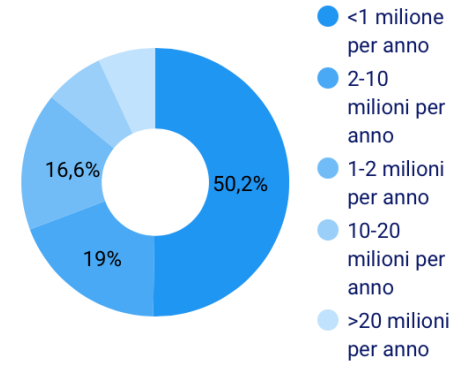
Le microimprese risultano essere le più vulnerabili, con il 40% delle imprese sotto i 5 dipendenti e il 23% tra 5 e 10 dipendenti colpite da attacchi. Questo può essere spiegato analizzando diversi fattori e incrociando le risposte a diverse domande del questionario:

- ***risorse limitate:*** le microimprese spesso non dispongono di budget adeguati da dedicare alla sicurezza informatica (alla domanda: "Esiste un responsabile che definisca e gestisca il budget per la sicurezza informatica" il 38% delle imprese risponde No);
- ***mancanza di competenze interne:*** in molte di queste aziende non esistono figure dedicate alla gestione della sicurezza (alla domanda: "La sua azienda ha una persona ufficialmente responsabile della sicurezza informatica" il 38% delle aziende risponde No);
- ***minore consapevolezza:*** la formazione in materia di cybersecurity è spesso trascurata (alla domanda: "Qual è il livello di consapevolezza da parte dei suoi dipendenti della sicurezza informatica nella sua azienda?" con scelta multipla che prevede vari tipi di gestione della formazione, il 55% risponde "Nessuna delle precedenti").

Distribuzione degli attacchi per n. di dipendenti



Distribuzione degli attacchi per fatturato



Questo si ripercuote su scelte fondamentali in materia di sicurezza; infatti:

- il 42% delle imprese dichiara che le password vengono scelte dai dipendenti senza ulteriore controllo sulla sicurezza della password stessa;
- sempre il 42% dichiara che i dipendenti possono connettere liberamente i propri dispositivi personali alla rete;
- praticamente nessuna delle quasi 2.500 mPMI partecipanti al questionario dispone di una certificazione e questo è uno dei dati più significativi (alla domanda: "L'organizzazione ha un certificato di sicurezza informatica?" il 91% risponde No).

A livello di fatturato, il 50% delle imprese sotto il milione di euro è stato colpito, insieme al 19% di quelle con fatturato tra 2 e 10 milioni di euro. Questo evidenzia che le realtà con limitate risorse economiche sono più esposte, mentre le imprese più grandi, pur essendo più strutturate, non sono immuni.

Distribuzione territoriale

Le risposte al PID Cyber Check sono ben distribuite sul territorio italiano, con una partecipazione equilibrata:

- Nord Italia: 37,6%
- Centro Italia: 36,4%
- Sud e isole: 26%

Questi dati mostrano un'ampia consapevolezza del problema a livello nazionale, ma anche una leggera disparità tra nord e sud. Questa differenza potrebbe riflettere la

diversa maturità digitale delle imprese nelle diverse aree con il nord che storicamente beneficia di un'adozione più avanzata delle tecnologie.

Dal punto di vista strettamente tecnologico, la maggioranza delle aziende dichiara di avere aggiornamenti automatici del software, di proteggersi con firewall e antivirus, backup regolari con copie sul cloud ed esegue regolarmente scansioni delle vulnerabilità. Il 49% però dichiara di non analizzare le informazioni di registrazioni e log.

Di fatto le aziende si sono dotate di sistemi che poi non vengono supportati da competenze e processi interni.

Conclusioni

I dati del PID Cyber Check rivelano un panorama in cui le mPMI italiane si trovano esposte a rischi informatici significativi, con un livello di rischio medio che domina e un'ampia percentuale di aziende che ha già subito attacchi.

Per affrontare il problema della maggiore esposizione delle imprese con fatturato inferiore a un milione di euro e per mitigare i rischi anche per quelle più strutturate, è necessario adottare una combinazione di strategie mirate che tengano conto delle risorse limitate delle micro e piccole imprese e delle esigenze più complesse delle aziende più grandi.

Una soluzione potrebbe includere iniziative come l'implementazione di servizi di cybersecurity accessibili e scalabili, progettati specificamente per le mPMI. Ad esempio, soluzioni di sicurezza "as-a-service", come firewall gestiti, software antivirus avanzati e strumenti di monitoraggio delle minacce, potrebbero essere offerti a costi contenuti tramite consorzi di settore o incentivi pubblici, come gli attuali fondi PNRR messi a disposizione dalla rete dei Centri di Competenza e degli EDIH.

In parallelo, è fondamentale **investire nella formazione del personale,** poiché molte minacce, come il phishing, si basano su errori umani. Workshop, moduli di e-learning e simulazioni pratiche potrebbero aiutare i dipendenti a riconoscere e prevenire attacchi, aumentando la resilienza anche in aziende con budget ridotti.

Per le medie imprese già più strutturate, la soluzione dovrebbe concentrarsi sul rafforzamento delle infrastrutture critiche come l'adozione di sistemi di autenticazione multifattoriale, la segmentazione delle reti e piani di backup avanzati. Inoltre, l'integrazione di sistemi di monitoraggio e risposta automatizzata agli incidenti permetterebbe loro di reagire rapidamente alle minacce in corso.

Concludiamo ricordando che, come nel caso del PID Cyber Check, la collaborazione tra pubblico e privato è sempre un punto centrale. Attraverso fondi governativi, incentivi fiscali e partnership con enti di formazione e fornitori di tecnologia, si riesce a facilitare l'accesso a strumenti di sicurezza avanzati anche ad aziende con risorse limitate, contribuendo a innalzare il livello generale di sicurezza nel Sistema Paese.

Il gruppo di lavoro ha da poco rilasciato la nuova versione del PID Cyber Check realizzato da DINTEC, CNR, START 4.0 e CYBER 4.0 a cui si affianca un nuovo modello di assessment chiamato PID Cyber Check Plus dedicato a una prima valutazione di alto livello della compliance alla nuova Direttiva NIS2.

Chi volesse approfondire, può trovarli al link: https://www.puntoimpresadigitale.camcom.it/paginainterna/assessment-checkup-sicurezza-it-imprese

Riferimenti START 4.0
Paola Girdinio, presidente Start 4.0
Georgia Cesarone, responsabile innovazione e formazione

Riferimenti DINTEC
Antonio Romeo, direttore Dintec
Alessio Misuri, responsabile unità Digitale e Innovazione
Giovanni Manigrasso, responsabile attività CyberSecurity e Artificial Intelligence
Marco Damiano, responsabile attività Certificazione Competenze

CyberFutures. Come sarà il nostro lavoro nel 2035?

(A cura di Alessandro Vallega e Guglielmo Duccoli)

L'iniziativa

La curiosità di sapere come evolverà la sicurezza, il rischio e la compliance negli anni a venire ha indotto la Clusit Community for Security a dedicare a questo tema un gruppo di lavoro apposito, il diciassettesimo dalla sua fondazione.

I temi affrontati in passato

Negli anni passati ci siamo occupati del tema della trasformazione digitale legata al successo delle tecnologie mobili, dei social network, del cloud, dell'IoT, dell'intelligenza artificiale, del GDPR e di altre questioni inerenti la sicurezza digitale.

Per ognuno di questi temi abbiamo elaborato gli aspetti sfidanti che le aziende si trovano ad affrontare e prodotto libri (scaricabili gratuitamente dal sito web della Community https://c4s.clusit.it/) per aiutare ad affrontarli. Le caratteristiche comuni sono:

- un approccio multidisciplinare con professionisti di vari settori, tra cui avvocati, consulenti, system integrator, vendor, ethical hacker, professori universitari, giornalisti e specialisti di sicurezza;
- una struttura organizzativa formale con team leader e microgruppi ridondanti;
- la partecipazione di oltre 80 persone e la produzione di almeno un centinaio di pagine in formato A4 per tema;
- decisioni collegiali e revisioni multiple degli output da parte di tutti i partecipanti.

Il messaggio per le PMI

Il messaggio per le PMI è stato un invito ad accogliere la digitalizzazione, necessaria per competere nel mercato globale, con cognizione dei rischi, della sicurezza e della

conformità a norme, leggi e regolamenti. Perché non innovare porta al fallimento, ma innovare senza attenzione può condurre al disastro.

La lettura delle nostre pubblicazioni ha aiutato numerose aziende ad affrontare con maggior serenità il futuro.

Dunque, abbiamo sempre cercato di creare consapevolezza su come fare bene le cose. In quest'ultimo lavoro, invece, ci siamo interrogati sul futuro.

Comprendere i possibili esiti della crescente digitalizzazione può permetterci di trarre vantaggi personali o aziendali, e addirittura, nei casi più eclatanti, potrebbe permetterci di agire a livello sociale e politico per influenzarne gli esiti.

Nei primi workshop intensivi abbiamo compreso che, pur non potendo prevedere il futuro, si possono comunque ipotizzare scenari a maggior o minor probabilità di accadimento. Alcuni possono risultare graditi o sgraditi, favorevoli o sfavorevoli per certe parti della società, può cambiare tutto (come nei film di fantascienza distopica) o poco (in una improbabile continuità con il passato). Prevedere il futuro non è mai stato facile. Il premio nobel Paul Krugman (2008) nel 1998 predisse (sbagliando clamorosamente) il rallentamento della crescita di Internet in un articolo intitolato proprio "Why most economists' predictions are wrong" [1]. È sempre più difficile prevedere il futuro per via dell'accelerazione della scienza e della tecnologia e per il fatto che le innovazioni si creano a partire da altre innovazioni in una spirale sempre più veloce.

L'Accelerazione esponenziale dell'evoluzione tecnica e scientifica

L'evoluzione tecnica e scientifica degli ultimi decenni ha subito una crescita esponenziale, superando di gran lunga il ritmo dei progressi conseguiti nelle epoche passate. Le grandi rivoluzioni della storia – agricola, industriale e digitale – hanno tutte contribuito a trasformare radicalmente la società, ma la velocità con le quali si sono realizzate è stata via via crescente: millenni, secoli, decenni. Non è escluso che se ne possa battezzare un'altra, ben più rapida delle precedenti: la rivoluzione dell'intelligenza artificiale (IA), che rappresenterebbe un punto di svolta unico.

L'IA sta rivoluzionando settori come la medicina, i trasporti e la finanza, permettendo analisi dei dati più profonde e decisioni rapide e precise. Il machine learning e il deep learning hanno aperto nuove frontiere nella comprensione e nell'elaborazione dei dati, conducendo a una vera esplosione di conoscenza e capacità tecnologiche. Non solo: le innovazioni nei campi della biotecnologia, dell'energia rinnovabile e della scienza dei materiali stanno creando un futuro in cui le possibilità sembrano illimitate.

[1] https://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html#?hn

L'evoluzione tecnica e scientifica procede a un ritmo così rapido che le soluzioni di ieri diventano rapidamente obsolete, sostituite da idee e strumenti sempre più avanzati. Questa accelerazione esponenziale non solo trasforma il presente, ma ridisegna continuamente le possibilità del futuro, rendendo ogni giorno una nuova opportunità di progresso e innovazione.

Guardando indietro, le persone meno giovani si ricorderanno che non avevamo i telefoni cellulari, che non c'era Internet e si usavano le enciclopedie cartacee. La programmazione si faceva sui mainframe. Non c'erano le app né la video conferenza, le segretarie (sì, c'erano le segretarie) lavoravano su macchine per scrivere, gli appuntamenti si prendevano al telefono, le circolari aziendali passavano di mano in mano accompagnate dal libro firme. Qualcuno ricorda le schede perforate e uno di noi ha scritto il suo primo programma in COBOL su carta, affinché venisse digitato da una signorina (erano tutte donne e tutte perforavano le schede velocissimamente)... Chi avrebbe detto, vent'anni fa, che tre grandi cloud provider avrebbero fatturato 60 miliardi di dollari al trimestre?[2]

Con il nostro lavoro più recente abbiamo voluto offrire un contributo all'individuazione del trend futuri: come il nostro lavoro potrà venir influenzato dalle svariate possibili evoluzioni della tecnologia e della società. Ci siamo concentrati su dieci temi principali, inoltre abbiamo condotto alcuni sondaggi per captare la percezione di quanto realistiche risultino tali prospettive e quale sia il loro livello di desiderabilità.

Contrasto ai deep fake

Questo gruppo di lavoro ha esplorato vari aspetti dei deep fake, tra cui la loro produzione e accessibilità per gli utenti generici, il legame con la diffusione delle fake news e i potenziali effetti su sicurezza informatica, opinione pubblica e società in generale. Inoltre, ha approfondito le sfide legate all'individuazione dei deep fake e al ruolo della tecnologia, nonché l'efficacia di norme e leggi nel contrastarne l'utilizzo malevolo.

L'incontro si è aperto con un video sorprendente: il presidente Sergio Mattarella in persona sembrava porgere i saluti istituzionali. Subito dopo è stato rivelato il trucco: si trattava di un deep fake, creato con una spesa minima (10 euro) e strumenti facilmente accessibili. L'esperimento, che ha colpito il pubblico, dimostra quanto sia semplice oggi manipolare contenuti digitali e creare falsi convincenti. Un watermark visibile e l'impronta hash del video hanno ribadito l'importanza di tecnologie per l'autenticazione dei contenuti.

[2] Microsoft Vs. AWS Vs. Google Cloud Earnings Q3 2024 Face-Off

Le potenzialità attuali dei deep fake

I progressi nel campo dei deep fake sono straordinari. Con una modesta potenza di calcolo è già possibile creare video credibili come quello di Mattarella. Con risorse più avanzate si raggiungono livelli di realismo impressionanti, come negli altri due casi mostrati: la ricostruzione digitale di Audrey Hepburn che canta una canzone di Ed Sheeran, e il face swap in tempo reale utilizzando tecnologie di punta come il Real-Time AI Face Animator di Microsoft.

Strumenti open source come DeepFakeLab su GitHub richiedono hardware potente, ma nulla che sia fuori portata per un utente con conoscenze tecniche. Questi esempi illustrano non solo le capacità tecniche, ma anche i rischi legati alla sempre più facile accessibilità di tali tecnologie.

Utilizzi odierni dei deep fake

I deep fake trovano applicazioni in diversi ambiti, sia leciti che illeciti. In politica, possono essere usati per diffondere disinformazione, come il caso del falso video in cui Zelensky invitava gli ucraini alla resa. Altri utilizzi includono truffe agli anziani, deep porn, e persino l'uso creativo per spot pubblicitari, come accaduto con Max Pezzali.

Un caso curioso arriva dalla Cina, dove i deep fake vengono impiegati per creare simulazioni di defunti, permettendo ai familiari di "interagire" con loro (una tecnologia anticipata in un noto episodio della serie Tv britannica "Black Mirror"). Nel mondo dello spettacolo, attori come Val Kilmer hanno recuperato la voce grazie a questi strumenti, e lo stesso è accaduto per pubblicità di noti marchi.

Proiezioni future: il 2035

Nel futuro, i deep fake saranno indistinguibili dai contenuti autentici. La tecnologia evolverà a tal punto che la verifica dell'autenticità richiederà strumenti avanzati. Probabilmente, si adotteranno sistemi di marcatura chiara dei contenuti generati da IA e norme legali più stringenti. Tuttavia, il divario tra creatori di deep fake e sistemi di riconoscimento potrebbe persistere, così come accade oggi nella cybersecurity.

La società dovrà adattarsi a questa nuova realtà. Le persone potrebbero limitare la condivisione di foto e video personali per evitare abusi. In ambito lavorativo, si ipotizza l'utilizzo di autenticazione biometrica continua durante call e videoconferenze, realizzata tramite dispositivi indossabili o chip sottopelle.

Avatar digitali e applicazioni positive

Nonostante i rischi, la tecnologia offre anche opportunità. Ipotizziamo che nel 2035 ognuno possa creare avatar digitali certificati, in grado di rappresentarci in riunioni

o compiere azioni quotidiane. Tali avatar potrebbero partecipare a manifestazioni, interagire con sistemi virtuali o persino rispondere al telefono per gestire chiamate indesiderate. In un contesto aziendale, però, emergono domande etiche: chi possiede i dati e le competenze del clone? Come prevenire abusi da parte dei datori di lavoro? Gli avatar potrebbero inoltre diventare bersagli di attacchi informatici o manipolazioni. Sarà cruciale sviluppare strumenti per monitorare le fonti di addestramento delle IA e garantire trasparenza sui dati utilizzati.

Conclusione

L'intervento si è concluso con una riflessione sulla convivenza con i deep fake. Se è impossibile eliminarli, è necessario adottare precauzioni per mitigarne i rischi e sfruttarne i vantaggi. Il futuro promette grandi cambiamenti, ma anche nuove sfide, in un mondo dove realtà e finzione si intrecciano sempre più strettamente.

Tutela dei diritti nell'utilizzo dell'IA

Il gruppo si è occupato della tutela dei diritti delle persone che è essenziale per promuovere la fiducia nei numerosi benefici dell'Intelligenza Artificiale, mentre il potenziale dell'IA di fornire un vantaggio competitivo per le imprese evidenzia la necessità di affrontare le problematiche legate alla cybersecurity e alla protezione dei dati.

Il progresso tecnologico e l'adozione sempre più ampia di soluzioni basate sull'IA stanno trasformando profondamente la nostra società, portando con sé opportunità straordinarie, ma anche significativi rischi per i diritti umani fondamentali. Questo gruppo di lavoro ha affrontato questioni cruciali, proponendo soluzioni e prospettive che possono guidarci verso un futuro più equo e trasparente. Il "Metodo dei tre orizzonti" ha offerto una cornice interpretativa per analizzare il presente, immaginare il futuro desiderabile e identificare le transizioni necessarie.

La situazione attuale e le criticità emergenti

Oggi, l'utilizzo dell'intelligenza artificiale (IA) è in rapida espansione, influenzando molteplici settori, tra cui la cybersecurity, la salute e la gestione delle informazioni. Tuttavia, tale sviluppo ha evidenziato diverse problematiche. La predominanza di poche grandi aziende nel mercato della generazione IA genera preoccupazioni legate al monopolio della conoscenza e alla mancanza di trasparenza degli algoritmi utilizzati. Gli impatti sui diritti fondamentali, come la privacy e la libertà di espressione, sono sempre più tangibili.

Ad esempio, i sistemi di intelligenza artificiale impiegati per le ricerche di informazioni stanno sostituendo i motori di ricerca tradizionali. Ciò potrebbe limitare il plurali-

smo informativo, consolidando un modello in cui poche piattaforme monopolizzano la produzione e la distribuzione della conoscenza, ancora di più rispetto al presente. Inoltre, l'assenza di regolamentazioni efficaci espone i cittadini a rischi crescenti, tra cui la manipolazione dei dati personali e la sorveglianza intrusiva.

Un futuro desiderabile

Il futuro preferibile immaginato dal gruppo di lavoro è caratterizzato da un ampio pluralismo nel mercato dell'IA, dove gli utenti possano scegliere liberamente tra diverse piattaforme e tecnologie. Questo scenario garantirebbe la trasparenza degli algoritmi, l'accesso alle fonti delle informazioni e il diritto di verificare i procedimenti alla base delle risposte dell'IA.

Un sistema ideale vedrebbe l'adozione di linee guida e framework internazionali per la gestione dell'IA atte a promuovere la responsabilità etica e l'innovazione sostenibile. La tutela della privacy sarebbe al centro dello sviluppo tecnologico, con strumenti che permettano agli utenti di mantenere il controllo sui propri dati personali.

Pockets of future in the present

Alcuni segnali positivi sono già visibili oggi. L'Unione Europea sta giocando un ruolo cruciale nella regolamentazione dell'IA:

- L'Articolo 13 dell'IA Act richiede che i sistemi di IA ad alto rischio siano progettati per garantire trasparenza e interpretabilità.
- L'Articolo 27 del DSA impone ai fornitori di piattaforme online di specificare i parametri utilizzati nei sistemi di raccomandazione e di offrire opzioni per modificarli.

Tali iniziative rappresentano passi fondamentali verso un futuro in cui l'IA divenga uno strumento di empowerment per gli individui, anziché una minaccia ai loro diritti.

Innovazioni e strategie per la transizione

Per realizzare questa visione, il gruppo di lavoro ha identificato alcune azioni chiave:

1. promuovere la pluralità delle IA: attraverso finanziamenti e incentivi, l'UE dovrebbe sostenere lo sviluppo di motori di IA da parte di Stati membri e imprese locali, riducendo la dipendenza da grandi aziende globali;
2. garantire trasparenza e accesso alle fonti: progetti che integrano pratiche etiche e trasparenti, come la tracciabilità delle decisioni algoritmiche, devono essere incoraggiati e valorizzati;
3. collaborare con partner strategici: centri di ricerca, università e start-up sono attori fondamentali per la creazione di tecnologie innovative.

Ad esempio, programmi di partnership pubblico-privato potrebbero accelerare l'adozione di soluzioni etiche;

4. educare gli utenti: la consapevolezza e la formazione sono strumenti indispensabili per consentire ai cittadini di interagire in modo critico e consapevole con le tecnologie emergenti.

Conclusione

La tutela dei diritti nell'utilizzo dell'IA richiede un approccio proattivo, che integri innovazione, regolamentazione e collaborazione. Solo attraverso uno sforzo congiunto tra istituzioni, aziende e società civile sarà possibile trasformare le sfide attuali in opportunità per un futuro più equo e sostenibile. Come suggerito dal Metodo dei tre orizzonti, il presente contiene già i semi di un futuro desiderabile: è nostro compito coltivarli con attenzione e responsabilità.

Per guidare questa transizione tecnologica, proponiamo tre pilastri fondamentali:

- **principio di esplicabilità:** dobbiamo superare il "black box problem" dell'IA, esigendo algoritmi interpretabili e decisioni tracciabili;
- **dialogo interdisciplinare:** è fondamentale creare sinergie tra giuristi, informatici, filosofi ed esperti di etica per sviluppare sistemi di IA allineati con i nostri valori socio-giuridici;
- **centralità del rapporto umano:** Come sottolineato da Luciano Floridi, dobbiamo aspirare a una "società aumentata", non "automatizzata". L'IA deve rimanere uno strumento di supporto, non un sostituto del giudizio umano.

L'obiettivo non è frenare l'innovazione, ma guidarla verso un futuro in cui l'IA amplifichi il potenziale umano senza compromettere i diritti fondamentali. Questa è la sfida che ci attende: una sfida che richiede vigilanza, collaborazione e, soprattutto, una visione chiara dei valori che vogliamo preservare nel mondo di domani.

La tecnologia plasma il nostro futuro, ma sta a noi assicurarci che questo futuro rimanga profondamente umano.

Tutela dei diritti nell'utilizzo di IoT e BIO IoT

L'argomento trattato è l'Internet of Things (IoT) applicato ai sistemi biologici, spesso indicato come Internet of Bodies (IoB). La discussione sullo stato attuale e sui rischi per i dati, ha esaminato l'efficacia delle normative e delle misure di controllo esistenti, ha esplorato l'evoluzione dell'IoT e dell'IoB e ha affrontato il tema di come guidare l'innovazione verso un futuro sicuro, salvaguardando i valori etici.

L'avvento dell'Internet of Things e la successiva evoluzione verso l'Internet of Bodies rappresentano una delle rivoluzioni tecnologiche più rilevanti degli ultimi decenni. Questi sistemi, caratterizzati dalla connessione di dispositivi capaci di raccogliere, elaborare e scambiare dati, stanno trasformando profondamente settori come la medicina, l'industria e il consumo. Tuttavia, tali innovazioni sollevano anche questioni critiche in termini di privacy, sicurezza e diritti individuali, specialmente quando i dispositivi IoB interagiscono direttamente con il corpo umano. L'IoT e l'IoB, se adeguatamente regolamentati, possono migliorare la qualità della vita e aumentare l'efficienza di molti settori. Ma, è fondamentale bilanciare queste opportunità con un'attenta considerazione dei potenziali rischi etici e sociali.

Definizioni e contesti di applicazione

L'IoT si riferisce a un ecosistema di dispositivi interconnessi che raccolgono dati ambientali o personali e li elaborano per migliorare servizi e applicazioni. L'IoB, come sottoinsieme dell'IoT, è costituito da dispositivi progettati per monitorare, migliorare o modificare le funzionalità del corpo umano. Esempi includono pacemaker intelligenti, interfacce cervello-computer e wearable per il monitoraggio della salute.
I principali contesti di applicazione dell'IoB spaziano dalla medicina (dispositivi per il monitoraggio di malattie croniche o interventi chirurgici assistiti) al consumo (smartwatch, abiti con sensori), fino all'ambito militare e industriale (esoscheletri, monitoraggio dei lavoratori in contesti pericolosi).

In ambito sanitario, i dispositivi IoB permettono diagnosi più rapide e terapie personalizzate. Nel settore industriale, migliorano la sicurezza sul lavoro grazie a sensori che monitorano costantemente le condizioni fisiche dei lavoratori. Per quanto riguarda il consumo, strumenti come i fitness tracker stanno trasformando il modo in cui le persone si prendono cura della propria salute.

Rischi associati

L'integrazione di IoT e IoB espone gli utenti a rischi considerevoli. Tra i principali si annoverano:

- **cybersecurity:** vulnerabilità nei dispositivi possono essere sfruttate per accedere a dati personali o per compromettere il funzionamento dei device stessi, con conseguenze fisiche e psicologiche per gli individui;
- **privacy:** i dati raccolti dai dispositivi IoB, spesso sensibili, possono essere utilizzati in modo improprio, violando la riservatezza degli utenti;
- **sicurezza fisica:** il malfunzionamento o la compromissione dei dispositivi medici potrebbe mettere a rischio la vita dei pazienti;

- **etica:** l'utilizzo di tali tecnologie pone interrogativi sull'autonomia individuale e sul controllo delle informazioni personali.

Un esempio pratico è rappresentato dai dispositivi medici connessi, che potrebbero essere vulnerabili a cyberattacchi, mettendo a repentaglio non solo la sicurezza dei dati ma anche la salute dei pazienti. Inoltre, la crescente raccolta di dati biometrici solleva dubbi sul loro utilizzo per finalità discriminatorie o commerciali.

Normative e misure di mitigazione

La regolamentazione gioca un ruolo cruciale per garantire l'uso sicuro e responsabile delle tecnologie IoT e IoB. In Europa, il GDPR rappresenta un punto di riferimento per la protezione dei dati personali, mentre normative come il Cybersecurity Act forniscono linee guida specifiche per la sicurezza informatica.

Tra le misure di mitigazione dei rischi figurano:

- **sicurezza by design:** dispositivi progettati con protocolli di sicurezza integrati;
- **crittografia avanzata:** per proteggere i dati durante la trasmissione e l'archiviazione;
- **audit indipendenti:** verifiche periodiche sulla sicurezza e conformità normativa;
- **sensibilizzazione degli utenti:** programmi di educazione per aumentare la consapevolezza sui rischi e sui diritti digitali.

In aggiunta, è fondamentale promuovere la collaborazione tra governi, aziende e organismi di regolamentazione per sviluppare standard globali che garantiscano l'interoperabilità e la sicurezza dei dispositivi IoT e IoB.

Scenari futuri

Con il continuo sviluppo di tecnologie avanzate, l'IoB si avvicina sempre più a una piena integrazione con il corpo umano. Applicazioni come le interfacce neurali promettono di rivoluzionare il trattamento delle malattie neurologiche e di migliorare la qualità della vita di chi ne è affetto, ma persino, in un orizzonte temporale non lontanissimo, di estendere funzioni cerebrali (come la memoria), sensoriali e motorie, di decodificare e trasmettere il pensiero a distanza, o di controllare i sistemi industriali col pensiero.

Questi scenari aprono a nuove declinazioni dei diritti fondamentali: si parla ormai sempre più spesso di "neurodiritti", "mental privacy", "cognitive liberty", "mental integrity", "psychological continuity". Osserviamo che, in questo senso, sono già state promulgate norme sullo sviluppo e utilizzo di neurotecnologie e sulla protezione dei dati neurali (ad esempio, negli Stati Uniti alcune normative privacy sono state estese a queste tipologie di dato personale).

Diviene quindi cruciale che tale progresso tecnologico si sviluppi grazie alla rigorosa applicazione di principi etici nel rispetto dei diritti e della dignità di tutti i soggetti coinvolti, tenendo in considerazione, in un futuro prossimo, la presenza di soggetti cosiddetti "ibridi", il cui cervello potrebbe essere il prodotto integrato di biologia e innesti elettronici connessi a una Intelligenza Artificiale.
In generale,la governance delle tecnologie IoT e IoB richiede un approccio globale e collaborativo tra governi, industrie e società civile. Solo così sarà possibile bilanciare l'innovazione tecnologica con la protezione dei valori fondamentali della società di oggi e di domani. Investimenti in ricerca e sviluppo, accompagnati da un robusto quadro normativo ma anche sostenuti da un profondo e responsabile impegno etico, possono garantire un futuro in cui tecnologia e diritti umani coesisteranno armoniosamente.

Sovranità EU sull'High Tech

Il gruppo di lavoro ha auspicato il colloquio con le agenzie nazionali di cybersecurity, la promozione di un sigillo di certificazione, il miglioramento dell'istruzione e della formazione, il sostegno alle aziende tecnologiche nazionali ed europee e la promozione di regolamenti internazionali armonizzati in materia di cyber.
Inoltre, l'importanza della certificazione della sicurezza informatica dell'UE e del CERT-EU, nonché l'adozione di soluzioni open-source per l'hardware e la creazione di standard di interoperabilità per i servizi cloud.

Il contesto e la posta in gioco

Nel contesto geopolitico attuale, la sovranità digitale rappresenta una delle sfide più critiche per l'Unione Europea. Il controllo dell'informazione, gestita principalmente attraverso hardware e software di origine americana e, in misura minore, cinese, è diventato un elemento fondamentale di potere politico ed economico. L'approccio europeo, incentrato sulla tutela dei diritti individuali piuttosto che sugli interessi commerciali, richiede una strategia articolata per proteggere i dati dei cittadini e delle istituzioni.

I domini della sovranità digitale e i rischi attuali

La sovranità digitale si articola in quattro domini principali: tecnologico, software, dati e controllo del cittadino sui propri dati. L'importanza di tali ambiti è evidenziata da episodi significativi, come le intercettazioni della cancelliera Merkel o il caso Cambridge Analytica: essi hanno dimostrato come il controllo dell'informazione possa influenzare processi democratici, dinamiche di mercato e comportamenti sociali su larga scala.

Lo stato dell'arte e le iniziative in corso

Lo scenario attuale presenta diverse criticità. L'Europa rischia di perdere il controllo non solo sull'informazione, ma anche sulle infrastrutture critiche e sull'evoluzione etica della tecnologia e dell'intelligenza artificiale. Il pericolo è che la tecnologia diventi principalmente un'esportazione di capitali anziché un investimento per il futuro del continente. Per contrastare questa tendenza, l'UE ha avviato diverse iniziative, tra cui investimenti nella produzione di chip, nello sviluppo dell'IA e del quantum computing, oltre a programmi per il controllo delle infrastrutture critiche e la cybersecurity.

Obiettivi strategici per il 2035

Per raggiungere una reale sovranità digitale entro il 2035, sono stati identificati obiettivi ambiziosi:

- il controllo sulle materie prime e sui processi produttivi;
- la gestione autonoma dell'informazione europea;
- il controllo sulla spiegabilità dei processi informativi e sulle infrastrutture critiche.

Particolare attenzione viene riservata all'evoluzione etica della tecnologia e dell'IA, con l'obiettivo di reinvestire le risorse nella ricerca europea anziché esportarle.

Le proposte operative

Le proposte concrete per raggiungere questi obiettivi si concentrano su due aree principali: formazione e promozione delle aziende tecnologiche europee. Sul fronte formativo, si propone l'introduzione di programmi obbligatori a tutti i livelli scolastici, partendo dalla quinta classe primaria, e la formazione continua nel settore pubblico e privato. Si caldeggia anche un sistema di incentivi per studenti, imprese e cittadini, con verifiche delle competenze attraverso enti accreditati.

Lo sviluppo del settore tecnologico europeo

Per quanto riguarda lo sviluppo del settore tecnologico, si punta alla promozione di architetture open source hardware e software, al sostegno di startup e PMI innovative per lo sviluppo di soluzioni "full EU", e all'adeguamento di salari e incentivi per trattenere i talenti europei. Si prevede anche la creazione di un fondo di investimenti dedicato al settore tecnologico e la promozione di progetti ad alto contenuto innovativo.

Ostacoli e sfide future

Tuttavia, esistono fattori che potrebbero ostacolare questi obiettivi: instabilità geopolitica, difficoltà di accesso alle materie prime, debolezza politica nei confronti dei "poteri forti" e una visione politica poco lungimirante che non privilegi gli investi-

menti nella sovranità digitale e nell'educazione delle nuove generazioni.
La sfida per l'Europa sarà quella di mantenere la rotta verso questi obiettivi strategici nonostante le possibili turbolenze economiche e politiche globali.

Formazione e awareness di cybersecurity

La discussione riguardava un'analisi dell'attuale contesto di consapevolezza della cybersecurity, considerando sia le prospettive delle aziende che quelle dei consumatori, con l'obiettivo di affrontare le minacce presenti e future che incombono sugli individui. È stato suggerito un approccio strutturato alla formazione e alla sensibilizzazione, concentrandosi sul colmare le lacune esistenti in termini di competenze, di cultura informatica e di genere, e sottolineando l'importanza di coinvolgere le istituzioni governative, gli enti di formazione e di integrare la formazione sulla sicurezza nelle roadmap organizzative sulla cybersecurity.

Lo scenario attuale e le criticità

Nel 2024, il panorama della formazione e della consapevolezza in ambito cybersecurity presenta diverse criticità significative. Si registra una generale mancanza di competenze, sia a livello lavorativo che nella popolazione di "fruitori della tecnologia". Questa carenza viene in parte mitigata dall'esistenza di programmi non ancora molto strutturati di formazione scolastica sulla cybersecurity a vari livelli e da iniziative di sensibilizzazione rivolte sia alla popolazione generale che alle aziende.

Approcci tradizionali alla sensibilizzazione

Le proposte di sensibilizzazione sviluppate dal gruppo in ottica di breve termine si sviluppano su due fronti principali. Per la popolazione meno informatizzata, si utilizzeranno canali tradizionali come spot televisivi, serie TV educative e campagne pubblicitarie classiche, inclusa la distribuzione di materiale informativo sui prodotti tecnologici. In ambito lavorativo, invece, si punterà all'obbligo di formazione personalizzata per tutti i soggetti dell'organizzazione, dai vertici aziendali fino ai singoli dipendenti, con particolare attenzione ai settori critici come Finance, Legal, IT e sviluppo software.

Innovazioni nelle strategie di sensibilizzazione

Un approccio innovativo prevederà l'istituzione di programmi di mentorship e giornate dedicate alla promozione della sicurezza informatica, con particolare attenzione alle PMI. Si propone di sviluppare una significativa collaborazione con gli influencer digitali per raggiungere il pubblico più giovane attraverso le piattaforme social. Particolare importanza viene data al ruolo del CISO (Chief Information Security Officer), la cui presenza dovrebbe diventare obbligatoria in determinate realtà aziendali.

Il percorso verso il 2035: apprendimento continuo e istantaneo

La visione per il futuro in ottica di lungo termine si basa sul concetto di "lifelong learning" - imparare a imparare - come competenza fondamentale. Questo approccio si concretizza attraverso piattaforme di continuous learning in grado di prevedere:

- autori e contenuti certificati;
- fruizione multi-canale;
- cyber range e simulazioni;
- sistemi di verifica dell'efficacia e certificazioni.

Lo stato dell'arte previsto per il 2035

Per il 2035, si prevede l'implementazione di tecnologie avanzate per la formazione, tra cui:

- utilizzo diffuso di realtà virtuale (VR) e aumentata (AR) per simulazioni di attacchi cyber;
- sistemi di formazione basati su intelligenza artificiale per l'apprendimento personalizzato;
- simulazioni avanzate di minacce in ambiente virtuale;
- gamification integrata nei programmi formativi.

Cultura della sicurezza e collaborazione globale

Si prevede lo sviluppo di una cultura aziendale che promuova l'apprendimento continuo in materia di sicurezza informatica, con programmi formativi incorporati nei processi di lavoro quotidiani. Particolare importanza verrà data alla collaborazione globale e allo scambio di informazioni tra organizzazioni e istituzioni per fronteggiare le minacce emergenti.

Standardizzazione e certificazione

Un elemento chiave della visione futura è lo sviluppo di standard di certificazione riconosciuti a livello mondiale per la valutazione e dimostrazione delle competenze acquisite in materia di sicurezza informatica. Tali standard faciliteranno la mobilità professionale e garantiranno elevati livelli di formazione, contribuendo a creare un ecosistema più sicuro e resiliente.

Strumenti avanzati e integrazione tecnologica

Si prevede lo sviluppo di piattaforme di sensibilizzazione che useranno l'analisi comportamentale per identificare e mitigare i rischi legati all'errore umano. Tali strumenti verranno integrati nei flussi di lavoro quotidiani, fornendo consigli contestuali e supporto immediato. L'integrazione di tecnologie generative IA permetterà di creare

contenuti formativi personalizzati e rispondere alle esigenze di apprendimento degli utenti.

Supply Chain Security

La discussione ha coperto le sfide attuali della Supply Chain Security, evidenziato le principali best practice in materia, proposto dei possibili approcci per una gestione efficace del rischio sistemico, che può impattare pesantemente sulle catene di fornitura delle organizzazioni europee, e analizzato le evoluzioni conseguenti all'entrata in vigore di nuove normative quali la direttiva NIS 2 e il regolamento DORA . Ha esplorato inoltre le caratteristiche che dovranno possedere le Supply Chain per essere a prova di futuro e immaginato scenari alternativi per il 2035, sottolineando la necessità di affrontare i requisiti della Supply Chain Security di oggi in retrospettiva.

Il contesto e le sfide attuali

La sicurezza della Supply Chain rappresenta oggi una delle sfide più critiche per le organizzazioni, con impatti significativi in termini di resilienza, agilità e sostenibilità, oltre alle tradizionali dimensioni di costo, servizio e qualità. L'analisi si concentra su tre possibili scenari futuri, dal più ottimistico al più pessimistico, valutando gli impatti delle tecnologie abilitanti e le minacce emergenti nel campo della cybersecurity.

Gli scenari al 2030

L'analisi PESTLE (Politica, Economia, Società, Tecnologia, Legislazione, Ambiente) ha permesso di identificare tre scenari principali:

- scenario ottimistico: caratterizzato da stabilità politica, prosperità economica e leadership EU-US nel commercio globale;
- scenario intermedio: contraddistinto da alleanze instabili e dominio delle tech giants
- scenario pessimistico: marcato da instabilità politica, protezionismo e forte; disuguaglianza sociale.

Le tecnologie abilitanti

Per ciascuno scenario sono state identificate le tecnologie chiave che influenzeranno l'evoluzione delle Supply Chain:

- Internet of Things e Data Science per la raccolta e l'analisi dei dati;
- Intelligenza Artificiale per l'ottimizzazione dei processi;
- sistemi cloud e infrastrutture di comunicazione;
- Blockchain e sistemi di trasporto autonomi;

- tecnologie di identificazione e localizzazione;
- manifattura additiva.

Impatti sulla sicurezza della Supply Chain

Gli scenari presentano diverse implicazioni per la sicurezza:

- nello scenario ottimistico, l'aumento della digitalizzazione amplia la superficie di attacco, ma viene bilanciato da alleanze internazionali coordinate;
- nello scenario intermedio, si registra un progressivo aumento degli attacchi in un ambiente politico e sociale meno stabile;
- nello scenario pessimistico, si prevede un aumento esponenziale degli attacchi cyber motivati da disruption politiche e sociali

Gestione del rischio e resilienza

L'evoluzione della gestione del rischio varia significativamente nei tre scenari:

- scenario ottimistico: maggiore cooperazione per la condivisione delle informazioni e la pianificazione del recovery;
- scenario intermedio: necessità di rafforzare la gestione delle minacce cyber in un contesto di minor fiducia;
- scenario pessimistico: frammentazione del mercato e Supply Chain locali con minor resilienza.

Le principali minacce future

Secondo l'analisi ENISA delle minacce cyber per il 2030, i rischi principali per le Supply Chain includono:

- compromissione delle dipendenze software;
- errori umani e sistemi legacy vulnerabili:
- attacchi mirati potenziati dai dati dei dispositivi smart;
- abuso dell'Intelligenza Artificiale;
- provider ICT transfrontalieri come single point of failure.

Prospettive e raccomandazioni

Per affrontare le sfide future, si raccomanda:

- lo sviluppo di framework di gestione del rischio adattivi;
- una maggiore cooperazione internazionale per la sicurezza cyber;
- il rafforzamento delle competenze e della formazione;
- l'implementazione di sistemi di valutazione del rischio cyber dei fornitori;
- lo sviluppo di soluzioni complementari per far fronte alle limitazioni delle polizze di cyber insurance nel caso di rischi sistemici.

Il percorso verso il 2035 richiede un approccio olistico che consideri non solo gli aspetti tecnologici, ma anche quelli organizzativi, normativi e di governance, con particolare attenzione alla resilienza e alla sostenibilità delle Supply Chain in un contesto di crescente complessità e interconnessione.

Infrastrutture critiche

La discussione ha trattato la classificazione delle infrastrutture critiche attuali e future, la considerazione se il panorama delle Infrastrutture Critiche (IC) stia diventando più locale, europeo o globale, l'esame del quadro normativo esistente in materia di sicurezza e l'esplorazione di nuove iniziative, nonché la definizione di un perimetro di sicurezza in un contesto di internazionalizzazione.

La presentazione esplora il futuro delle IC con lo sguardo proiettato al 2035, affrontando le sfide emergenti e i possibili scenari evolutivi. Le IC sono identificate come risorse strategiche la cui compromissione minerebbe gravemente le funzioni vitali della società. È significativo notare come la definizione stessa di IC sia in continua evoluzione, riflettendo i cambiamenti nelle priorità nazionali e nelle dinamiche globali.
L'analisi identifica un complesso intreccio di fattori che guidano l'evoluzione delle IC, ciascuno con proprie specificità e impatti:

Dimensione geopolitica e politico-economica

La geopolitica emerge come fattore primario, influenzando direttamente le scelte strategiche nella gestione delle IC. Le tensioni internazionali e gli equilibri di potere determinano quali infrastrutture diventano critiche e come proteggerle. Gli aspetti politico-economici si manifestano nella dialettica tra gestione pubblica e privata, come evidenziato nell'esempio dell'acqua potabile presentato nel documento.

Transizione digitale e sociale

La digitalizzazione continua delle infrastrutture porta con sé nuove vulnerabilità e necessità di protezione. L'interconnessione tra sistemi fisici e digitali crea nuove dipendenze e richiede approcci innovativi alla sicurezza. La dimensione sociale influenza le priorità nella protezione delle IC, considerando l'impatto su comunità e territori.

Cambiamenti climatici e salute

I mutamenti climatici stanno ridefinendo quali infrastrutture siano davvero critiche, introducendo nuove necessità di protezione ambientale e resilienza. Il settore sanitario assume un ruolo sempre più centrale, richiedendo particolare attenzione nella protezione delle relative infrastrutture.

Analisi dettagliata degli scenari prospettici

Scenario 1 - Guerra frammentata

In questo scenario di elevata tensione internazionale le IC si sviluppano secondo logiche di autonomia e resilienza locale:

- i trasporti si orientano verso sistemi terrestri locali, privilegiando la sicurezza sulla efficienza;
- la produzione si riorganizza in ottica di reshoring, con focus su beni strategici come farmaci e armamenti;
- il settore sanitario si frammenta in strutture piccole, ma autonome;
- l'energia viene prodotta in modo decentralizzato, bilanciando fonti rinnovabili e tradizionali;
- le catene logistiche diventano più corte ma più numerose, con elevata capacità di adattamento.

Le implicazioni per la cybersecurity in questo scenario includono:

- lo sviluppo di backbone cloud standardizzati e certificati;
- dei sistemi avanzati di verifica delle informazioni;
- la classificazione rigorosa dei dati sensibili.

Scenario 2 - Distensione internazionale

Questo scenario di maggiore cooperazione internazionale porta a:

- ottimizzazione delle catene di approvvigionamento con standardizzazione dei processi;
- creazione di infrastrutture dedicate all'IA con elevata potenza di calcolo;
- evoluzione del settore sanitario verso grandi strutture private internazionali;
- potenziamento dei collegamenti ferroviari e marittimi internazionali;
- sviluppo di mega-impianti per energie rinnovabili.

La cybersecurity si concentra su:

- la regolamentazione internazionale dell'IA;
- la protezione centralizzata di dati biologici e genetici;
- la certificazione delle catene di approvvigionamento.

Scenario 3 - Crisi climatica

Lo scenario climatico estremo richiede adattamenti radicali delle IC:

- rivoluzione dei trasporti con preferenza per collegamenti aerei e sotterranei;

- trasformazione dell'agricoltura verso sistemi protetti e controllati;
- strutture sanitarie diffuse ma interconnesse;
- massima espansione delle energie rinnovabili con integrazione del nucleare;
- implementazione di grandi opere difensive contro eventi estremi.

Le priorità di cybersecurity includono:

- la protezione dei sistemi di previsione meteorologica;
- la sicurezza delle banche dati su risorse critiche per la sopravvivenza;
- la difesa contro l'uso del clima come arma di cyberwarfare.

Orizzonte 2035: la centralità del fattore umano

L'analisi evidenzia come nel 2035 il ruolo umano rimarrà cruciale ma con nuove vulnerabilità:

- sviluppo di tecniche di analisi delle espressioni facciali (FEA);
- sfruttamento delle distorsioni cognitive;
- necessità di proteggere la privacy del pensiero;
- evoluzione verso una cybersecurity human-centric.

Il ruolo dell'Intelligenza Artificiale

L'IA emerge come elemento trasformativo per le IC, considerando come elementi di rischio che:

- le infrastrutture informatiche che gestiscono i servizi AI saranno esse stesse delle infrastrutture critiche;
- le infrastrutture informatiche saranno sempre di più in mano a operatori colossali che potranno influenzare le politiche nazionali.

Saranno quindi necessari:

- nuovi paradigmi e sistemi di sicurezza per controbilanciare il "potere" dell'AI;
- bilanciamento tra automazione e controllo umano;
- protezione contro manipolazioni e bias algoritmici.

Conclusioni e implicazioni

La presentazione delinea un futuro in cui la protezione delle IC richiederà un approccio sempre più sofisticato e multidimensionale. La convergenza tra minacce fisiche e digitali, unita all'emergere di nuove vulnerabilità legate al fattore umano e all'IA, suggerisce la necessità di ripensare i tradizionali paradigmi di sicurezza.

La capacità di adattarsi rapidamente ai diversi scenari e di implementare strategie di protezione flessibili sarà cruciale per garantire la resilienza delle IC nel prossimo decennio.

Self-sovereign Identity

La Self-Sovereign Identity (SSI) è un concetto innovativo che sta emergendo come risposta alle problematiche legate alla gestione dell'identità digitale. La discussione si è focalizzata sulle sue fondamenta, i portafogli digitali e l'impatto delle Big Tech, con particolare attenzione ai rischi connessi a tali tecnologie. È stato evidenziato come la creazione di ecosistemi sostenibili e affidabili sia essenziale, considerando la necessità di mantenere il controllo sull'identità digitale, migliorare l'esperienza utente e garantire elevati standard di sicurezza.

Nel corso degli anni, l'evoluzione dell'identità digitale ha visto una transizione significativa, passando dal Web 1.0 al Web 3.0, cambiando gradualmente il bilanciamento tra privacy e convenienza. La SSI emerge come una soluzione alle problematiche attuali, proponendosi come alternativa ai modelli centralizzati e federati, dove la gestione dei dati è affidata a provider esterni o Identity Provider. Tale evoluzione riflette una crescente consapevolezza dei rischi legati alla gestione centralizzata delle identità digitali, come i furti di account, l'uso di identità false e le violazioni della privacy, spingendo verso soluzioni più sicure e user-centriche.

Principi fondamentali del modello SSI

Il modello di SSI, elaborato da Christopher Allen nel 2016, si fonda su dieci principi chiave che ridefiniscono il rapporto tra gli utenti e la loro identità digitale. Tra questi, oltre ai principi di esistenza, controllo e trasparenza, vengono enfatizzati concetti come la portabilità, che permette agli utenti di non essere legati a specifiche identità o giurisdizioni, e l'interoperabilità, che garantisce l'uso dell'identità su più piattaforme. Fondamentale è anche il principio della minimizzazione, che impone di limitare la condivisione dei dati al minimo indispensabile, e quello del consenso, che richiede un'autorizzazione esplicita da parte dell'utente per ogni operazione. Infine, la protezione dei diritti e delle libertà individuali assume priorità rispetto alle esigenze della rete.

Vantaggi e benefici

I benefici della SSI sono molteplici e coinvolgono diversi ambiti. Le organizzazioni traggono vantaggio da una significativa riduzione dei costi operativi, una semplificazione nella compliance alle normative e una minore esposizione ai rischi derivanti da

violazioni dei dati. Inoltre, si aprono nuove opportunità di business, in particolare nel campo della verifica delle identità. Per gli utenti, i vantaggi sono altrettanto rilevanti: maggiore controllo sui propri dati personali, una fruizione più semplice e uniforme dei servizi digitali, riduzione dei rischi di furto d'identità e gestione più efficace delle credenziali digitali.

Scenari Applicativi

Le applicazioni della SSI si estendono a numerosi settori. Nei servizi finanziari, ad esempio, la SSI semplifica i processi di Know Your Customer (KYC), migliora la gestione delle credenziali per transazioni bancarie e consente verifiche rapide per prestiti e mutui. In ambito sanitario, offre una gestione sicura delle cartelle cliniche digitali e facilita la condivisione selettiva delle informazioni tra specialisti. Anche nel settore educativo, permette la gestione di diplomi e certificazioni digitali, la verifica delle qualifiche e la portabilità internazionale dei titoli di studio. Nei servizi governativi, la SSI si applica alla digitalizzazione dei documenti di identità, alla gestione delle patenti di guida digitali e all'accesso semplificato ai servizi pubblici.

Implementazione a livello europeo

A livello europeo, l'Unione Europea sta portando avanti l'adozione della SSI tramite iniziative come l'EUDI Wallet, che prevede una roadmap fino al 2026 e un investimento di 77 milioni di euro per sviluppare progetti pilota e prototipi di wallet. Alcuni dei progetti pilota attualmente in corso includono la digitalizzazione delle SIM, l'introduzione delle patenti digitali e lo sviluppo di sistemi di pagamento e gestione di documenti di viaggio elettronici.

Sfide e ostacoli

Nonostante le sue potenzialità, l'implementazione della SSI incontra diverse sfide. Tra quelle tecniche, la creazione di infrastrutture tecnologiche avanzate e la necessità di garantire l'interoperabilità tra diversi sistemi sono prioritarie. Le sfide organizzative riguardano la resistenza al cambiamento da parte delle aziende e gli elevati investimenti richiesti. Inoltre, è necessario superare le difficoltà di mercato, come la necessità di raggiungere una massa critica di utenti e la concorrenza con soluzioni esistenti, nonché definire modelli di business sostenibili.

Prospettive future

Le prospettive future della SSI, al 2035, vedono l'integrazione con tecnologie avanzate come il riconoscimento biometrico nei wallet digitali e l'uso dell'intelligenza artificiale per nuovi sistemi di autenticazione. Si prevede anche una crescente ado-

zione della SSI in vari ambiti quotidiani e una maggiore consapevolezza riguardo alla protezione dei dati personali.

Collaborazione Internazionale

Il successo della SSI dipende dalla collaborazione tra organizzazioni internazionali e attori chiave, come il World Wide Web Consortium (W3C), la Decentralized Identity Foundation (DIF) e la Sovrin Foundation. Inoltre, è cruciale lo sviluppo di protocolli e standard comuni per garantire l'interoperabilità e la creazione di framework globali di fiducia.

Conclusione

In conclusione, la SSI rappresenta una vera e propria rivoluzione nella gestione dell'identità digitale, con il potenziale di garantire un futuro in cui gli utenti possano esercitare pieno controllo sui propri dati, beneficiando al contempo di servizi digitali più sicuri ed efficienti. Tuttavia, la sua realizzazione richiede un impegno collettivo tra pubblico, privato e società civile, ma i vantaggi che essa può portare giustificano pienamente gli sforzi necessari.

New Space Economy

Nel 2035, la Space Economy sarà un pilastro strategico dell'economia globale, integrando settori chiave come telecomunicazioni, osservazione della Terra, esplorazione spaziale e servizi di navigazione. Tuttavia, con questa crescita esponenziale, emergeranno rischi cyber senza precedenti, dovuti alla dipendenza tecnologica, alla molteplicità di attori coinvolti e alla mancanza di normative aggiornate e universali. La Space Economy sarà basata su un ecosistema altamente interconnesso, che include:

- **segmenti spaziali:** satelliti per comunicazioni, sensori orbitali e stazioni spaziali operative;
- **segmenti terrestri:** centri di controllo, infrastrutture critiche per la gestione dei dati e l'elaborazione delle informazioni;
- **segmenti di collegamento:** reti di trasmissione dati tra spazio e Terra, altamente vulnerabili agli attacchi cyber;
- **segmenti utenti:** applicazioni finali che influenzano settori civili, militari e industriali.

Questa complessità introduce molteplici punti di vulnerabilità, aumentando l'esposizione ad attacchi mirati. A tal fine le minacce principali verteranno su:

- **cyberattacchi ai satelliti** come lo Hijacking, il controllo ostile dei satelliti con

conseguenze sulla sicurezza nazionale e l'interruzione dei servizi globali.

- Interferenza nelle comunicazioni attraverso blocco o manipolazione di segnali satellitari per telecomunicazioni, navigazione GPS e osservazioni;
- **attacchi ai Segmenti di Terra** con intrusioni nei centri di controllo e relativa compromissione di infrastrutture critiche per accedere ai sistemi operativi spaziali.
- **DoS e DDoS** con potenziale sovraccarico delle reti terrestri, rendendo inaccessibili i servizi spaziali;
- **compromissione della Supply Chain** laddove l'ecosistema spaziale dipenderà da fornitori di hardware e software globali. La compromissione delle supply chain potrebbe introdurre vulnerabilità in componenti critici;
- **manipolazione e Furto di Dati** con il potenziale rischio che i dati sensibili raccolti dai satelliti (es. osservazioni climatiche, dati finanziari o militari) diventino bersagli primari per cybercriminali e stati ostili;
- **weaponizzazione dello Spazio** attraverso attori malevoli intenti a sviluppare malware specifici per ambienti spaziali, progettati per danneggiare fisicamente i satelliti o interferire con i loro sistemi operativi.

Ai fini degli impatti su larga scala, potremmo assistere a quelli economici, con interruzioni nei servizi satellitari potrebbero causare perdite miliardarie nei settori bancario, energetico e logistico. La Sicurezza Nazionale sarebbe esposta attraverso la vulnerabilità delle infrastrutture spaziali che potrebbero diventare una minaccia strategica per i governi. Anche l'innovazione potrebbe essere pregiudicata, laddove gli attacchi cyber potrebbero rallentare gli investimenti privati e la fiducia nell'economia spaziale. Qual è, dunque, la strategia di mitigazione che auspicabilmente deve essere intrapresa? Per affrontare questi potenziali rischi nel 2035, saranno necessarie infrastrutture resilienti e il consolidamento della segmentazione e crittografia avanzata delle reti. La governance globale dovrà disporre di normative condivise per regolamentare la sicurezza spaziale e cyber e la formazione unitamente alla consapevolezza dovranno avere oggettivo riscontro con training costante per gli operatori e programmi di simulazione di attacchi cyber. Infine una collaborazione pubblico-privata attraverso partnership idonee per condividere tecnologie di sicurezza avanzate. Mentre la Space Economy offrirà opportunità straordinarie, la crescente digitalizzazione e l'interconnessione porteranno rischi cyber significativi. Il successo di questa economia emergente dipenderà dall'implementazione di una solida strategia di sicurezza per proteggere le infrastrutture critiche e garantire la sostenibilità del progresso tecnologico nello spazio.

Sondaggi

Il futuro è un viaggio ed esso è plasmato da noi stessi attraverso le nostre scelte, l'introduzione di nuove scoperte e tecnologie che cambiano lo scenario, o da interventi legislativi che modificano le regole del gioco, generando possibili sviluppi aleatori dovuti a sliding doors non facilmente preventivabili.

Undici diversi continuum sono divenuti altrettanti sondaggi, dove il pubblico ha espresso la propria desiderabilità e probabilità sullo scenario futuro e sul suo opposto.

I Sondaggi sono stati:

1. Immaginando un continuum con due scenari opposti: "Cyborg" vs Divieto al potenziamento umano" quale dei due è preferibile e/o probabile?
   Neuralink di Musk ci ha già dimostrato che lo scenario cyborg non è fantascienza. I votanti hanno ritenuto probabile o molto probabile il futuro auspicato da Musk (74%) e il 32% lo ritiene perfino desiderabile.

2. Schedati dal marketing, è questo che ci attende?
   I votanti hanno ritenuto molto probabile la profilazione avanzata (67%) pur considerandola complessivamente poco o non desiderabile (96%).

3. Cyber war: quale futuro? Accordo internazionale o cyberwar continua?
   Nessuna sorpresa in questo sondaggio. I votanti sono sfiduciati sulla possibilità che si raggiunga un accordo internazionale sul contenimento del cyber crime. Il 78% lo ritiene non probabile mentre il 94% lo ritiene desiderabile.

4. Professionista e IA: Chi avrà l'ultima parola?
   I votanti non sembrano fidarsi troppo dell'IA ritenendo non così desiderabile affidarsi interamente a essa (78%).

5. Ritorneremo tutti in ufficio? è questo il futuro?
   83% è il numero di chi auspica una vita lontano dagli uffici.

6. Deepfake o deeptruth?
   Con questo sondaggio è stato chiesto quale fosse la preferibilità per poter riconoscere un fake. Meglio un tag per evidenziare i contenuti generati dall'IA o meglio un tag sui contenuti autentici.

7. Stato di sorveglianza: verso il controllo totale?
   Un ipotetico stato di sorveglianza alla Minority Report non è desiderato (14%) ma è ritenuto probabile (71%) dal nostro pubblico.

8. Internet of bodies: quali tutele normative per i dati di una umanità interconnessa?
   In questo sondaggio abbiamo chiesto ai votanti se si dovesse adottare un approccio regolamentato alla produzione e trasmissione di dati IoB e IoT.

9. Guida autonoma oppure No?
   Il 53% dei nostri votanti vorrebbe un auto senza volante che li porti a destinazione a suon di comandi vocali.

10. Data monetization o Privacy?
    In uno scenario futuro in cui esista una borsa valori dei dati e un mercato libero, quanto varrebbe la nostra privacy? Il 35% sarebbe felice di rinunciare alla propria privacy in cambio di un ritorno economico.

11. Personal computers o personal robot?
    Il 69% dei votanti è pronto a correre a comprare un personal robot.

I sondaggi sono tutti navigabili alla pagina: https://cyberfutures.clusit.it/ dove è possibile votare, prendere visione delle fonti che hanno suffragato la realizzazione dei sondaggi e ovviamente consultare i risultati di quest'ultimi. Alla pagina LinkedIn: https://www.linkedin.com/company/2035cyberfutures/ è anche possibile interagire con l'iniziativa dei cyberfutures.

Conclusione

Questa iniziativa si è appena conclusa con l'ultimo webinar dedicato ai temi della formazione. Le registrazioni della conferenza e dei webinar si trovano qui: https://cyberfutures.clusit.it/

Nel momento in cui scriviamo questo focus per il Rapporto Clusit, la Clusit Community for Security sta definendo quale sarà il tema del prossimo gruppo di lavoro fino a marzo 2026. Le istruzioni per partecipare alla Community sono sul nostro sito: https://c4s.clusit.it/ sono benvenuti i professionisti che si occupano di sicurezza, rischio e compliance.

Le tendenze 2025 nel settore della sicurezza ibrida

(A cura di Dirk Schrader e Maurizio Tagliorетti, Netwrix)

Sintesi

Nel 2024, Netwrix Research Lab ha condotto l'annuale sondaggio, tramite questionario online, su 1309 professionisti IT di 104 paesi, confrontandone i risultati con i report sulla sicurezza dei dati nel cloud ("Cloud Data Security Report") pubblicati nel 2022, 2020 e 2019 e con i report sulle tendenze IT ("IT Trends Report") pubblicati nel 2023 e nel 2020. Il report relativo potrà essere utile alle organizzazioni per concentrare gli sforzi di sicurezza sulle questioni effettivamente prioritarie. Tra i risultati principali emersi dal sondaggio:

L'ARCHITETTURA IT

Circa 3 organizzazioni su 4 dispongono di un'architettura IT ibrida, quota rimasta invariata rispetto al 2023. La percentuale di chi utilizza un'infrastruttura esclusivamente on-premise è diminuita leggermente, passando dal 19% al 15%. Questo è in linea con quanto osservato lo scorso anno, quando il 37% delle organizzazioni on-premise only prevedeva di adottare tecnologie cloud entro 12 mesi.

GLI INCIDENTI DI SICUREZZA

Il 79% delle organizzazioni ha rilevato un attacco informatico negli ultimi 12 mesi, in aumento rispetto al 68% del 2023. Nel 2023, le infrastrutture on-premise avevano subito più attacchi rispetto a quelle cloud; quest'anno, abbiamo registrato risultati quasi identici per entrambe. Gli attacchi associati alla compromissione degli account nel cloud continuano ad aumentare: nel 2024 ha segnalato questo tipo di incidente il 55% dei partecipanti al sondaggio, rispetto ad appena il 16% del 2020. Gli attacchi mirati sono diventati più comuni on-premise: ha rilevato questo tipo di attacco il 27% dei partecipanti, rispetto ad appena il 19% del 2023.

LE SFIDE RELATIVE ALLA SICUREZZA

Quest'anno, errori o negligenza dei dipendenti sono in cima alla lista, in salita dal terzo posto del 2023. Continuano a occupare l'ultimo posto, invece, le azioni dolose dei dipendenti.

LE CONSEGUENZE DEGLI ATTACCHI INFORMATICI

La percentuale di organizzazioni che non ha subito conseguenze derivanti da incidenti di sicurezza è scesa, dal 45% dell'anno scorso al 38% del 2024. La principale conseguenza negativa sono state le spese impreviste per colmare le lacune della sicurezza, citate dal 45% e dal 40% dei partecipanti, rispettivamente nel 2024 e nel 2023. Un'organizzazione su 6 (17%) ha stimato di aver subito danni finanziari da incidenti informatici per almeno $50.000.

LE MISURE DI SICUREZZA ATTUALI

Nel corso dell'ultimo anno, le organizzazioni hanno migliorato la propria postura di sicurezza. Il progresso più notevole si registra nella governance dell'identità: nel 2024, il 55% dei partecipanti disporrà di una soluzione di questo tipo nel cloud e il 58% on-premise, contro (rispettivamente) il 44% e il 43% del 2023. Inoltre, il sondaggio evidenzia che i principali miglioramenti dell'ultimo anno sono stati apportati nel cloud, piuttosto che on-premise.

LE MISURE DI SICUREZZA PIANIFICATE

La classificazione dei dati è in cima alla lista delle misure che le organizzazioni intendono implementare per migliorare la sicurezza informatica, nel cloud e on-premise.

LE PRIORITÀ IT

A preoccupare maggiormente sono la sicurezza dei dati, la sicurezza di rete e la formazione sulla sicurezza informatica. Aumenta l'interesse per l'implementazione di strumenti di intelligenza artificiale, dal 12% dei partecipanti nel 2020 al 28% nel 2024. La percentuale di organizzazioni che danno priorità all'adozione del cloud continua a crescere ed è pari al 36% nel 2024, in crescita rispetto al 32% del 2023 e al 23% del 2020.

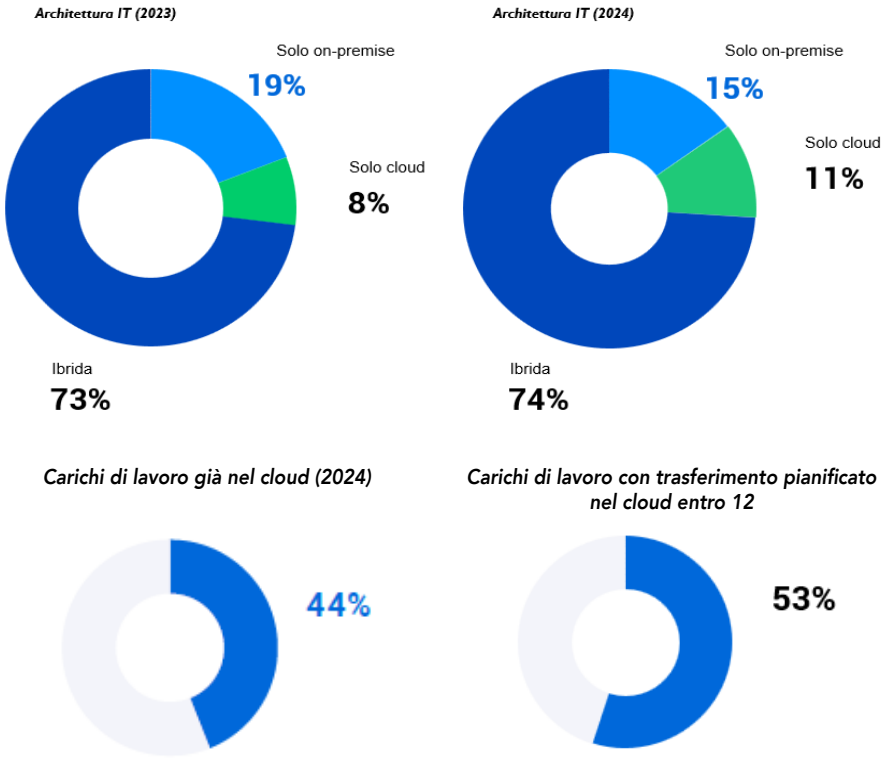
LE ASSICURAZIONI CONTRO I RISCHI IT

Il 62% delle organizzazioni ha stipulato una polizza assicurativa contro i rischi informatici o prevede di farlo entro 12 mesi. Lo scorso anno, quasi un'organizzazione assicurata su 5 (19%) ha usufruito della propria polizza.

L'architettura IT

Il lavoro da remoto e ibrido, unitamente alle esigenze aziendali di flessibilità ed efficienza dei costi, continua a favorire l'adozione del cloud. Circa 3 organizzazioni su 4 dispongono di un'architettura IT ibrida, quota rimasta invariata rispetto al 2023. La percentuale di chi utilizza un'infrastruttura esclusivamente on-premise è diminuita leggermente, passando dal 19% al 15%. Questo è in linea con quanto osservato lo scorso anno: il 37% delle organizzazioni on-premise only prevedeva di adottare tecnologie cloud entro 12 mesi.

Tuttavia, lo spostamento nel cloud dei carichi di lavoro è avvenuto più lentamente rispetto alle previsioni: la percentuale è aumentata leggermente, dal 41% nel 2022 al 44% del 2023, per poi assestarsi nel 2024, contro il 53-55% previsto dai partecipanti al sondaggio. Una previsione che si è ripetuta quest'anno, a indicare che i professionisti IT continuano a voler ampliare l'adozione del cloud.



Il **58%** delle organizzazioni on-premise only che prevedono di adottare tecnologie cloud; il 30% prevede di farlo entro 12 mesi.

Commenti degli autori

Spesso è difficile prevedere con precisione le tempistiche di progetto per una transizione tecnologica importante come la migrazione al cloud. Lo scorso anno, oltre alle sfide consuete legate alla pianificazione dei progetti, le organizzazioni hanno dovuto affrontare anche l'incertezza dovuta alle difficoltà economiche globali. Un buon modo per mantenere il ritmo desiderato di adozione del cloud è suddividere la transizione in fasi, più facili da gestire e controllare.

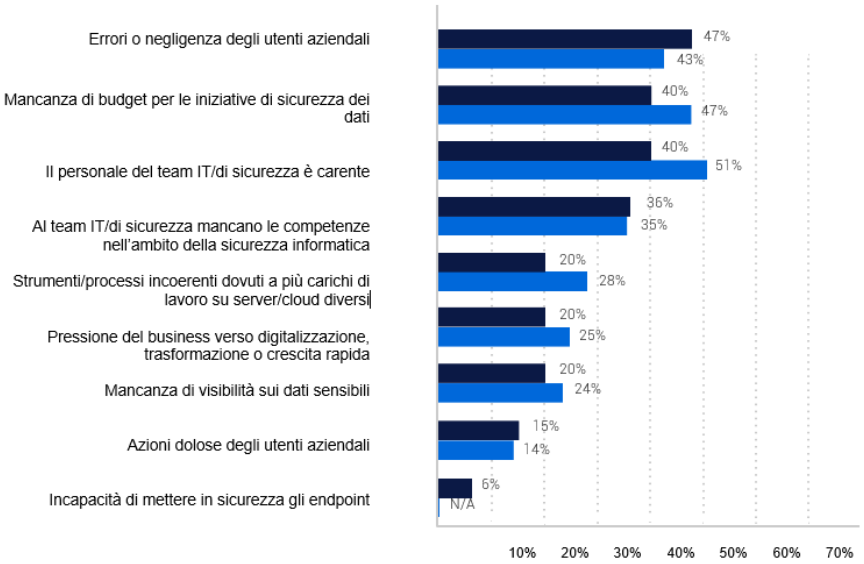
La migrazione al cloud è un processo continuo, apparentemente privo di una conclusione definitiva. Man mano che un'organizzazione si evolve, i carichi di lavoro da

trasferire nel cloud, o da riportare on-premise, vengono continuamente rivalutati; e la decisione si basa solitamente su fattori come l'efficienza operativa, i costi e la conformità a leggi e regolamenti applicabili. Tra i carichi di lavoro generalmente migrati nel cloud sono inclusi quelli relativi alle risorse umane, al marketing e alla fatturazione, nonché i processi lato cliente, che richiedono di scalare senza soluzione di continuità.

Le sfide relative alla sicurezza

Se garantire la sicurezza dei dati è un compito arduo, alcuni ostacoli sono più rilevanti di altri. Abbiamo chiesto ai partecipanti al sondaggio di classificare le principali sfide per la sicurezza dei dati che si trovano ad affrontare: quest'anno, errori o negligenza dei dipendenti sono in cima alla lista, in ascesa dal terzo posto del 2023, mentre le azioni dolose, sempre dei dipendenti, rimangono in fondo alla classifica.

Le sfide principali affrontate per garantire la sicurezza dei dati (2023, 2024)



Commenti degli autori

Per affrontare la sfida principale in materia di sicurezza emersa dal sondaggio, i team dedicati devono implementare controlli tecnici che aiutino gli utenti a evitare gli errori, senza causare inconvenienti rilevanti. Una gestione intuitiva delle

password consente accessi al tempo stesso fluidi e sicuri, mentre un'attenta autenticazione multi fattore aiuta a prevenire l'abuso delle credenziali senza creare un peso eccessivo sui dipendenti. Una moderna soluzione PAM è in grado di fornire privilegi sufficienti solo per il tempo necessario a svolgere un'attività, riducendo la superficie di attacco senza creare attrito. Trovare il giusto equilibrio tra sicurezza e un'esperienza utente valida è essenziale per proteggere adeguatamente l'organizzazione.

Possiamo aspettarci che budget ridotti, carenza di personale e mancanza di competenze in materia di sicurezza continueranno a essere tra le preoccupazioni principali dei team di sicurezza IT, perlomeno nei prossimi anni. Per affrontare queste sfide, le organizzazioni possono adottare strategie che consentano agli utenti di lavorare in modo più efficiente. Framework come NIST CSF e ISO 27001 aiutano a focalizzare gli interventi di sicurezza e a definirne le priorità; inoltre, le organizzazioni possono rivolgersi a fornitori di servizi di sicurezza gestiti (MSSP) per colmare le lacune di competenze o di personale, e sfruttare soluzioni software, per automatizzare le attività che richiedono più forza lavoro e per ridurre rumore e falsi positivi.

Gli incidenti di sicurezza

Il **79%** delle organizzazioni che hanno rilevato un attacco informatico negli ultimi 12 mesi, in aumento rispetto al 68% del 2023.

Cloud e on-premise a confronto

Abbiamo chiesto ai partecipanti di condividere i dettagli degli incidenti di sicurezza rilevati all'interno delle loro organizzazioni: per il 2023, sono stati segnalati più attacchi alle infrastrutture on-premise rispetto al cloud, in particolare di phishing e malware; quest'anno, invece, il dato è pressoché identico per entrambi i segmenti dell'infrastruttura (grafico 4).

Commenti degli autori

Nel corso dell'ultimo anno, l'infrastruttura cloud è stata presa di mira più di frequente dagli autori di attacchi. Le organizzazioni continuano ad adottare tecnologie cloud e a trasferire i propri carichi di lavoro, anche se non al ritmo previsto. Per aumentare la flessibilità dell'infrastruttura IT nel complesso, la scelta si orienta verso tecnologie come SaaS (software-as-a-service), PaaS (platform-as-a-service) e IaaS (infrastructure-as-a-service), fornite da terze parti, o sviluppate internamente. La superficie di attacco nel cloud continua quindi ad ampliarsi, così come il numero di incidenti di sicurezza.

Quest'anno, il numero di organizzazioni che ha rilevato un attacco alla propria infrastruttura IT è aumentato. Strumenti di hacking pronti all'uso, programmi di affiliazione e una serie di alternative di cybercrime-as-a-service mettono gli attacchi alla portata anche dei criminali meno esperti. Al tempo stesso, chi da questi attacchi si deve difendere sta potenziando le proprie capacità di rilevamento, incrementando il numero di attacchi identificati. Inoltre, cresce tra i dirigenti aziendali la consapevolezza dei rischi di business derivanti dagli incidenti di sicurezza, il che porta a una maggiore trasparenza, con un impatto anche sul numero di incidenti segnalati.

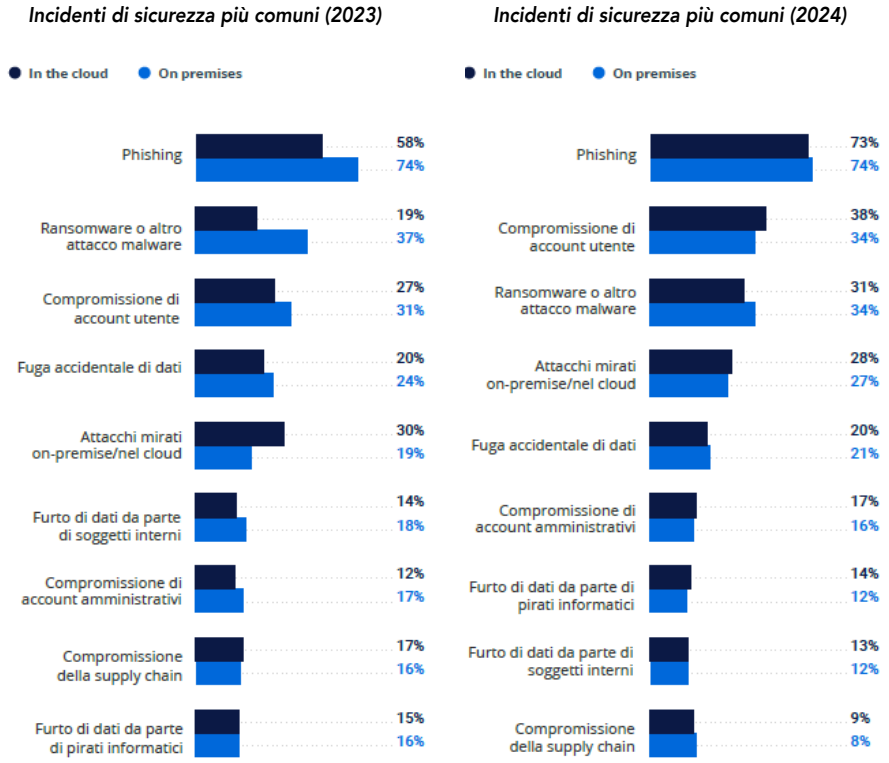


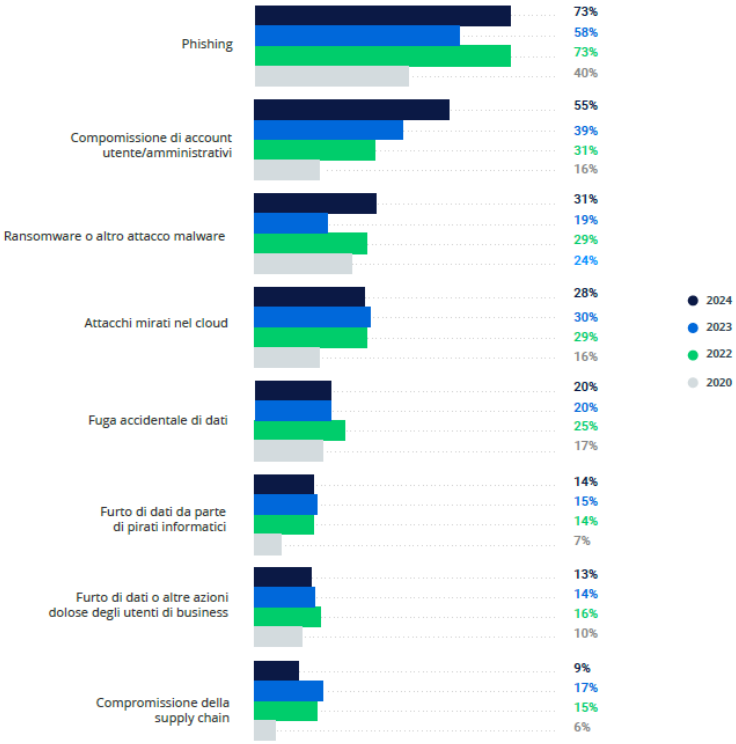
Grafico 4

Gli incidenti di sicurezza nel cloud

Abbiamo confrontato i risultati relativi agli incidenti di sicurezza nel cloud di quest'anno con quelli del 2020, 2022 e 2023. Il phishing rimane la tipologia più diffusa, ma gli attacchi associati alla compromissione degli account nel cloud continuano a

guadagnare slancio: nel 2020, solo il 16% dei partecipanti al sondaggio aveva segnalato questo tipo di incidenti, che nel 2024 sono invece arrivati a una percentuale di ben il 55%.

Incidenti di sicurezza più comuni nel cloud (2020, 2022, 2023, 2024)



Commenti degli autori

I risultati del sondaggio confermano quello che gli esperti del settore dicono da anni: l'identità è il nuovo perimetro. Gli autori di attacchi continueranno a prenderla di mira e, prima o poi, riusciranno nel loro intento. I team di sicurezza IT dovrebbero porsi come obiettivo un approccio equilibrato alla protezione degli account. Oltre a implementare il principio del privilegio minimo, possono ridurre il rischio di compromissione tramite l'autenticazione multi fattore, il Single Sign-On e la formazione finalizzata ad aumentare la consapevolezza degli utenti.

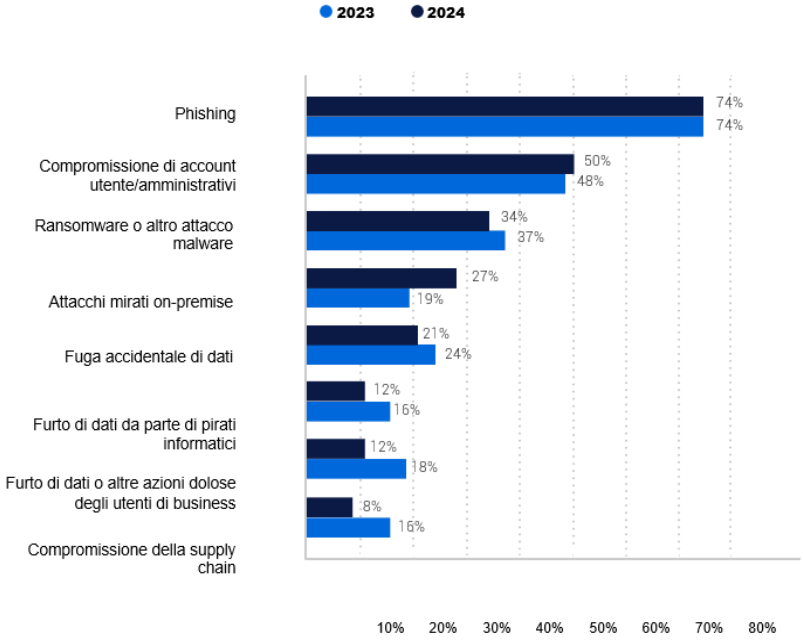
L'implementazione di soluzioni SaaS di terze parti o di soluzioni cloud interne aumenta significativamente il numero delle identità utilizzate; non stupisce, quindi,

che continuino ad aumentare anche gli attacchi associati alla compromissione degli account utente e amministrativi. Per gestire questo rischio e ridurre la superficie di attacco, è fondamentale attenersi al principio del privilegio minimo e garantire la governance dell'identità, in modo che ogni utente disponga esclusivamente dei diritti necessari e sufficienti a svolgere il proprio lavoro. Le organizzazioni dovrebbero valutare l'implementazione dell'autenticazione multi fattore (MFA) per tutti gli account che accedono alle soluzioni cloud interne, seguendo l'approccio adottato di default dai provider di servizi cloud. Nel caso di applicazioni interne rivolte ai clienti, l'MFA rappresenta un requisito essenziale e non negoziabile.

Gli incidenti di sicurezza on-premise

Per comprendere le tendenze relative agli incidenti di sicurezza on-premise, abbiamo confrontato i risultati del nostro report del 2023 con i dati raccolti nel 2024. Di particolare evidenza è la percentuale di coloro che hanno subito un attacco mirato, aumentata di ben il 42%, dal 19% al 27%.

Incidenti di sicurezza on-premise più comuni (2023, 2024)



Commenti degli autori

Le campagne non mirate sono più facili da identificare e gestire, per i team di sicurezza e per i normali utenti aziendali. Di conseguenza, gli autori di attacchi stanno passando a un approccio individualizzato. Inoltre, la creazione di attacchi mirati oggi è più semplice: grazie all'intelligenza artificiale, i criminali informatici raccolgono e analizzano i dati provenienti da violazioni precedenti, dai social media e da altre fonti di pubblico dominio, per adattare le loro campagne dolose a settori e organizzazioni specifici, o persino a singoli individui. Tuttavia, sebbene gli attacchi mirati aumentino le probabilità di un'infiltrazione iniziale, si sviluppano come tutti gli altri: un'escalation di privilegi finalizzata a ottenere l'accesso a dati sensibili.

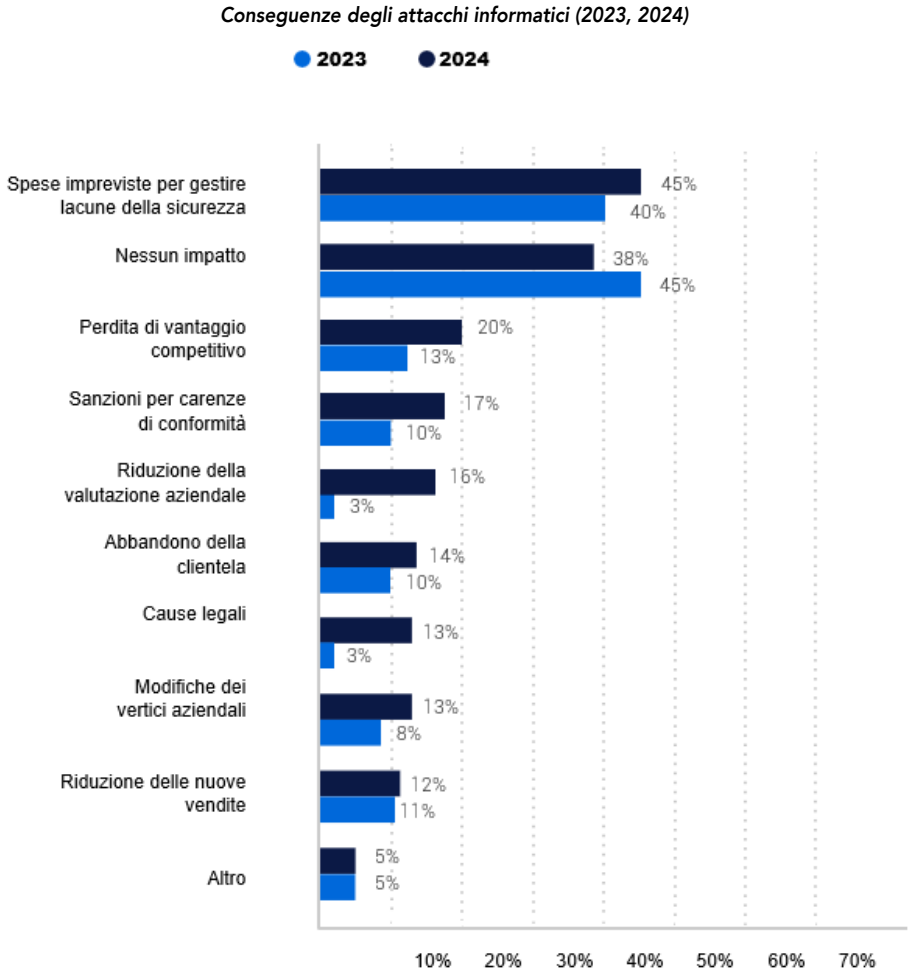
Storicamente, gli ambienti on-premise dispongono di controlli e processi di sicurezza maggiormente consolidati. I team sono più esperti e il ritmo del cambiamento tecnologico più lento rispetto a quanto avviene, in media, nel cloud, quindi, le organizzazioni con carichi di lavoro on-prem sono più preparate a contrastare gli attacchi di compromissione drive-by. Gli avversari motivati finanziariamente o politicamente a prendere di mira questi ambienti riscontrano percentuali di successo più limitate con un approccio "taglia unica" e sono costretti a definire strategie più mirate per queste organizzazioni.

Le conseguenze degli attacchi informatici

Non tutti gli attacchi informatici provocano danni: tuttavia, la percentuale di organizzazioni che non ha subito alcun impatto a causa degli incidenti di sicurezza quest'anno è scesa dal 45% al 38. La principale conseguenza negativa sono state le spese impreviste per colmare le lacune della sicurezza, citate dal 45% dei partecipanti nel 2024 e dal 40% nel 2023.

Tra le altre conseguenze, danni al vantaggio competitivo dell'azienda, alla sua valutazione o al flusso di ricavi, ma anche costi di conformità e legali; in effetti, nel 2024 il numero di organizzazioni che le ha subite è notevolmente aumentato.

1 su 5 Organizzazioni che segnalano la perdita di vantaggio competitivo a causa di un attacco informatico.



Commenti degli autori

I dirigenti sono sempre più consapevoli dell'importanza della sicurezza, il che migliora la comprensione della portata dei rischi derivanti dalle lacune in questo ambito, che vanno ben oltre i tempi di inattività e la perdita di dati. Ecco perché sempre più organizzazioni investono risorse in audit esterni o interni, per individuare, analizzare e correggere la causa principale di un incidente di sicurezza, e prevenire eventi simili in futuro. Gli interventi di mitigazione vanno da semplici modifiche alla configurazione dei sistemi a progetti di grandi dimensioni, ad esempio di rilevazio-

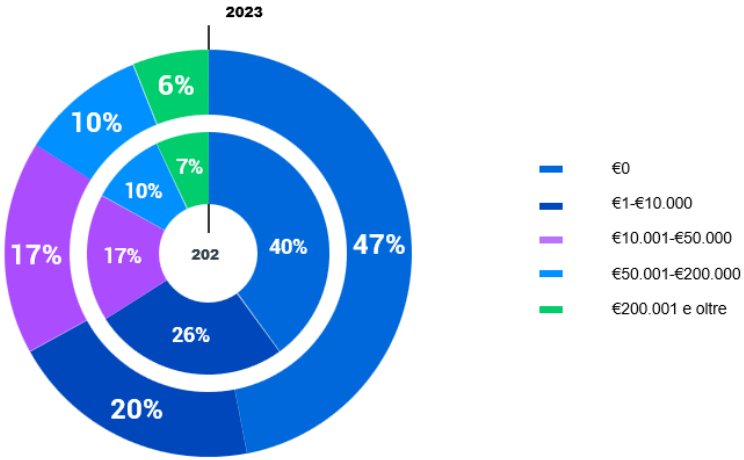
ne e classificazione dei dati, o di riprogettazione della gestione dell'accesso alle identità.

Un incidente informatico può evidenziare lacune nella sicurezza, come privilegi amministrativi eccessivi, account inattivi, password deboli o mai aggiornate, configurazioni o password predefinite e sistemi privi di patch. Colmare queste lacune non implica necessariamente un esborso in denaro, ma richiede sicuramente un impegno in termini di tempo al team di sicurezza IT. In altre parole, gestire la causa principale di un incidente di sicurezza comporta un investimento aggiuntivo, in termini di denaro o di sforzi.

I costi degli incidenti di sicurezza

Non tutti gli attacchi provocano danni finanziari, ma alcuni possono avere conseguenze molto pesanti. In effetti, un'organizzazione su 6 (17%) stima di aver subito un danno finanziario da incidenti informatici per almeno $50.000. Non solo: rispetto all'anno scorso, la percentuale di organizzazioni che, al contrario, non ha subito alcun impatto finanziario è scesa dal 47% al 40%.

Costi degli incidenti di sicurezza (2023, 2024)

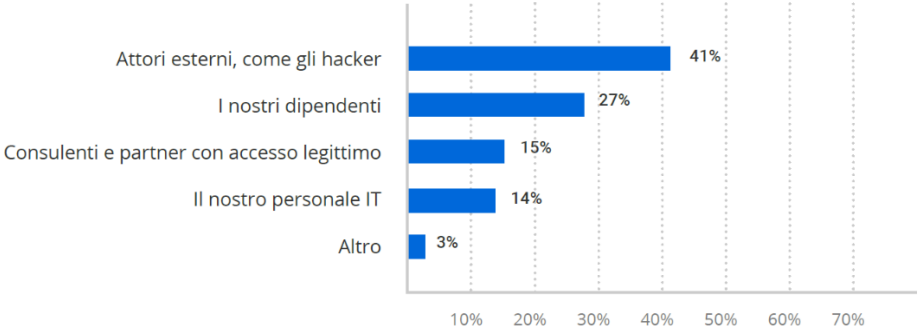


1 su 6 le organizzazioni che hanno segnalato danni finanziari dovuti a minacce informatiche per almeno €50.000

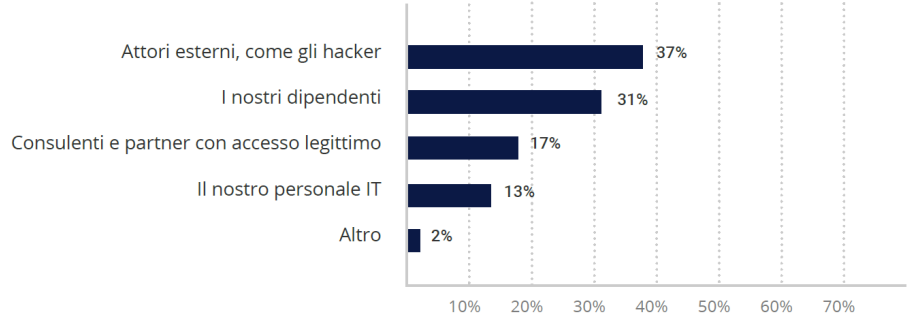
Gli attori delle minacce

Determinare chi rappresenta una minaccia è fondamentale per costruire un'architettura di sicurezza efficace. Abbiamo chiesto ai partecipanti al sondaggio di scegliere la tipologia di attore che, all'interno della loro organizzazione, rappresenta il rischio maggiore per la sicurezza dei dati. Ne è emerso che, per l'infrastruttura on-premise, a preoccupare maggiormente i professionisti IT sono i dipendenti dell'azienda; per il cloud, sono gli attori esterni.

Chi rappresenta il rischio maggiore per la sicurezza dei dati on-premise (2024)



Chi rappresenta il rischio maggiore per la sicurezza dei dati nel cloud (2024)



Commenti degli autori

Le minacce derivanti dagli utenti aziendali sono collegate, di solito, a errori o negligenza, più che ad azioni dolose. Il metodo più efficace per mitigare questi rischi è adottare misure di sicurezza in grado di evitare conseguenze significative causate da errori degli utenti finali o degli amministratori; e il primo passo consiste nell'ottenere una visibilità completa sui dati e sui privilegi assegnati. Si passa quindi alla

revisione dei diritti di accesso e alla rimozione di tutti i privilegi eccessivi, da ripetere regolarmente. Per ridurre ulteriormente la superficie di attacco, è possibile implementare una soluzione di gestione degli accessi privilegiati (PAM) che fornisca privilegi just-in-time.

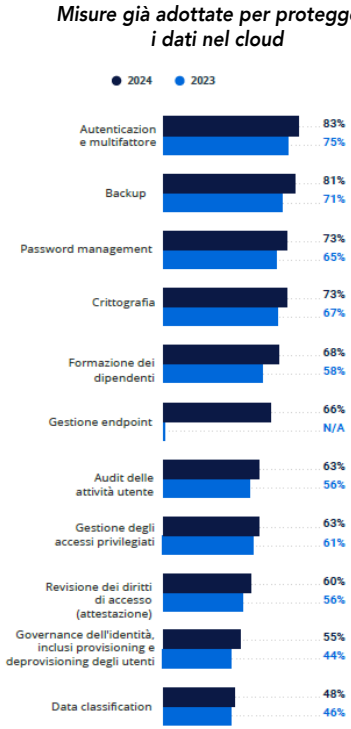
La sicurezza è una responsabilità condivisa tra i fornitori di servizi cloud e le organizzazioni, che devono però comprendere chiaramente come sono suddivise queste responsabilità: devono sapere che tipo di garanzie vengono offerte e stabilire se sono adeguate ai rischi aziendali. A volte, saranno sufficienti buone recensioni di clienti e altri operatori del settore. Più spesso, è necessaria una convalida di terze parti, come certificazioni, accesso ai risultati di audit o l'impegno a effettuare test di penetrazione periodici. In contesti ad alto rischio, l'organizzazione potrebbe richiedere un accesso diretto per ispezionare l'infrastruttura del fornitore e prendere parte a esercitazioni red team.

Le misure di sicurezza attuali

Abbiamo chiesto ai partecipanti al sondaggio quali misure adottano per proteggere i dati, nel cloud e on-premise. Dal confronto con i risultati dell'anno scorso emerge che, nel complesso, le organizzazioni hanno migliorato il loro livello di sicurezza, implementando misure aggiuntive. Il progresso più notevole si registra nella governance dell'identità: attualmente, il 55% dei partecipanti dispone di una soluzione di questo tipo nel cloud e il 58% on-premise, contro (rispettivamente) il 44% e il 43% del 2023. Il sondaggio, inoltre, rivela che i principali miglioramenti dell'ultimo anno sono stati apportati nel cloud, piuttosto che on-premise (**grafico 11**).

Il **51%** delle organizzazioni con architettura full-cloud che dispongono di una soluzione PAM, rispetto al 63% delle organizzazioni in totale

Il **47%** delle organizzazioni con architettura solo on-premise che dispongono di una soluzione IGA, rispetto al 58% delle organizzazioni in totale.



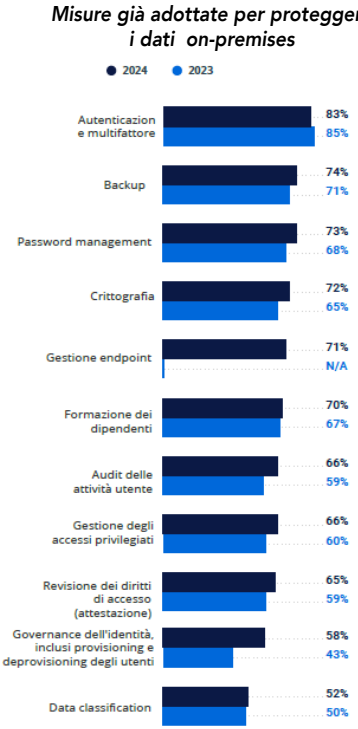


Grafico 11

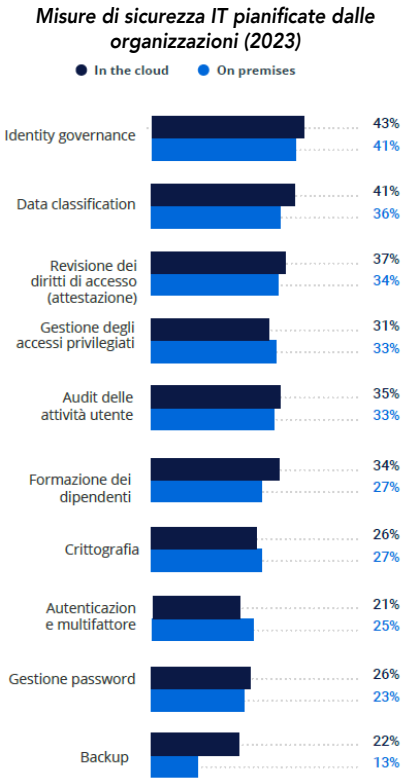
Le misure di sicurezza pianificate

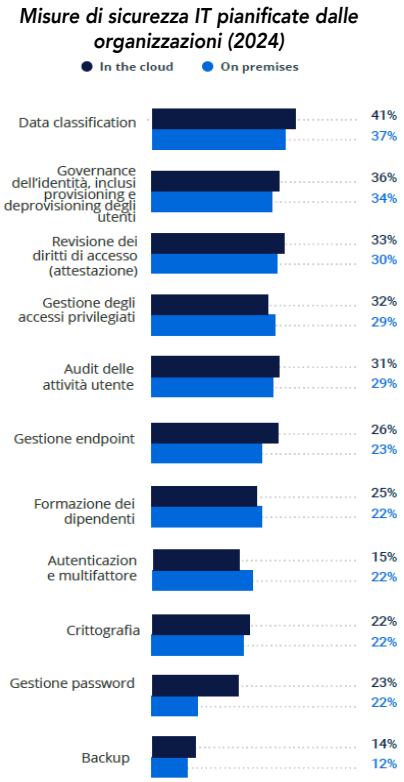
Le priorità delle organizzazioni

Quest'anno, la classificazione dei dati è in cima alla lista delle misure che le organizzazioni intendono implementare per migliorare la sicurezza informatica, nel cloud e on-premise. Come già detto, la percentuale di adozione della governance dell'identità è aumentata rispetto al 2023; non sorprende, quindi, che questa soluzione sia passata dal primo al secondo posto nella classifica del 2024.

Commenti degli autori

L'adozione del cloud ha portato i team di sicurezza IT a spostare l'attenzione dalla protezione del perimetro di rete, i cui confini si sono fatti meno definiti, all'identità, considerata il nuovo perimetro della sicurezza. La governance dell'identità, la revisione dei diritti di accesso e la gestione degli accessi privilegiati (PAM)





contribuiscono a garantire la correttezza dell'accesso, in termini di utenti, modalità, contenuti e tempistiche. L'automazione di questi processi consente al team IT di risparmiare tempo prezioso e migliora la precisione, generando una postura di sicurezza resiliente e flessibile.

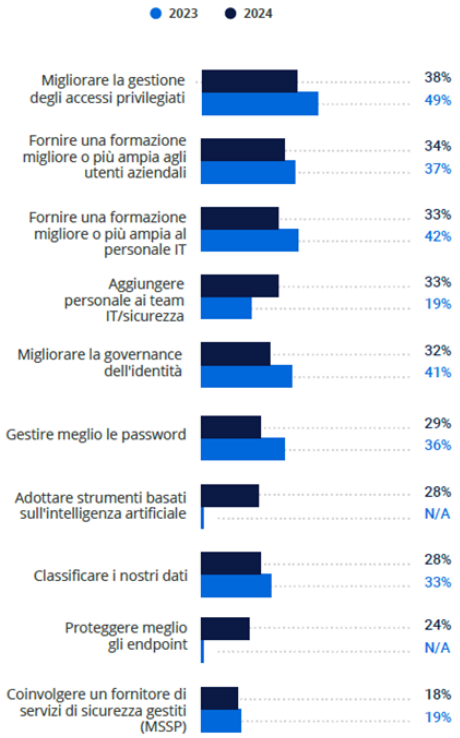
La classificazione dei dati resta la misura principale che le organizzazioni intendono aggiungere all'arsenale della loro sicurezza. Tuttavia, solo la metà l'ha effettivamente implementata. La sfida principale è rappresentata dallo sforzo richiesto dagli approcci manuali; e, in effetti, sono gli utenti aziendali a sapere quale tipo di informazioni sono contenute nei documenti che allegano a un'e-mail o trasferiscono in una posizione condivisa. Ma la classificazione manuale non è sostenibile su larga scala: richiede un enorme investimento di tempo, finendo per ostacolare la produttività degli utenti; e risulta altamente incoerente e soggetta all'errore umano. La classificazione automatizzata affronta queste sfide; ma bisogna tenere

presente che adattare i sistemi e i processi in modo da soddisfare i cambiamenti delle realtà aziendali e regolamentari richiede una stretta collaborazione tra i reparti.

LE PRIORITÀ DEI PROFESSIONISTI IT

Come l'anno scorso, abbiamo chiesto ai partecipanti al sondaggio quali miglioramenti avrebbero implementato se avessero potuto scegliere come migliorare la sicurezza della loro organizzazione. In cima alla lista c'è sempre il PAM, seguito dalla formazione per il personale IT e per gli utenti aziendali abituali. Tuttavia, l'interesse per altre misure di sicurezza è diminuito e risulta distribuito in modo più uniforme. È interessante notare che, nel 2024, il 33% dei partecipanti al sondaggio dichiara di voler aumentare il personale addetto all'IT/sicurezza, rispetto ad appena il 19% di un anno fa.

Misure di sicurezza informatica alle quali i professionisti IT darebbero priorità (2023, 2024)



"La crescita nell'adozione del cloud e la rapidità dei cambiamenti in quell'ambito rendono la carenza di personale un problema ogni anno più rilevante. È naturale che i professionisti IT, alla ricerca di soluzioni per gestire meglio i carichi di lavoro, valutino l'implementazione dell'intelligenza artificiale generativa e degli LLM (Large Language Model). Le aspettative, peraltro amplificate, in relazione a queste tecnologie devono ancora arrivare ai loro massimi, ma l'IA non sarà la soluzione a tutti i problemi. Le organizzazioni dovrebbero mantenere un atteggiamento pragmatico: le soluzioni basate sull'intelligenza artificiale possono rivelarsi utili in alcuni casi, ma non sostituiranno la necessità di una governance solida e di pratiche di sicurezza adeguate."
- ***Maurizio Taglioretti,*** *Regional Manager SEEUR, Netwrix*

Le priorità dell'IT in generale

Dato che nessuna organizzazione dispone di risorse umane e finanziarie illimitate, stabilire le priorità è fondamentale, anche per i team IT e di sicurezza. Abbiamo chiesto ai partecipanti al sondaggio quali fossero le priorità IT principali della loro organizzazione per il 2024, e abbiamo confrontato le loro risposte con quelle del 2020 (in pieno lockdown) e del 2023 (quando il lavoro da remoto e ibrido era diventato la nuova normalità).

Le aree problematiche principali sono rimaste le stesse: la sicurezza dei dati, la sicurezza di rete e la formazione sulla sicurezza informatica. L'interesse per l'implementazione di strumenti di intelligenza artificiale è aumentato, dal 12% dei partecipanti nel 2020 a ben il 28% nel 2024. Continua a crescere anche la percentuale di organizzazioni che danno priorità all'adozione del cloud, passata dal 23% nel 2020 al 32% nel 2023, per arrivare al 36% nel 2024.

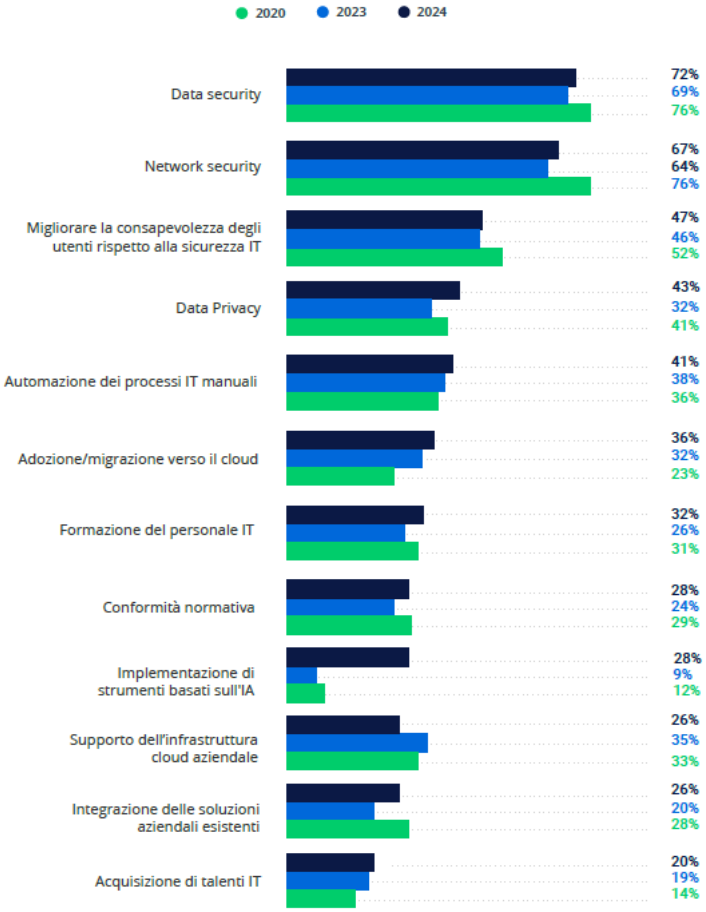
Commenti degli autori

Quando si prendono in considerazione soluzioni basate sull'IA, è essenziale partire da un obiettivo realistico: accelerare i processi aziendali senza compromettere la sicurezza. Per identificare i processi più adatti a essere automatizzati, è utile porsi alcune domande:

- *Il processo è ripetitivo e la sua esecuzione manuale richiede molto tempo?*
- *Il processo è ben definito, abbastanza da poter essere trasformato in un algoritmo?*
- *Il processo fornisce risultati verificabili che consentano di stabilire se qualcosa non va?*

Queste domande di screening sono utili per assicurare che l'intelligenza artificiale venga utilizzata per migliorare l'efficienza e la precisione dei processi, mantenendo comunque il controllo sui risultati.

Priorità IT dell'organizzazione (2020, 2023, 2024)



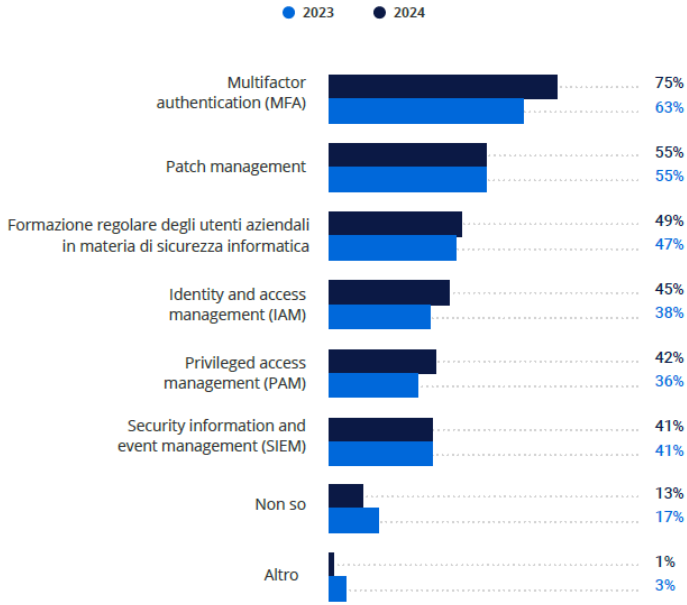
Le assicurazioni contro i rischi IT

Nessuna polizza contro i rischi informatici può recuperare i dati o ripristinare le operazioni di un'organizzazione dopo un incidente. Tuttavia, un risarcimento può alleviare l'impatto finanziario subito dall'azienda e, in alcuni casi, impedirne il fallimento. Si tratta di un approccio alla gestione del rischio piuttosto diffuso: il 43% delle organizzazioni ha stipulato una polizza e il 19% prevede di farlo entro i prossimi 12 mesi.

I requisiti degli assicuratori

Come l'anno scorso, abbiamo chiesto ai partecipanti al sondaggio che avevano stipulato un'assicurazione contro i rischi IT quali requisiti dovevano soddisfare per ottenere la polizza. Essenzialmente le risposte sono rimaste invariate ma, attualmente, le compagnie assicurative sembrerebbero più propense a richiedere sia la gestione dell'identità e degli accessi (IAM) sia la gestione degli accessi privilegiati (PAM). Inoltre, nel 2024 il 75% delle organizzazioni assicurate doveva aver implementato l'MFA, in aumento rispetto al 63% del 2023.

Quali requisiti ha dovuto soddisfare la tua organizzazione per ottenere l'emissione della polizza da parte della compagnia assicurativa? (2023, 2024)



Il 62% delle organizzazioni che hanno stipulato una polizza di assicurazione contro i rischi informatici o prevedono di stipularne una entro 12 mesi, in aumento rispetto al 59% del 2023.

Commenti degli autori

Se c'è una cosa di cui le compagnie assicurative sono esperte, è la gestione del rischio. Sanno bene che, prima o poi, attori con risorse e motivazione sufficienti riusciranno a penetrare in qualsiasi ambiente IT. Una soluzione PAM rende più difficile per gli autori di attacchi muoversi lateralmente nell'ambiente e incrementare i

privilegi, e garantisce che lasceranno più tracce. Tutto questo offre a chi si difende maggiori opportunità di rilevare gli attacchi e di rispondere in modo da prevenire perdite rilevanti: e minimizzare le perdite (ad esempio i risarcimenti) è esattamente l'obiettivo delle compagnie assicurative.

Le modifiche richieste per stipulare una polizza o ridurne il costo

Come nel 2023, quasi la metà (48%) delle organizzazioni ha dovuto apportare modifiche alla propria strategia di sicurezza per soddisfare i criteri previsti dalla polizza assicurativa desiderata. Tuttavia, un'analisi più dettagliata evidenzia che, nell'ultimo anno, le compagnie assicurative hanno inasprito i requisiti: la percentuale delle organizzazioni che hanno dovuto implementare misure di sicurezza aggiuntive solo per essere idonee a stipulare una polizza è aumentata dal 22% al 30%; inoltre, solo il 18% ha apportato queste modifiche per ridurre il premio assicurativo, in calo rispetto al 28% dell'anno scorso.

Avete apportato modifiche per soddisfare i requisiti di polizza? (2023, 2024)

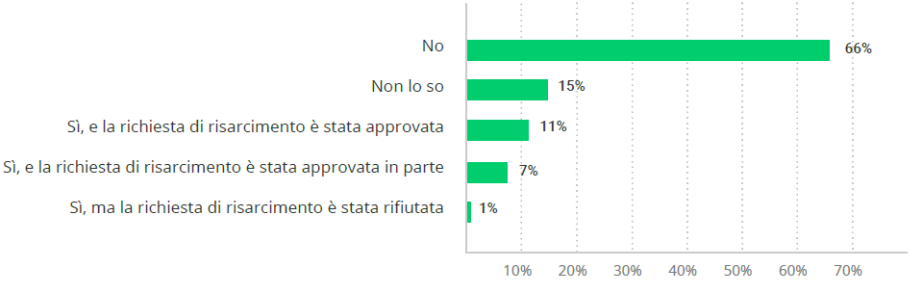
I controlli di sicurezza più efficaci sono quelli che corrispondono al percorso di attacco più comune. In primo luogo, gli autori di attacchi cercheranno di entrare nel sistema sfruttando le vulnerabilità o ricorrendo ad attacchi di phishing o basati su password, per acquisire le credenziali degli utenti. Per contrastarli, è importante disporre di una solida gestione delle password e dell'autenticazione multifattore (MFA).
Gli autori di attacchi che riescono a infiltrarsi nella rete tenteranno quindi di muoversi lateralmente e di compromettere le identità privilegiate: ecco perché anche il PAM deve essere una priorità. La fase finale dell'attacco consiste nel sottrarre i dati o danneggiare i sistemi; risultano quindi essenziali anche l'accesso protetto ai dati sensibili, nonché la disponibilità di funzionalità di backup e ripristino. - ***Dirk Schrader,*** *VP Security Research, Netwrix*

Le richieste di risarcimento

Non deve stupire che i requisiti per ottenere una polizza assicurativa contro i rischi informatici siano diventati più rigidi: la probabilità che un attacco informatico vada a buon fine e, di conseguenza, che venga presentata una richiesta di risarcimento è

elevata in modo preoccupante. Quasi un'organizzazione su 5 (19%), tra quelle assicurate, ha usufruito della propria polizza lo scorso anno.

La tua organizzazione ha usufruito della propria polizza contro i rischi informatici negli ultimi 12 mesi?



Commenti degli autori

I requisiti assicurativi e le normative sulla conformità rappresentano due fattori fondamentali nel determinare i livelli di riferimento per la sicurezza. Entrambi evolvono parallelamente ai progressi tecnologici e ai cambiamenti nel panorama delle minacce, ma le compagnie assicurative tendono a rispondere con maggiore rapidità e attenzione ai dettagli, adeguando i propri requisiti in tempi più brevi. Con l'emergere di megatrend tecnologici come l'informatica quantistica e l'intelligenza artificiale, che offrono nuove opportunità di attacco, è prevedibile che il settore delle assicurazioni informatiche introdurrà nuovi standard di controllo per la sicurezza.

Appendice. Osservazioni specifiche per il settore enterprise

L'adozione del Cloud

Le grandi aziende (con oltre 1.000 dipendenti) stanno migrando al cloud più rapidamente rispetto alle organizzazioni di minori dimensioni. Mentre, in media, il 74% dei partecipanti dichiara di avere un'infrastruttura ibrida, la percentuale è più alta per il settore enterprise (84%); e solo il 9% delle grandi imprese lavora esclusivamente on-premise, rispetto al 15% della media di mercato (**grafico 18**).

Le priorità IT

Le due priorità IT principali sono le stesse per le organizzazioni di tutte le dimensioni: sicurezza dei dati e sicurezza di rete. L'automazione dei processi IT manuali si posiziona al terzo posto per importanza nel settore enterprise: quasi la metà dei partecipanti al sondaggio (49%) l'ha indicata come una delle massime priorità per il 2024, a fronte del quinto posto per le organizzazioni in generale (**grafico 19**).

L'architettura IT nel settore Enterprise

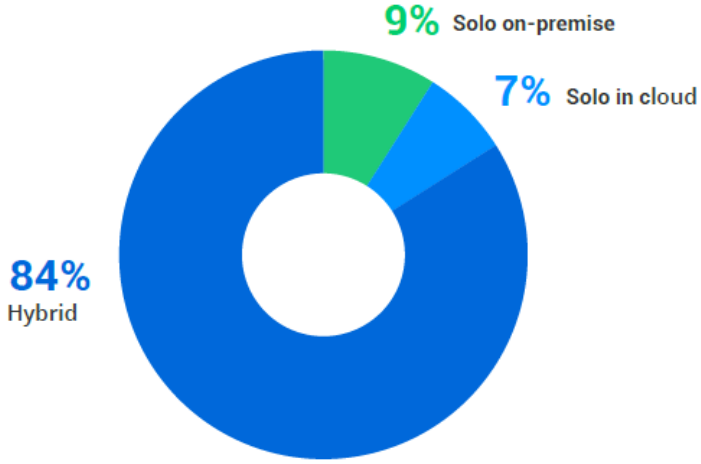


Grafico 18

Le priorità IT principali per il settore enterprise

Grafico 19

Commenti degli autori

Le soluzioni di sicurezza completamente automatizzate sono spesso viste come un obiettivo ideale. Ma cosa accade se questa automazione viene compromessa? Queste valutazioni devono essere integrate nei programmi aziendali di gestione del rischio. I rischi legati all'automazione potrebbero richiedere l'implementazione di nuove misure di mitigazione, ma anche i controlli esistenti, come l'accesso just-in-time o la revisione degli accessi, possono svolgere un ruolo significativo nel contenere questi rischi emergenti.

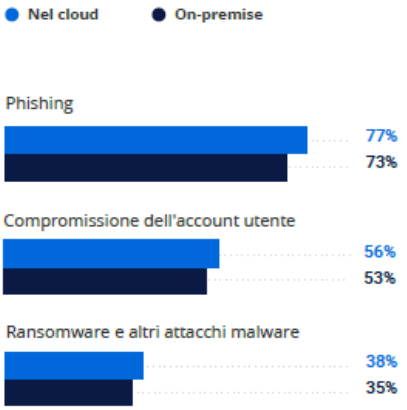
L'automazione può offrire vantaggi per una vasta gamma di attività svolte dai reparti IT e di sicurezza. In primo luogo, può facilitare l'implementazione del self-service per gli utenti senza compromettere la sicurezza, ad esempio quando agli utenti vengono concessi diritti di amministratore locale per i loro endpoint. In secondo luogo, i team

IT possono cercare di incrementare l'automazione della gestione del cloud e dei container e di migliorare l'analisi degli eventi di registro, in modo da automatizzare le risposte agli incidenti rilevati.

Gli incidenti di sicurezza

L'84% delle organizzazioni nel settore enterprise ha rilevato un attacco informatico negli ultimi 12 mesi, con un aumento rispetto al 65% del 2023. Inoltre, questa percentuale è superiore a quella relativa alle aziende di tutte le dimensioni per il 2024 (79%).

Incidenti di sicurezza più comuni nel settore enterprise

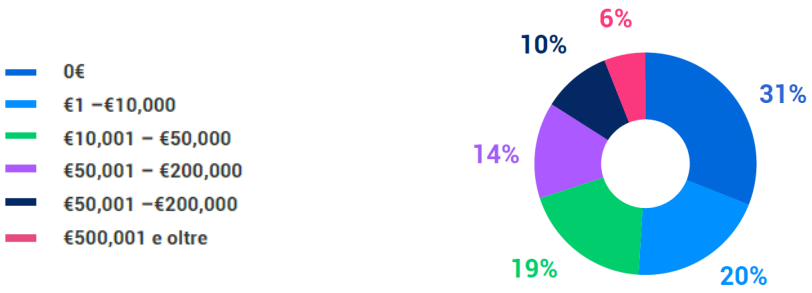


L'aumento degli attacchi contro le organizzazioni di tutte le dimensioni, incluso il segmento enterprise, potrebbe indicare che l'automazione basata sull'IA si è rivelata estremamente utile per gli attori delle minacce. Con l'avvento dell'intelligenza artificiale, inviare un numero massiccio di e-mail di phishing e sondare sistemi e servizi alla ricerca di vulnerabilità è diventata una semplice questione di orchestrazione sulle piattaforme gestite dai criminali informatici.
La pressione costante mette a dura prova i team di sicurezza e potrebbe portare a livelli di protezione ridotti o inefficaci. Per alleggerire questo peso, le organizzazioni dovrebbero valutare di coinvolgere investigatori esterni, come parte del loro piano di risposta agli incidenti. Questo aiuterà a sollevare il team di sicurezza interna dalla responsabilità di gestire gli attacchi in corso." - ***Dirk Schrader,*** *VP Security Research, Netwrix*

Il costo degli attacchi informatici

Per il 53% delle grandi imprese, un attacco informatico ha comportato spese extra impreviste per correggere le falle nella sicurezza, rispetto al 45% delle organizzazioni nel complesso. Un'azienda su cinque ha subito sanzioni per mancato rispetto delle norme (22%) e ha visto ridursi il suo vantaggio competitivo (21%). In effetti, tra le grandi imprese, ben il 30% stima di aver subito un danno finanziario derivante da minacce informatiche per almeno €50.000, rispetto ad appena il 17% delle organizzazioni nel complesso.

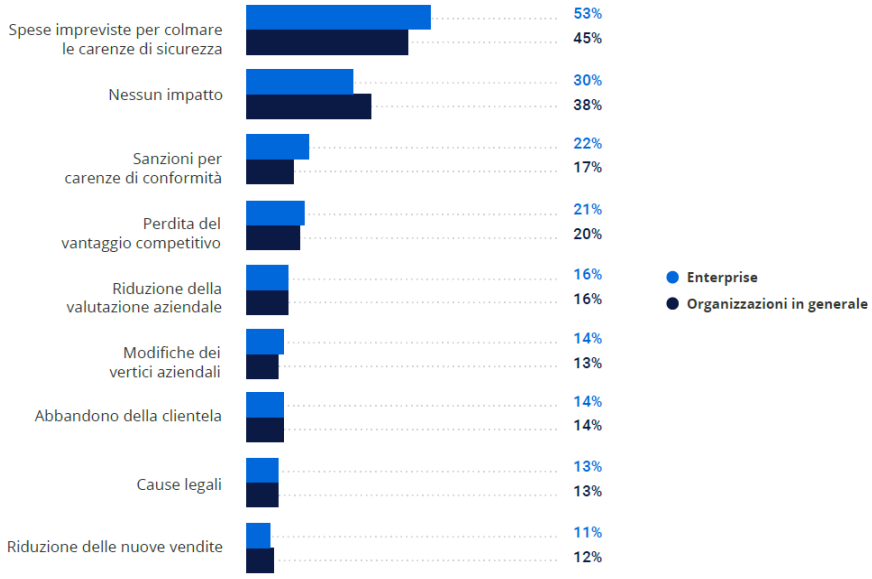
Stima dei danni finanziari causati dalle minacce informatiche alle grandi imprese



Commenti degli autori

I team di sicurezza di alto livello non si affidano solo ai controlli preventivi: stanno investendo in soluzioni di rilevamento e correzione come parte di una strategia di difesa stratificata, il che contribuisce all'aumento delle segnalazioni di incidenti. Inoltre, le aspettative del settore e delle entità nazionali in materia di trasparenza stanno cambiando, aumentando la visibilità della reale portata del problema.

Conseguenze degli attacchi informatici per le grandi imprese



Commenti degli autori

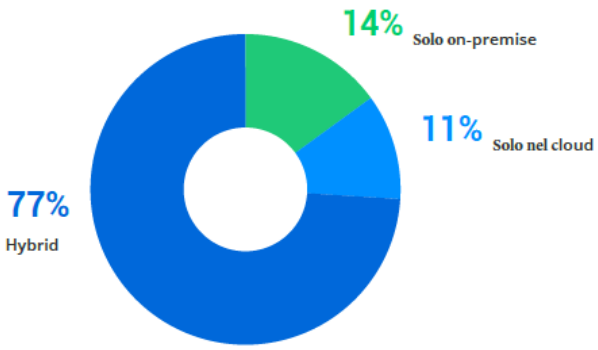
In genere, le grandi imprese hanno già implementato i controlli di sicurezza di base e, quindi, devono affrontare problemi più complessi e costosi successivamente a un attacco. Mentre un'organizzazione più piccola può optare per accettare alcuni rischi e adottare una soluzione rapida, le grandi imprese devono investire nel potenziamento del team di sicurezza, nell'adeguamento dei processi e nell'adozione di strumenti per colmare anche le più piccole vulnerabilità già sfruttate dagli autori di attacchi.

Osservazioni specifiche per il settore MSP (Managed Service Provider)

L'adozione del Cloud

I fornitori di servizi gestiti adottano le tecnologie cloud a un ritmo simile a quello del resto del mercato. Indicativamente 3 MSP su 4 dispone di un'architettura IT ibrida, e l'11% sono cloud-only.

L'architettura IT degli MSP



Le priorità IT

Come nel 2023, le principali priorità IT per il settore MSP sono la sicurezza dei dati e la sicurezza di rete, entrambe citate da 7 MSP su 10 (grafico 24).

Abbiamo anche chiesto ai partecipanti al sondaggio quali miglioramenti avrebbero implementato, se avessero potuto scegliere come migliorare la sicurezza della loro organizzazione: gli interventi più desiderati riguardano la formazione rivolta al personale IT e agli utenti abituali.

Sorprendentemente, l'implementazione di strumenti basati sull'IA si è classificata al secondo posto (mentre è solo al settimo negli altri settori).

Le priorità IT principali dell'organizzazione per gli MSP

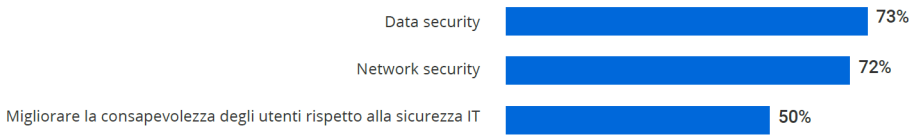
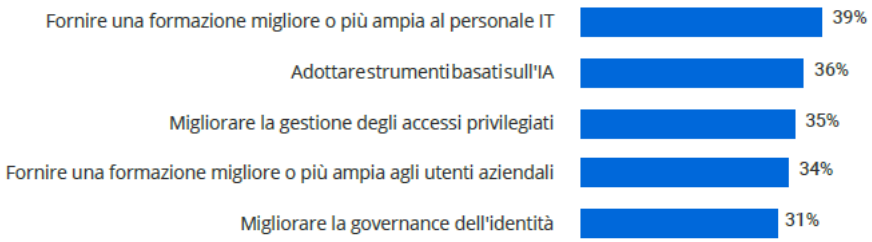


Grafico 24

Misure di sicurezza informatica prioritarie per i professionisti IT che lavorano per gli MSP



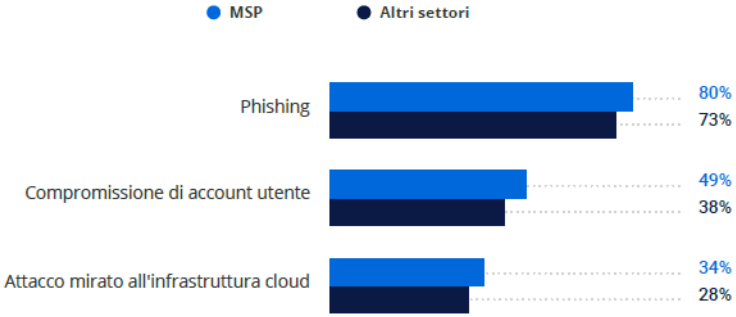
Commenti degli autori

La tecnologia basata sull'intelligenza artificiale offre agli MSP la possibilità di ottenere un risultato molto ambito: potenziare il talento delle persone, migliorando il servizio a costi ridotti e raggiungendo un numero maggiore di clienti. In ambienti IT complessi, una delle attività più dispendiose in termini di tempo è l'analisi dei segnali in ingresso. Delegare a strumenti di IA la gestione delle notifiche benigne, dei falsi positivi e degli schemi di attacco reali rappresenta una prospettiva interessante; ma solo il tempo dirà quando questo approccio diventerà realmente praticabile.

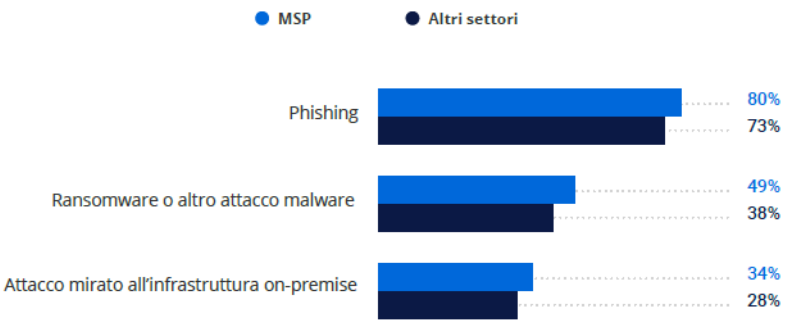
Gli incidenti di sicurezza

Il 76% degli MSP ha rilevato un attacco informatico contro la propria infrastruttura negli ultimi 12 mesi, una percentuale simile a quella delle organizzazioni in generale (79%). Per il settore MSP, un incidente nel cloud su due è stato associato alla compromissione degli account utente, mentre il 46% degli attacchi on-premise è stato di tipo ransomware (o altro attacco malware). Queste tipologie sono state invece meno comuni in altri settori.

Incidenti di sicurezza più comuni nel cloud per gli MSP



Incidenti di sicurezza più comuni on-premise per gli MSP



Commenti degli autori

MSP si affidano in larga misura a soluzioni SaaS (software-as-a-service), PaaS (platform-as-a-service) e IaaS (infrastructure-as-a-service). Queste soluzioni sono generalmente accessibili anche ai loro clienti, rendendo difficoltosa l'implementazione di limitazioni basate sulla rete, come i filtri degli indirizzi IP. Ecco, quindi, che gli autori di attacchi concentrano i loro sforzi su queste soluzioni basate sul cloud, che spesso risultano più vulnerabili e, una volta violate, consentono di ottenere le "chiavi" per accedere a numerosi ambiti diversi.

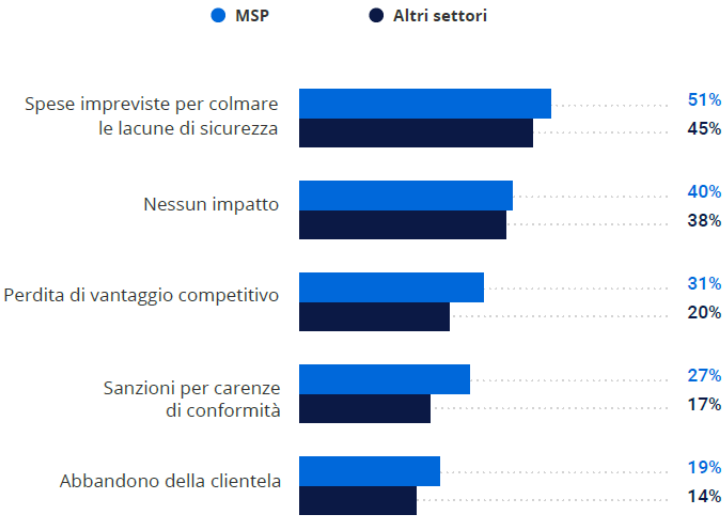
Il provider di servizi costituisce un bersaglio allettante per gli autori di attacchi ransomware. Da un lato, gli MSP difficilmente possono permettersi tempi di inattività, e saranno più propensi a cercare di ripristinare rapidamente le operazioni, il che aumenta le possibilità di un pagamento del riscatto. Dall'altro, compromettere un fornitore di servizi può essere solo il primo passo verso l'obiettivo finale: un attacco

alla supply chain. Gli MSP dovrebbero valutare adeguatamente i rischi e prendere le proprie decisioni in materia di sicurezza in base all'intelligence sulle minacce.

Le conseguenze degli attacchi informatici

Dal sondaggio emerge che il settore MSP subisce conseguenze dagli attacchi informatici con maggiore frequenza rispetto ad altri. Tra gli MSP oggetto di attacchi, uno su due (51%) ha dovuto affrontare spese impreviste per gestire le falle nella sicurezza; in aggiunta, il 31% ha subito una perdita di vantaggio competitivo e il 27% sanzioni per mancata conformità, rispetto al 20% e al 17% degli altri settori.

Le conseguenze degli attacchi informatici per gli MSP

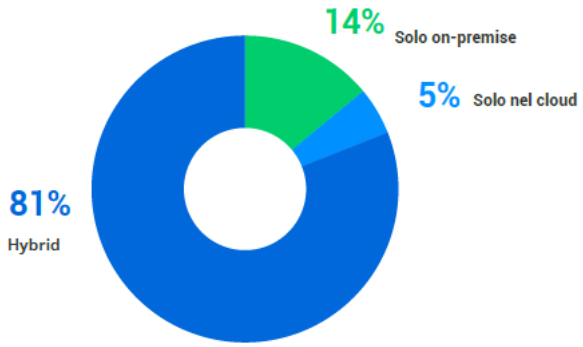


Osservazioni specifiche per il settore scolastico

L'adozione del cloud

L'81% degli istituti scolastici ha un'architettura IT ibrida, rispetto al 74% degli altri settori. Tra il 14% che opera esclusivamente on-premise, il 47% prevede di adottare tecnologie cloud in futuro.

L'architettura IT degli istituti scolastici



Security challenges

La metà degli istituti scolastici (51%) individua nella mancanza di risorse finanziarie la sfida principale per la sicurezza dei dati, seguita dagli errori e dalla negligenza degli utenti.

Le principali sfide per la sicurezza dei dati degli istituti scolastici

Commenti degli autori

Gli istituti universitari o i distretti scolastici possono avere un numero di account utente paragonabile a quello di alcune multinazionali globali: ma gli istituti scolastici, malgrado i loro ambienti dinamici possano avere lo stesso livello di complessità delle grandi organizzazioni, in genere non dispongono di budget e risorse sufficienti a gestirli adeguatamente. È fondamentale che i team di sicurezza IT nel settore dell'istruzione dispongano di processi e strumenti per gestire le identità, verificarne l'attività e monitorare eventuali comportamenti anomali o dannosi.

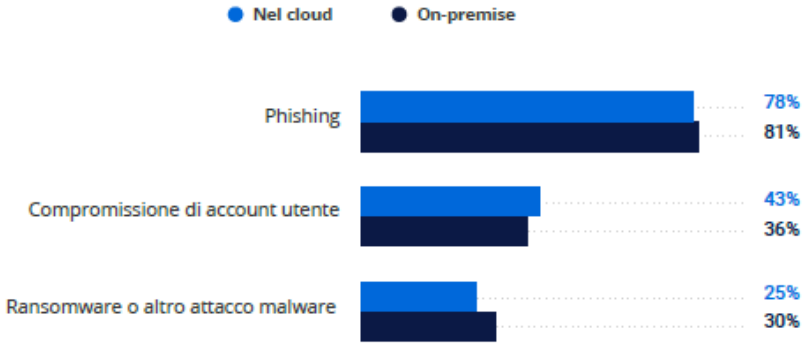
Per favorire la ricerca e la collaborazione compatibilmente con il budget a disposizione, gli istituti scolastici spesso forniscono agli utenti una serie di dispositivi e

sistemi condivisi esposti su Internet, generando una superficie di attacco enorme. Per mitigare il rischio, è fondamentale applicare policy avanzate relative alle password, che impediscano l'uso di password deboli e compromesse, ma anche implementare l'autenticazione multi fattore (MFA) e applicare il principio del privilegio minimo.

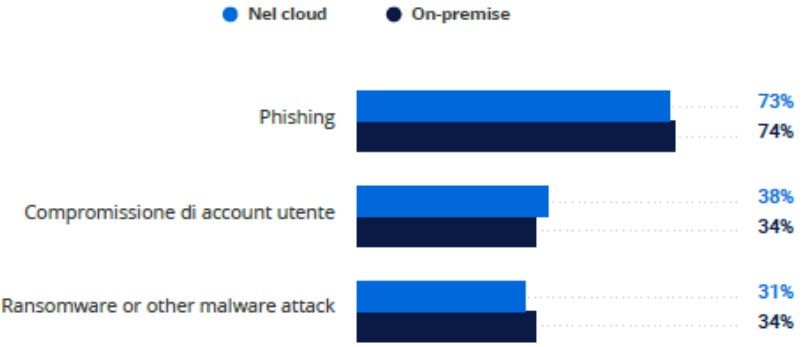
Gli incidenti di sicurezza

Il 77% delle organizzazioni nel settore scolastico ha rilevato un attacco informatico negli ultimi 12 mesi, con un aumento rispetto al 69% del 2023. I vettori di attacco più comuni sono simili a quelli riscontrati in altri settori: phishing, compromissione degli account utente e attacchi ransomware o con altri malware.

Gli incidenti di sicurezza più comuni nel settore scolastico



Gli incidenti di sicurezza più comuni negli altri settori



Commenti degli autori

Dato che molti servizi cloud vengono forniti agli istituti scolastici a prezzi scontati, è normale che il cloud venga utilizzato più di frequente in questo settore. L'utilizzo delle impostazioni di sicuzza predefinite, combinato con un elevato turnover delle identità cloud in uso, si traduce in una superficie di attacco più ampia e, quindi, in attacchi nel cloud più frequenti, rispetto agli altri settori oggetto del sondaggio.

Le conseguenze degli attacchi informatici

Quasi la metà (47%) delle organizzazioni scolastiche ha dovuto sostenere costi imprevisti per colmare le lacune di sicurezza emerse a seguito di un incidente. Inoltre, una su 7 ha subito sanzioni per non conformità, mentre una su 10 ha riportato come conseguenze azioni legali e avvicendamenti ai vertici dell'istituto.

Le conseguenze degli attacchi informatici per il settore scolastico

Un incidente può evidenziare lacune nella sicurezza, come privilegi amministrativi eccessivi, account inattivi, password deboli o mai aggiornate, password o configurazioni predefinite e sistemi privi di patch, tutte dovuti a negligenza o mancanza di conoscenze. Colmare queste lacune non implica necessariamente e immediatamente un esborso in denaro, ma richiede sicuramente un impegno in termini di tempo al team di sicurezza IT. In altre parole, gestire la causa principale di un incidente di sicurezza comporta un investimento aggiuntivo, in termini di denaro o di sforzi.

In seguito a una violazione, le organizzazioni devono dare priorità alle misure di ripristino per ridurre i rischi futuri. Ad esempio, una risposta immediata potrebbe includere l'applicazione di patch al software sui server più critici e l'aggiunta di una fase di revisione manuale su determinate operazioni. Per una correzione a lungo termine, potrebbe essere necessario attendere il successivo ciclo di bilancio, acquisendo software, servizi o personale aggiuntivi.

Informazioni sul report

Questo report è prodotto dal Netwrix Research Lab, che realizza sondaggi mirati tra professionisti IT a livello globale per analizzare i cambiamenti e le tendenze più significative nel settore.

Altri report sono disponibili all'indirizzo https://www.netwrix.com/netwrix_researches_for_it_pros.html

Guida Pratica alla Cloud Threat Detection, Investigation e Response

(A cura di Ivan Tresoldi, Wiz)

Introduzione

La **sicurezza nel Cloud** rappresenta oggi una sfida di primaria importanza per le aziende di qualsiasi settore. Le organizzazioni moderne, spinte dall'innovazione e dall'esigenza di maggiore agilità, hanno trasferito una quota significativa dei propri servizi, infrastrutture e applicazioni all'interno di ambienti Cloud (pubblici, privati o ibridi). Questa migrazione promette enormi vantaggi in termini di scalabilità, velocità di sviluppo e flessibilità, ma introduce anche **nuove complessità e rischi** dal punto di vista della sicurezza.

In teoria, la disponibilità di **telemetria dettagliata** (ad esempio i log generati dagli ambienti Cloud, le chiamate API ai vari servizi, i tracciamenti di rete, i metadati sui container e così via) consentirebbe ai team di sicurezza di ottenere una **visibilità senza precedenti** sull'intero sistema. In pratica, però, trasformare questa potenziale "miniera d'oro" di dati in un programma di sicurezza operativo — in grado di rilevare e bloccare le minacce in tempo reale — si è rivelato un compito molto più arduo.

Una delle ragioni principali di questa difficoltà è che gli **strumenti di sicurezza tradizionali**, come i SIEM (Security Information and Event Management) e gli EDR (Endpoint Detection and Response), non sono stati concepiti per gli **scenari Cloud-native**, dove esistono centinaia di servizi, entità effimere che nascono e muoiono in pochi minuti, e architetture distribuite con confini di rete molto più sfumati rispetto all'on-premises. Ne conseguono **sfide** come:

- l'ottenimento di **visibilità centralizzata e in tempo reale** su una grande mole di dati, con costi non sempre sostenibili;
- il **rilevamento** di minacce che si muovono tra workload, identità e dati in modo rapido e dinamico;
- l'**investigazione** di alert e la ricerca di root cause in ambienti in continua evoluzione e con configurazioni spesso complesse;
- **l'azione di risposta** immediata (containment), in modo da isolare e bloccare rapidamente le minacce, senza interrompere le attività di produzione o provocare downtime indesiderato.

Mai come nell'ambito della Detection and Response nel Cloud, il termine "evolving threat landscape", che solitamente potrebbe risultare più una frase fatta e un "marketing claim" che una minaccia reale, appare invece assolutamente fondato. Man mano che la presenza nel Cloud aumenta, anche le minacce si spostano, e la superficie d'attacco cambia a sua volta, radicalmente e costantemente. A complicare ulteriormente le cose, l'utilizzo dei servizi Cloud è spesso affidato a gruppi differenti, costringendo il SOC a collaborare più che mai con tutto il resto dell'organizzazione.

Da questa esigenza è emersa la **Cloud Detection and Response** (CDR), un insieme di soluzioni e funzionalità che portano la mentalità "assume breach" nel mondo del Cloud. Con "**assume breach**" si intende un approccio secondo cui gli operatori di sicurezza partono dal presupposto che, prima o poi, un attacco andrà a buon fine, e dunque strutturano processi, strumenti e competenze per **rilevare, investigare e contenere** rapidamente qualsiasi compromissione.

Questo articolo si pone l'obiettivo di illustrare i concetti fondamentali della CDR, spiegare perché gli strumenti preesistenti non sono più sufficienti a coprire i casi d'uso tipici del Cloud, e come una piattaforma di Cloud Detection and Response possa integrarsi nel flusso di lavoro dei gruppi di sicurezza, portando benefici reali all'intera organizzazione e riducendo il **Mean Time to Detect (MTTD)** e il **Mean Time to Respond (MTTR)**.

Ottimi spunti di osservazione sulle possibili minacce derivanti dall'utilizzo del Public Cloud sono sicuramente MITRE ATT&CK, che offre un framework completo per determinare quali tecniche, tattiche, procedure (TTP) si applicano al Cloud pubblico. La Cloud Security Alliance, invece, pubblica ogni anno l'elenco delle undici principali minacce per la sicurezza nel Cloud.

Che cos'è la Cloud Detection and Response (CDR)?

La **Cloud Detection and Response** nasce per fornire ai team di SecOps — in particolare SOC (Security Operations Center) e IR (Incident Response) — le capacità di cui hanno bisogno per monitorare, individuare e bloccare attacchi **specifici per il Cloud**. In molte aziende, la responsabilità di Detection & Response ricade appunto sui **SOC** o su un centro operativo di sicurezza che si occupa anche di Incident Response. Gli analisti del SOC sono chiamati quotidianamente a:

- **rilevare** comportamenti malevoli e indicatori di compromissione (IoC) in tempo reale;
- **indagare** a fondo sulle segnalazioni (alert), distinguendo i falsi positivi dalle vere minacce e comprendendo cause e impatto di un eventuale incidente;

- **rispondere** in modo rapido e coordinato, impedendo all'attaccante di propagarsi o di causare danni peggiori.

Fino a poco tempo fa, buona parte delle attività di rilevamento e risposta si basava solo su strumenti come i SIEM (per la raccolta centralizzata dei log e la correlazione degli eventi) e gli EDR (per la protezione degli endpoint). Tuttavia, il **Cloud introduce molte peculiarità**: entità che non sono semplici endpoint (ad esempio funzioni serverless, container in cluster Kubernetes, identità e ruoli IAM), control plane e infrastruttura di rete più complessi da difendere, e una **molteplicità di sorgenti di log** che possono risultare complicate da gestire.

Le soluzioni di CDR hanno dunque lo scopo di **automatizzare e semplificare** queste operazioni nel contesto Cloud, in modo da fornire:

- **visibilità e telemetria** dettagliata sull'intero ambiente, anche in ottica multi-Cloud;
- **rilevamento** real-time di eventi sospetti o potenzialmente malevoli, basato su regole, analisi comportamentale e anomaly detection applicata a componenti Cloud specifici;
- **investigazione** e triage efficaci, con interfacce intuitive che permettono di correlare rapidamente entità, log di rete, ruoli IAM, permessi, azioni passate e altro ancora;
- **risposta e contenimento** rapidi, tramite la possibilità di intervenire sul Control Plane del Cloud (ad esempio modificando policy, security group o privilegi assegnati a un'identità) per isolare e neutralizzare la minaccia.

È da sottolineare che, accanto al termine CDR, sta emergendo anche la definizione di **CIRA (Cloud Investigation and Response Automation)**. Questo sottolinea l'importanza dell'automazione e dell'integrazione con pipeline di incident response che possano avvenire senza intervento manuale o, perlomeno, con intervento minimo.

Perché serve una soluzione di Cloud Detection and Response?

Come il Cloud è diverso: prospettiva dell'attaccante

L'aumento dell'adozione del Cloud da parte delle aziende non è passato inosservato ai **malintenzionati**. Se un tempo i criminali informatici si concentravano principalmente sul perimetro di rete on-premises e sulla compromissione di endpoint tradizionali (PC, server fisici), oggi spostano sempre più il mirino verso:

- **servizi esposti pubblicamente**: nel Cloud, molte componenti sono raggiun-

gibili tramite Internet, ed è molto più facile per un attaccante effettuare una scansione automatica e individuare asset potenzialmente vulnerabili (sia a livello di configurazioni, sia a livello di software);
- **velocità di propagazione**: l'automazione e le API Cloud consentono agli aggressori di muoversi rapidamente, ricorrendo a tecniche automatizzate per la scansione e lo sfruttamento di vulnerabilità note;
- **accesso altamente privilegiato tramite il control plane**: se un attaccante riesce a compromettere le credenziali (ad esempio token IAM) o a sfruttare una configurazione errata del Control Plane del Cloud, può ottenere privilegi elevati e addirittura "cambiare" l'infrastruttura a proprio vantaggio (creando nuove macchine, disabilitando log, aprendo flussi di rete).

Episodi celebri come le violazioni di Capital One, Uber, CircleCI e Ubiquiti hanno evidenziato come errori di configurazione, gestione impropria delle chiavi di accesso o exploit su componenti Cloud possano portare a incidenti gravi, con furto di grandi quantità di dati o interruzioni di servizio.

L'**iperconnettività** del Cloud diventa un'arma a doppio taglio: se da un lato abilita la produttività e l'agilità, dall'altro facilita la ricognizione e il movimento laterale all'interno dell'infrastruttura.

Come il Cloud è diverso: prospettiva del difensore

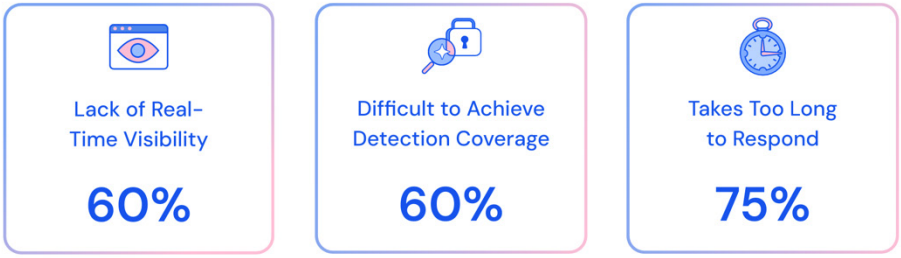
Dal punto di vista dei team di sicurezza, il Cloud comporta uno scenario radicalmente nuovo:

- **esplosione delle entità**: centinaia di servizi su più provider (AWS, Azure, GCP, ecc.), migliaia di container che vivono per pochi minuti, ruoli e identità IAM di servizio, innumerevoli tipi di risorse (funzioni serverless, bucket di storage, reti virtuali, API gateway, database gestiti, e così via). Gestire e monitorare questa mole di elementi è complesso;
- **carichi di lavoro effimeri**: un container che vive qualche ora per elaborare un job può sparire prima che ci si accorga di un'eventuale compromissione. Questo rende difficile eseguire analisi forensi tradizionali o conservare le tracce dell'incidente;
- **architetture in continuo cambiamento**: le pipeline DevOps o DevSecOps favoriscono un rilascio rapido di nuove versioni dell'applicazione o dell'infrastruttura. Aggiornamenti frequenti significano topologie di rete dinamiche, configurazioni che mutano, nuovi servizi che si aggiungono o si spostano. Un SOC che fatica ad avere visione completa potrebbe non rendersi conto di un attacco in corso se non è attrezzato con strumenti adeguati.

Evidenze dal campo

Le difficoltà sopra descritte non sono soltanto teoriche. Nel corso di un'indagine condotta da Wiz su **oltre 200 CISO e responsabili di sicurezza di più di 150 aziende**, sono emersi alcuni punti rilevanti che confermano la complessità dell'argomento:

- **oltre il 60%** delle organizzazioni intervistate ha dichiarato di non avere una **visibilità centralizzata e in tempo reale** sul proprio ambiente Cloud;
- **oltre il 60%** sottolinea di avere **carenze nelle capacità di rilevamento** (detection coverage) per gli scenari Cloud. Molte minacce restano "invisibili" a causa di log incompleti, alert rumorosi e mancanza di competenze di Cloud detection engineering;
- **più del 75%** lamenta difficoltà e tempi troppo lunghi nella fase di **risposta** a un attacco (troppo alto il valore di "Mean Time to Respond"), spesso dovuti a carenza di contesto e a processi manuali di triage che rallentano l'isolamento delle minacce.



Un altro elemento di criticità emerso è il **divario di competenze** (skills gap). Molte aziende hanno formato i propri security analyst su scenari on-premises e faticano a trovare professionisti che conoscano a fondo i servizi e le logiche Cloud-native. La rapida migrazione di molte applicazioni e workload in ambiente Cloud ha creato un deficit di know-how che espone le aziende a rischi operativi e di sicurezza.

Perché gli strumenti SecOps tradizionali e le soluzioni Cloud attuali non bastano

Le soluzioni di **Cloud Detection and Response** nascono proprio per coprire le lacune di strumenti general-purpose come SIEM, SOAR, XDR o EDR, che sono stati pensati inizialmente per contesti on-premises o per proteggere endpoint "classici" (desktop, laptop, server fisici). Nel Cloud, molte di queste soluzioni risultano:

1. **difficili da integrare** a livello di telemetria: i SIEM tradizionali si basano su un modello di raccolta e analisi di log generici, spesso con licenze basate sul volume dei dati. Nel Cloud, il volume di log può esplodere. Senza un approccio "intelligente" alla raccolta (ad esempio saper filtrare e correlare log in tempo reale, oppure gestire i costi), si rischia di pagare cifre esorbitanti o di non abilitare le fonti di log più critiche per risparmiare;
2. **non specializzati su entità Cloud-native**: serverless, Kubernetes, ruoli IAM, piani di controllo CSP (Cloud Service Provider) sono concetti che non esistevano in modo rilevante nell'era on-premises. Un sistema EDR tradizionale potrebbe non "vedere" una funzione Lambda o un bucket S3 che trasmette dati anomali, se non è stato appositamente integrato;
3. **generare alert poco precisi**: la mancanza di contestualizzazione Cloud fa sì che le piattaforme tradizionali possano produrre segnalazioni rumorose (false positive) o, peggio, non segnalino comportamenti effettivamente anomali. In un ambiente Cloud, "anomalie" possono variare di continuo (pensiamo a picchi di traffico su un container che viene scalato automaticamente);
4. **proporre tempi di risposta eccessivi**: in un mondo in cui un container esiste per pochi minuti, attendere che un analista SIEM collezioni manualmente i log, effettui query e ricostruisca la sequenza di eventi può far perdere la finestra critica per bloccare un attaccante.

Anche le soluzioni **native dei provider Cloud** potrebbero risultare incomplete se l'azienda utilizzasse più Cloud contemporaneamente (approccio multi-Cloud) o se i meccanismi di rilevamento fossero troppo generici e non producano alert azionabili. Inoltre, i servizi CSP-nativi si concentrano tipicamente sul singolo Cloud, mentre molte aziende adottano almeno due piattaforme Cloud ed hanno quindi necessità di unificare la vista su tutti gli ambienti, al fine di avere un quadro completo.

La conseguenza di queste limitazioni è che il **Mean Time to Detect (MTTD)** e il **Mean Time to Respond (MTTR)** possono aumentare notevolmente, esponendo l'azienda a una superficie di attacco più ampia e a tempi di reazione insufficienti.

Come la Cloud Detection and Response apporta benefici al business

Implementare una soluzione di CDR concepita appositamente per il Cloud può portare **benefici tangibili** su diversi fronti:

1. **visibilità in tempo reale e centralizzata**: grazie a un'**automazione intelligente** della raccolta e della correlazione dei log provenienti dalle API dei CSP, i

team di sicurezza possono disporre di una mappa aggiornata dell'infrastruttura e dei relativi eventi sospetti. Questa visibilità non richiede l'installazione di agenti su ogni risorsa, poiché il Cloud consente di sfruttare le API esistenti;

2. **copertura di rilevamento più completa**: una piattaforma CDR copre **identità, dati, network e compute plane**. Rispetto ai tradizionali EDR o CWPP (Cloud Workload Protection Platform), che si focalizzano solo sul workload, la CDR estende il monitoraggio a tutti i piani di servizio (ad esempio azioni sul Control Plane del Cloud, modifiche a ruoli IAM, attività anomale su bucket di storage);
3. **riduzione del MTTR**: la CDR fornisce informazioni contestualizzate e pronte all'uso, per cui un analista SOC non deve più passare ore a incrociare dati da fonti disparate. Per esempio, se un alert segnala un tentativo di escalation di privilegi su una macchina virtuale, la piattaforma mostrerà la cronologia dei log di audit del Cloud control plane relativamente a quella macchina, l'identità che ha lanciato l'azione, le relazioni di rete con altri componenti e così via. Questo accorcia sensibilmente i tempi di triage;
4. **eliminazione di overhead operativi**: invece di scrivere regole manuali o query per ogni scenario, la CDR offre una **libreria di rilevamenti specifici** per il Cloud, spesso arricchita da meccanismi di anomaly detection. Gli aggiornamenti vengono forniti dal vendor, e i team di sicurezza non devono più essere chiamati a "reinventare la ruota";
5. **riduzione dei costi**: molte soluzioni CDR prevedono un modello di pricing basato sugli asset monitorati o su risorse effettivamente analizzate in tempo reale, evitando i costi esplosivi di un SIEM che cresce in base ai TB di log ingeriti. Inoltre, la capacità di pre-filtrare ed elaborare i log in maniera intelligente (anziché acquisirli tutti indistintamente) porta spesso a un risparmio notevole.

In ultima analisi, **l'impatto sul business** è duplice: da un lato, la riduzione dei rischi e dei possibili danni reputazionali o economici dovuti a una violazione; dall'altro, un incremento dell'efficienza dei processi, che consente ai team di sicurezza e sviluppo di continuare a **sfruttare a pieno** le potenzialità del Cloud.

Come la CDR si integra nei flussi operativi di SecOps e con le CNAPP

Integrazione con i flussi SecOps

Nel flusso di lavoro di un SOC, l'adozione di una **soluzione EDR** sugli endpoint on-premises è ormai da anni lo standard. L'EDR raccoglie i dati dai dispositivi, applica logiche di rilevamento specifiche, genera alert che poi vengono inviati al SIEM o

al SOAR, dove gli analisti effettuano triage, e infine permette di isolare le macchine compromesse con un clic.

La **CDR** agisce come **"l'equivalente" dell'EDR per il Cloud**. Intercetta e processa i dati generati dalle risorse Cloud (CSP audit log, flow log di rete, log di servizi specifici come S3, CloudTrail, VPC Network Flow, Azure Activity Log, ecc.) per rilevare pattern pericolosi, invia alert e fornisce strumenti integrati per investigare e rispondere. I team operano, di conseguenza:

1. **monitorando** l'interfaccia della CDR (o le notifiche inviate a un SIEM/SOAR) alla ricerca di nuovi alert;
2. **tornando** alla piattaforma CDR per svolgere analisi approfondite (ad esempio, una visualizzazione grafica di tutte le relazioni tra un container compromesso e i bucket S3 a cui accede);
3. **attivando** azioni di containment direttamente dalla piattaforma CDR, come modificare un security group per bloccare il traffico, o revocare temporaneamente le credenziali di un utente.

Integrazione con CNAPP

Oltre alla CDR, negli ultimi anni si è sviluppato il concetto di **CNAPP (Cloud-Native Application Protection Platform**), una categoria di soluzioni che riunisce diverse funzionalità di sicurezza in un'unica piattaforma, tra cui:

- **CSPM (Cloud Security Posture Management)**: analisi e correzione delle configurazioni errate nel Cloud;
- **CIEM (Cloud Infrastructure Entitlement Management)**: gestione centralizzata e analisi dei privilegi e delle identità;
- **IaC scanning**: scansione del codice infrastrutturale (ad esempio Terraform, CloudFormation) per prevenire misconfigurazioni;
- **Container e workload security**: analisi delle vulnerabilità e dei runtime containerizzati;
- **Data Security Posture Management**: individuazione e protezione dei dati sensibili;
- **AI-SPM**: governo della postura di sicurezza dei servizi e tecnologie in ambito AI/ML;
- **DSPM (Data Security Posture Management)**: individuazione e protezione dei dati sensibili.

La **CDR** si pone in modo **complementare** rispetto al CNAPP. Mentre quest'ultimo punta a migliorare la **postura di sicurezza** (proattiva, "left-of-boom"), la CDR mira

a intervenire in modo reattivo, "**right-of-boom**", quando la minaccia è già in atto. L'integrazione tra CDR e CNAPP consente:

- alla CDR di **utilizzare i risultati** di posture management (come la presenza di vulnerabilità critiche, configurazioni esposte o attack path identificati) per **dare priorità** agli alert o perfezionare il rilevamento;
- al CNAPP di **agire** dopo che la CDR ha isolato una minaccia, fornendo strumenti di correzione definitiva (remediation) sulla configurazione, sulle pipeline DevOps o sugli IaC template in uso.

In tal modo, l'azienda può mettere in atto un **ciclo di miglioramento continuo**:

1. il CNAPP individua le configurazioni a rischio e offre suggerimenti di correzione;
2. la CDR monitora in tempo reale e interviene se un attaccante tenta di sfruttare quelle lacune di sicurezza;
3. una volta contenuto l'attacco, si ritorna nel CNAPP per risolvere il problema alla radice, impedendo che lo stesso vettore venga sfruttato in futuro.

Capacità fondamentali degli strumenti di Cloud Detection & Response

Per implementare correttamente la Detection, Investigation & Response in ambiente Cloud, gli **strumenti di CDR** dovrebbero offrire un ventaglio di funzionalità sufficientemente **ampio e integrato**. Nel dettaglio, sono quattro i **pilastri fondamentali** da prendere in considerazione:

1. **monitoraggio della telemetria e analisi della visibilità**
2. **rilevamento completo progettato per il Cloud**
3. **interfaccia intuitiva per il triage**
4. **funzionalità di containment**

1. Monitoraggio della telemetria e analisi della visibilità

Un requisito essenziale è la **capacità di raccogliere e analizzare** in modo **scalabile e automatico** la telemetria disponibile nel Cloud. In uno scenario multi-Cloud, ciò significa tipicamente ingaggiare le API native dei provider (AWS, Azure, GCP, ecc.) per rilevare:

- **Cloud Audit Logs** (ad esempio AWS CloudTrail, Azure Activity Log, GCP Audit Logging) che tracciano le azioni sul Control Plane del Cloud, come la creazione di nuovi servizi, la modifica di policy, le chiamate ai servizi di gestione delle identità, e così via;
- **Flow Log** di rete per visualizzare il traffico in entrata e in uscita, rilevando pattern anomali o spostamenti laterali;

- **Data event logs** (ad esempio S3 Data Events, accessi agli Storage Account in Azure ecc.) per monitorare chi accede a dati sensibili, come e quando;
- **Service level logs** (ad esempio key vault logs, load balancer logs, database gestiti) che forniscono dettagli sul funzionamento specifico di certi servizi Cloud;
- **Sensor telemetry** da workload (container, VM): qui entrano in gioco agent o soluzioni agentless (dipende dall'architettura) per raccogliere informazioni di runtime su processi, file system, chiamate di rete, e altre attività potenzialmente malevole all'interno del workload.

La piattaforma CDR dovrà **normalizzare** e **correlare** queste fonti di dati, costruendo una vista coerente su ciò che sta succedendo nell'ambiente Cloud. In assenza di uno strato di normalizzazione, un SOC dovrebbe gestire manualmente formati di log diversi, le differenze tra i vari CSP, e volumi di dati potenzialmente enormi.

2. Rilevamento completo progettato per il Cloud

Per ridurre i carichi di lavoro manuali e il rumore generato da alert irrilevanti, una **soluzione CDR** dovrebbe:

1. **supportare nativamente** le entità e i servizi Cloud: deve capire cosa sia un "AWS Lambda", un "Azure Function", un "GCP IAM role", un "container in un cluster Kubernetes EKS", e così via;
2. **applicare regole mirate** su questi servizi, combinando **tecniche di rilevamento basate su regole** (indicatori di compromissione noti, firme di attacchi) e **approcci di anomaly detection** (rilevamento di comportamenti inusuali in base allo storico o a pattern appresi);
3. **integrare più segnali** prima di generare un alert, in modo da aumentare la precisione (ridurre falsi positivi). Ad esempio, combinare l'analisi di log CloudTrail (azione anomala su IAM), con i log di rete (connessione SSH sospetta) e i metadati di configurazione (ruolo con permessi eccessivi);
4. **fornire spiegazioni e contesto**: se si basa su anomaly detection, deve rendere comprensibile all'analista il perché un determinato comportamento venga giudicato sospetto.

Senza queste caratteristiche, correremmo il rischio di ricevere avvisi poco azionabili, che richiederebbero investigazioni lunghissime per capire se si tratti realmente di una minaccia o meno.

3. Interfaccia intuitiva per il triage

La fase di **investigazione** è spesso l'anello più debole della catena, perché:

- gli analisti SOC devono raccogliere molte informazioni da fonti diverse (log di Identity Provider, log di CNAPP, big data repository, portali dei provider Cloud, e così via);
- in un attacco reale, il tempo è critico: più si ritarda nel capire la portata di un incidente, più si rischia che l'attaccante compia ulteriori danni (esfiltrazione di dati, persistenza, sabotaggio ecc.)

Una **piattaforma CDR** di qualità dovrebbe **aggregare e visualizzare** in modo chiaro tutti i dati utili. Ad esempio, quando scatta un alert, l'analista deve poter vedere a colpo d'occhio:

1. **Chi** ha effettuato l'azione sospetta (utente, ruolo IAM, chiave di accesso)?
2. **Quale** risorsa è coinvolta (macchina GCE, cluster AKS, bucket S3, credenziali, account di storage)?
3. **Da dove** proviene la richiesta (IP esterno, rete interna, paese, servizio)?
4. **Quando** è iniziata l'attività anomala e qual è la sequenza di eventi?

Inoltre, può rivelarsi fondamentale l'integrazione con **Identity Provider** (ad es. Okta, Ping, ecc.), con **CI/CD** (GitHub, CircleCI, Jenkins ecc.) e con **ticketing system** (Jira, ServiceNow ecc.). Questi dati forniscono un contesto aggiuntivo: per esempio, se l'attività sospetta proviene da un account che di recente ha subito un reset password, oppure se un utente in un altro fuso orario ha approvato un commit nel repository e subito dopo avvia operazioni anomale sul Cloud.

4. Funzionalità di containment

Una volta appurato che un incidente è reale ed è in corso, la **priorità** sarà contenere la minaccia prima che si espanda. Nel mondo on-premises o endpoint, la manovra classica è isolare la macchina dalla rete. Nel Cloud, si possono adottare contromisure come:

- **bloccare** o **restringere** i permessi di un ruolo IAM;
- **revocare** o **ruotare** chiavi di accesso;
- **modificare** le regole di un security group per interrompere il traffico;
- **sospendere** o **arrestare** una risorsa compromessa.

Tuttavia, queste azioni sono più delicate: cambiare una policy in modo errato potrebbe bloccare l'intero servizio di produzione, causando downtime e perdite economiche. Di conseguenza, è fondamentale che la **piattaforma CDR** offra **workflow di containment sicuri** e possibilmente *testati*, guidando l'analista o automatizzando le mosse iniziali più urgenti (ad esempio la quarantena di un container). Il tempo risparmiato con un containment istantaneo può fare la differenza tra un piccolo incidente

e un disastro conclamato.

Ulteriori caratteristiche chiave

Oltre alle quattro funzionalità principali, esistono altre caratteristiche che possono trasformare un prodotto di CDR in uno **strumento realmente completo**:

1. **detection "pre-tarate"** e regolarmente aggiornate: la piattaforma dovrebbe fornire regole pronte all'uso per le minacce più comuni in ambiente Cloud, riducendo il bisogno di scrivere o manutenere regole proprietarie. Allo stesso tempo, deve permettere di personalizzare le policy e di creare regole ad hoc;
2. **copertura multi-Cloud**: le aziende che usano AWS, Azure, GCP (o altri provider) hanno bisogno di una soluzione unificata che normalizzi i dati e applichi le stesse logiche di rilevamento in tutti gli ambienti, evitando "zone buie";
3. **integrazione con contesti esterni**: come citato, la piattaforma dovrebbe saper dialogare con Identity Provider, soluzioni CNAPP, DSPM (Data Security Posture Management), e avere connettori verso i più comuni SIEM e SOAR;
4. **automazione della risposta**: se l'azienda ha implementato pipeline di automazione (per esempio con SOAR), la CDR deve poter fornire PlayBook e API per orchestrare azioni di containment, recupero evidenze forensi e altre misure di emergenza in modo automatico o semi-automatico.

Considerazioni finali e prospettive per il futuro

La sicurezza nel Cloud non si risolve più soltanto con soluzioni perimetrali o con l'adozione di un SIEM che raccoglie tutto e genera report. Oggi, gli **attacchi Cloud-native** sfruttano configurazioni errate, identità mal gestite, errori di sviluppo e la stessa velocità del Cloud per propagarsi prima che i team di sicurezza possano intervenire.

In questo scenario, la strategia "**assume breach**" — ovvero presumere che, prima o poi, una violazione avverrà — diventa indispensabile. Bisogna dotarsi di strumenti e procedure che permettano di **rilevare** gli eventi anomali il più velocemente possibile, di **investigare** con il contesto adeguato e di **rispondere** confinando l'attaccante prima che arrechi danni irreparabili.

Le **soluzioni di Cloud Detection and Response (CDR)** offrono risposte concrete a queste sfide. Sono progettate per:

- gestire la **complessità** e la **variabilità** degli ambienti multi-Cloud;
- sfruttare la **ricchezza di dati** (telemetria, log, API) di cui il Cloud dispone, senza sommergere gli analisti di eventi inutili;
- integrare strumenti di **investigazione** specifici, capaci di ricostruire i percorsi di

un potenziale attacco (dalle identità agli asset, dal traffico di rete alle modifiche di configurazione);
- abilitare azioni di **risposta** rapide e mirate, grazie ai meccanismi di API e automazione che il Cloud stesso offre.

Quando combinate con piattaforme **CNAPP**, le soluzioni CDR forniscono una copertura a 360° che parte dalla riduzione della **superficie d'attacco** (con posture management, vulnerability scanning, IaC scanning ecc.) e arriva fino alla gestione efficiente di **incidenti in tempo reale** (CDR), in un ciclo continuo di miglioramento.

Di fronte all'aumento degli attacchi e all'evoluzione delle tattiche dei criminali informatici, **non è più un'opzione** fare a meno di un approccio strutturato alla detection e alla risposta nel Cloud: diventa una necessità strategica per qualsiasi organizzazione che voglia difendere seriamente i propri dati, la propria reputazione e la fiducia dei clienti.
Secondo le "2025 Cloud Security Predictions" di Wiz, i prossimi anni saranno fondamentali per definire come difenderemo le infrastrutture Cloud, ma la direzione appare chiara: la sicurezza nel Cloud si sta allontanando da modelli verticali e a compartimenti stagni, per abbracciare approcci olistici, federati e supportati dall'IA, che si integrano senza soluzione di continuità in ogni livello dell'organizzazione. Dalla governance centralizzata con responsabilità decentralizzata (l'ascesa dei modelli federati), fino alle architetture di sicurezza orizzontale in cui codice, pipeline e risorse Cloud condividono una visione unificata del rischio, i leader della sicurezza devono adeguarsi a un contesto che richiede velocità, responsabilità e principi di "secure by design".

Modelli Organizzativi Federati

L'interesse crescente per le strutture federate offre agilità e responsabilità diretta in ambienti complessi. Man mano che le pratiche di sicurezza Cloud-native si estendono a infrastrutture ibride e on-premises, le aziende avranno sempre maggiore bisogno di controlli di sicurezza uniformi.

Sicurezza Orizzontale

Allontanarsi dai silos verticali promette una collaborazione più stretta tra i team di sicurezza Cloud e quelli di sicurezza delle applicazioni. Integrando le verifiche di sicurezza nelle fasi iniziali dello sviluppo e concentrandosi su un'infrastruttura immutabile, le organizzazioni possono "spostarsi a sinistra" in modo più efficace, rilevando e risolvendo le vulnerabilità prima che possano aggravarsi.

IA come Fattore Abilitante e di Rischio

L'IA continuerà a trasformare la sicurezza, democratizzando le informazioni e accelerando rilevamento e risposta. Tuttavia, proteggere le pipeline e i dati dell'IA diventa altrettanto cruciale, poiché gli avversari mirano a sfruttare o compromettere i modelli di machine learning.

Sicurezza della Supply Chain

Eventi recenti evidenziano la necessità urgente di monitorare le dipendenze del codice e di applicare una rigorosa gestione della postura di sicurezza in tutto il ciclo di sviluppo. L'analisi in tempo reale delle distinte base software (SBOM) diventerà uno standard imprescindibile.

L'Identità come Pilastro Centrale

La gestione delle identità (umane e non) sarà sempre più centrale nel controllo degli accessi, soprattutto dove l'IA e la sicurezza dei dati si intersecano. Una gestione solida dei permessi sarà fondamentale per evitare violazioni e garantire la conformità normativa.

I "Nation-state Threats" stimoleranno l'Innovazione

L'aumento delle operazioni informatiche su scala nazionale spingerà verso regole di sicurezza più restrittive, soprattutto in settori critici come la sanità, la finanza e l'energia. Le organizzazioni dovranno rafforzare le loro strategie di difesa per mantenersi in vantaggio rispetto ad attacchi avversari sempre più sofisticati.

Riassumendo, il 2025 rappresenta un momento cruciale per la sicurezza nel Cloud. Le aziende che adotteranno un approccio orizzontale e federato — sostenuto da intuizioni basate sull'IA, rigorose valutazioni della supply chain, solida gestione delle identità e una particolare attenzione alle minacce di tipo statale — saranno le meglio posizionate per proteggere le proprie infrastrutture e accelerare l'innovazione. La chiave sarà la collaborazione: team di sicurezza, sviluppatori e stakeholder aziendali che lavorano all'unisono per creare e mantenere un ambiente Cloud "secure by design", in grado di evolversi con la stessa rapidità delle minacce.

Trends e osservazioni di un SOC OT gestito

(A cura di Alessio Aceti, Corrado Righetti e Raffaele Fazio, HWG Sababa)

Il nostro SOC sta osservando che gli ambienti di Operational Technology (OT) affrontano sempre più minacce informatiche, tuttavia la maggior parte degli incidenti che colpiscono le infrastrutture critiche, ma anche il settore manifatturiero leggero e pesante, ha origine da minacce IT generiche che si spostano lateralmente in OT a causa di una segregazione inadeguata. Infatti, osserviamo segmentazione e micro-segmentazione ben implementata in meno del 10% delle aziende esaminate (Immagine 2).

Secondo le nostre statistiche, monitoriamo diverse multiutility nella regione EMEA, aziende del settore energy e manufacturing in Italia, molte aziende nel food, nonché diverse aziende nel settore acciaio e nella relativa supply chain. I dati evidenziano in prima battuta mancanza di governance e processi adeguati e poi di una segmentazione insufficiente, sistemi legacy e false positive contribuiscano a creare vulnerabilità nelle reti industriali. Inoltre, molte organizzazioni si affidano esclusivamente a soluzioni di cybersecurity OT, sonde che nascono per fare anomaly detection, ma del tutto inutili o quasi perché nessuno ha una descrizione dettagliata della realtà, nessuna mappatura della rete, nessuna conoscenza del processo industriale in dettaglio da parte di chi dovrebbe occuparsi si proteggere tali processi ecc.

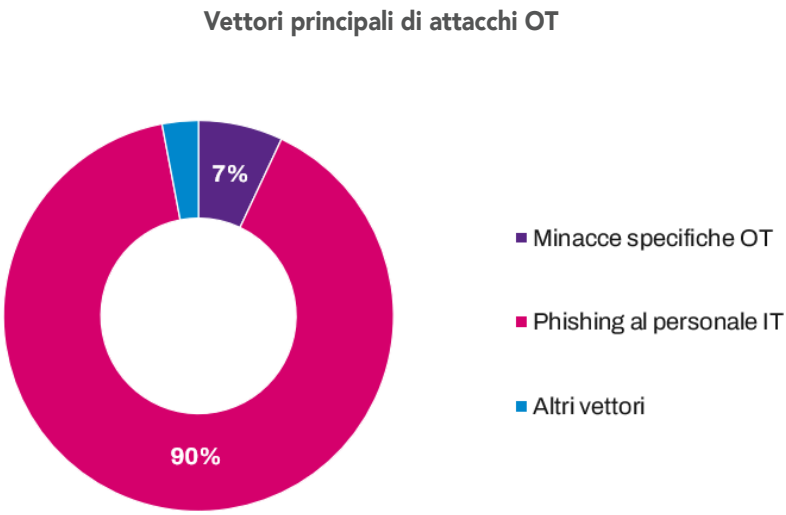
Osserviamo che dati e indicatori preziosi emergono dalla raccolta diretta di dati dai dispositivi OT e dallo studio dei processi dei clienti. In particolare, abbiamo investito molto nel settore della generazione di energia, e in questo settore l'analisi dei parametri relativi ai DCS consente di individuare anomalie potenzialmente correlate a cyber threats.

1. Panorama delle Minacce OT: Realtà vs Percezione

Mentre si presta molta attenzione alle minacce OT mirate, come malware PLC o exploit di protocolli industriali, la realtà è che la maggior parte degli incidenti negli ambienti OT deriva da minacce IT tradizionali che si propagano a causa di una segregazione insufficiente. La nostra analisi mostra:

- **l'85% degli incidenti di security in OT che abbiamo riscontrato ha origine dagli ambienti IT** tramite credential theft, propagazione di malware e remote access mal configurati;
- **solo il 7% degli incidenti rilevati coinvolge minacce specifiche OT**, come Triton, Industroyer o ransomware mirati ai PLC;

- **il 90% dei casi di ransomware che colpiscono ambienti industriali inizia con e-mail di phishing indirizzate al personale IT** e si estende ai network OT tramite meccanismi di autenticazione condivisi o remote access esposti.



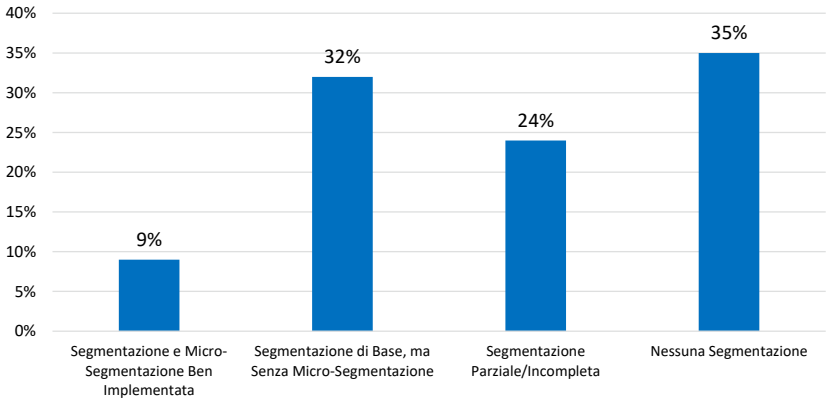
Source - HWG Sababa, 2024

2. Convergenza IT-OT: Il Punto Debole Principale

Il nostro SOC sta osservando che la mancanza di una rigorosa segmentazione tra IT e OT rappresenta una grave vulnerabilità. Le principali osservazioni:

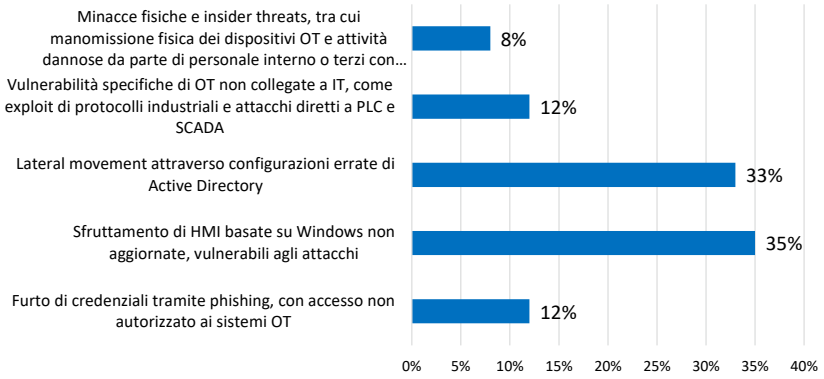
- **flat network architectures** permettono alle minacce IT (ransomware, botnet, credential attacks) di spostarsi lateralmente negli ambienti OT;
- **l'80% degli alert del SOC relativi agli ambienti industriali deriva da exploit IT**, come:
  - Credential theft tramite phishing con accesso non autorizzato ai sistemi OT;
  - Exploitation di HMI basate su Windows non aggiornate;
  - Lateral movement tramite configurazioni errate di Active Directory, senza citare che spesso in ambienti OT abbiamo password senza scadenza, utenze non nominali, utenze senza password ecc.
- **remote access rappresenta un vettore di rischio primario**, con il 65% delle compromissioni OT dovute a VPN o RDP sessions mal protette.

Adozione della Segmentazione e Micro-Segmentazione negli Ambienti OT



Source - HWG Sababa, 2024

Origine degli Alert SOC OT

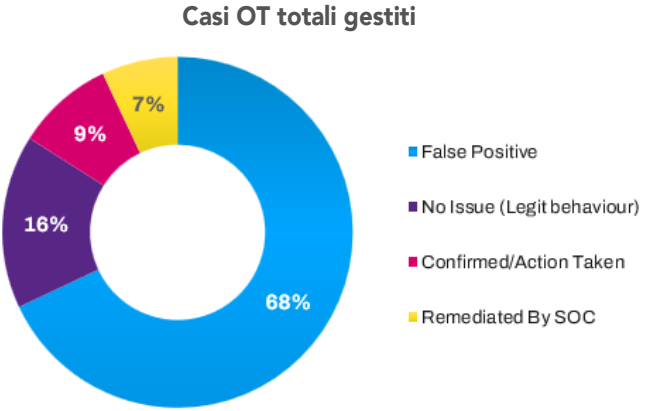


Source - HWG Sababa, 2024

3. False Positive e Alert Fatigue nel SOC OT

Secondo le nostre statistiche, i SOC OT affrontano notevoli difficoltà nel distinguere tra attività industriali legittime e comportamenti malevoli. Le nostre analisi mostrano:

- **il 68% degli alert di security nei SOC OT sono false positive**, principalmente a causa della mancanza di reperire documentazione e dati sui processi industriali;
- **alcuni protocolli degli Industrial Control System (ICS) non dispongono di autenticazione integrata**, rendendo più difficile il rilevamento delle anomalie senza una forte behavioral analysis;
- **i team SOC faticano a correlare gli alert tra ambienti IT e OT**, con tempi medi di detection e response superiori a 72 ore prima che una OT compromise venga identificata, soprattutto a causa di lentezze e problemi di comunicazione interna dei clienti, in particolare tra chi gestisce la cybersecurity e chi gestisce gli impianti.



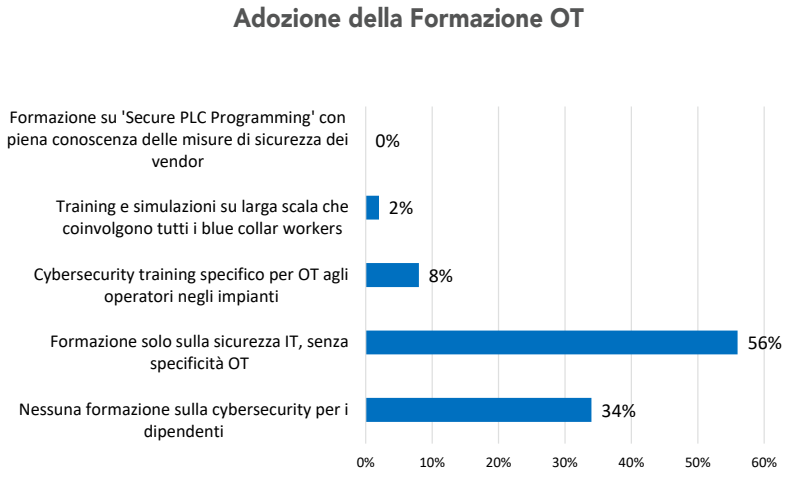
Source - HWG Sababa, 2024

4. Il Gap nella Formazione sulla Cybersecurity OT

Il nostro SOC osserva anche un significativo divario nella formazione sulla cybersecurity awareness OT. Mentre la formazione e la simulazione sulla IT security sono uno standard consolidato per l'enterprise IT, l'adozione nel settore OT è notevolmente inferiore. Secondo le nostre statistiche:

- **solo l'8% dei nostri clienti OT effettua cybersecurity training specifico per OT** agli operatori negli impianti;
- **solo il 2% dei nostri clienti OT effettua training e simulation su larga scala** che coinvolgono tutti i blue collar workers;

- **nessuno (0%) dei clienti su cui abbiamo erogato formazione di "Secure PLC programming" conosceva tutte le misure di sicurezza** che i vari vendor di sistemi industriali hanno inserito nei PLC negli ultimi anni, e per questo non facevano leva su tale prezioso strumento di protezione.



Source - HWG Sababa, 2024

Questa lacuna evidenzia la necessità di iniziative di awareness più robuste che includano il personale "blue collar", garantendo che tutti i dipendenti, dagli engineers agli operai di fabbrica, siano in grado di riconoscere e rispondere alle cyber threats. Una modalità che abbiamo trovato funzionale, è quella di associare corsi e esercitazione di cyber security awareness, alle sessioni formative sulla safety.

Conclusione

Il preconcetto secondo cui le minacce OT siano esclusivamente OT-specific attacks deve essere rivisto. La realtà è che una scarsa segregazione tra IT e OT consente **alle IT-based threats di diventare OT incidents**. Gli operatori delle critical infrastructures devono spostare l'attenzione da OT-specific malware alla correzione **delle vulnerabilità fondamentali negli ambienti IT** che espongono gli asset OT agli attacchi. Il nostro SOC OT gestito monitora e mitiga continuamente queste minacce, garantendo operazioni industriali resilienti, mentre c'è una totale mancanza di competenze cyber OT sul mercato.

Settore dell'energia a idrogeno: le sfide di cyber resilience

(A cura di Federica Maria Rita Livelli)

Scenario

Fonte: Immagine di freepik

Il settore dell'energia a idrogeno si sta affermando come una fonte energetica versatile e promettente per la transizione verso un futuro più sostenibile. Di fatto, l'idrogeno ha il potenziale per essere utilizzato nei trasporti per alimentare veicoli a celle a combustibile, nell'industria per supportare i processi produttivi e nello stoccaggio di energia per stabilizzare le reti elettriche. Inoltre, l'idrogeno prodotto da fonti rinnovabili - come il solare e l'eolico - è fondamentale nel processo di decarbonizzazione attualmente in corso. Tuttavia, con la rapida evoluzione del settore, caratterizzata anche da digitalizzazione e innovazione, è essenziale implementare misure di sicurezza flessibili per affrontare le crescenti minacce informatiche.

Secondo il rapporto CLUSIT pubblicato a marzo 2024, in Italia i cyber attacchi riusciti contro il settore energetico sono raddoppiati negli ultimi quattro anni, con il 90% dei casi classificati come di impatto "Critico" o "Alto". Inoltre, nel solo primo trimestre del 2024, il numero di incidenti nel settore Energy & Utilities è aumentato di oltre il 50% rispetto a tutto il 2023. I continenti più colpiti risultano essere l'UE e l'America,

dove si verifica l'80% dei casi analizzati. Al contrario, in Asia si è osservata una significativa diminuzione degli incidenti, mentre in Africa si è registrata una forte crescita.

Ancora, il cybercrime continua a essere la principale causa degli incidenti nel settore, rappresentando il motivo del 96% degli attacchi nel primo trimestre del 2024. Fenomeni di hacktivism sono stati rilevati nel primo trimestre del 2024, in linea con la tendenza del 2023, costituendo il 3,7% degli attacchi complessivi al settore.

Il report Security Intelligence & Analysis Service (SIAS), pubblicato dalla società di geopolitical & security intelligence Dragonfly, evidenzia che gli obiettivi principali della Russia in Europa sono: creare divisioni, ridurre la fiducia pubblica nei governi europei e minare il sostegno dell'Europa all'Ucraina.

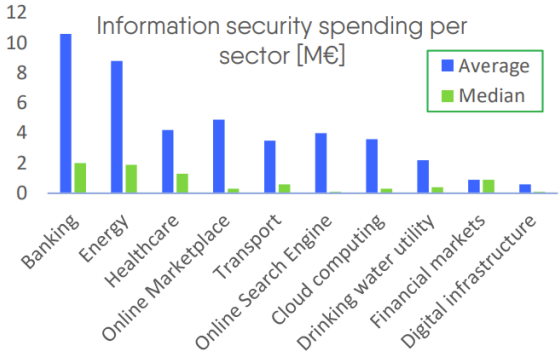
Gli attacchi informatici e il sabotaggio fisico nel settore energetico sono stati tra i metodi utilizzati per raggiungere questi obiettivi. Dall'inizio della guerra nel 2022, sono state segnalate pubblicamente almeno dieci violazioni da parte di gruppi di hacker sostenuti dallo stato russo. Tra questi, nel novembre 2023, la società energetica HSE ha subito un attacco informatico; mentre, la violazione più significativa è stata un'operazione contro 22 aziende energetiche in Danimarca ad aprile 2024, seguita da un attacco ransomware contro Electrica Group in Romania, che ha messo a rischio il servizio per oltre 3,8 milioni di utenti.

Dal 2022, secondo i dati raccolti da EnergiCERT -i.e. il centro di sicurezza informatica del settore energetico in Europa - si sono registrati i seguenti attacchi: 48 attacchi pubblicamente noti contro aziende energetiche e di fornitura europee; 31 attacchi ransomware, di cui 13 includono furto di dati; 15 attacchi che hanno interessato la tecnologia operativa (OT) delle reti.

I trend del continuo aumento degli attacchi cyber sono ulteriormente confermati anche dall'ultimo rapporto sulla cybersecurity nel settore elettrico pubblicato a novembre 2024 da Eurelectric (i.e. l'associazione di settore che rappresenta l'industria elettrica europea, da cui evince che gli attacchi ai paesi dell'UE sono passati dal 9,8% al 46,5% nel 2023.

Il report di Eurolectric evidenzia, altresì, che l'Europa sta investendo significativamente nella sicurezza informatica, con il settore energetico che si colloca al secondo posto per spesa, subito dopo il settore bancario. Tale aumento degli investimenti è stato in gran parte influenzato dalla guerra tra Russia e Ucraina e dagli attacchi informatici da parte di hacker russi e dal più recente conflitto in Medio Oriente, sottolineando la consapevolezza sulla necessità di proteggere le infrastrutture energetiche dalle minacce digitali.

È importante sottolineare che, a giugno 2024, la Commissione europea ha organizzato un'esercitazione paneuropea per valutare la resilienza delle infrastrutture energetiche dell'UE contro attacchi informatici simulati. In un contesto in cui le minacce informatiche sono in continua evoluzione, è fondamentale dare priorità alle esercitazioni di sicurezza informatica, dato che queste iniziative proattive non solo rafforzano la nostra capacità di difesa contro potenziali attacchi, ma dimostrano anche l'impegno nel proteggere i nostri ecosistemi nel settore energetico a fronte delle sfide che aumentano con la crescente complessità delle reti intelligenti, costituite da sistemi più interconnessi, che diventano più vulnerabili alle minacce informatiche.



Fonte immagine - "A snapshot of Cybersecurity in the EU" - Eurelectric position paper

Sfide di cyber resilience nel settore dell'energia a idrogeno

Gli impianti di produzione di idrogeno e le relative reti di distribuzione stanno diventando sempre più digitalizzati, incorporando sistemi IT e OT che risultano particolarmente suscettibili agli attacchi informatici. Tali attacchi possono compromettere non solo la continuità operativa e la sicurezza, ma anche causare disastri ambientali significativi, data la presenza di materiali pericolosi e beni di alto valore. È quindi fondamentale implementare soluzioni di sicurezza informatica per garantire operazioni sicure e ininterrotte.

Inoltre, è risaputo che molti sistemi di controllo industriale operano su software e sistemi operativi che in alcuni casi sono obsoleti e non sempre compatibili con le più recenti soluzioni di sicurezza.
Ancora, l'adozione di protocolli di sicurezza, che potrebbero richiedere riavvii o modifiche significative, rischia di interrompere i processi produttivi, generando rischi operativi considerevoli. Senza dimenticare che le peculiarità di questi sistemi indu-

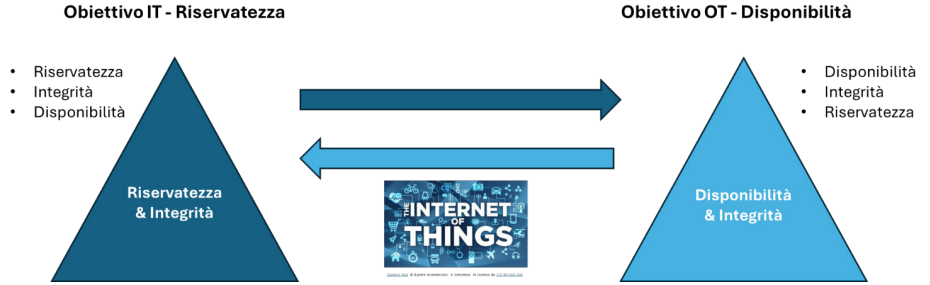
striali possono rendere gli aggiornamenti standard di sicurezza IT causa di instabilità. È doveroso evidenziare, altresì, che gli impianti di idrogeno - diversamente dagli impianti di produzione convenzionali o dalle centrali elettriche con layout e protocolli di sicurezza uniformi - spesso mancano di un piano di sicurezza unificato: Ciò è dovuto dal fatto che molti di essi derivano da progetti pilota o da ambienti di laboratorio, dove le misure di sicurezza informatica di base potrebbero essere state trascurate durante la transizione. Ne consegue che questa mancanza di standardizzazione e di approccio coerente alla sicurezza rende tali impianti particolarmente vulnerabili alle minacce informatiche.

Priorità di sicurezza diverse tra ambienti IT e OT

Il settore dell'energia dell'idrogeno si basa su ambienti IT e OT e la distinzione tra i due ambienti, per quanto riguarda la sicurezza informatica, è definita principalmente dai diversi obiettivi/priorità di protezione. E precisamente:

Priorità OT - Per quanto riguarda l'OT - soprattutto negli ambienti di produzione - l'obiettivo principale è mantenere la disponibilità dell'impianto e garantire che le operazioni non vengano interrotte da attacchi informatici. Il secondo livello di priorità si concentra sull'integrità dei dati, ovvero la protezione da alterazioni o manipolazioni non autorizzate dovute ad attacchi. Inoltre, anche se la privacy dei dati rimane un fattore importante, è considerata non prioritaria; mentre la protezione delle informazioni sensibili e della proprietà intellettuale hanno la precedenza.

Priorità IT - Le priorità nella sicurezza informatica sono invertite: la privacy dei dati viene prima di tutto, seguita dall'integrità dei dati e infine dalla disponibilità del sistema. Tale inversione di priorità tra i sistemi IT e OT rappresenta, quindi, una sfida complessa per lo sviluppo di una strategia di sicurezza equilibrata che soddisfi i requisiti e i rischi specifici di ciascuna area.



Rappresentazione grafica creata da Federica M.R. Livelli

Minimizzazione del rischio: AAA approccio olistico cercasi

A fronte di quanto sopra descritto, il settore dell'energia a idrogeno necessita un approccio alla sicurezza informatica su misura e in grado gestire le sfide del panorama operativo e tecnologico unico degli impianti di produzione di idrogeno. Di fatto, si tratta di garantire lo sviluppo e l'implementazione di misure di sicurezza flessibili - ma solide - in grado di proteggere dalle minacce attuali e di adattarsi alle sfide future, perseguendo una strategia di difesa suddivisa in tre livelli critici - ciascuno adattato a vulnerabilità e a rischi specifici, quali:

- **livello di sicurezza dell'impianto** – La sicurezza dell'impianto si basa su una serie di procedure volte a proteggere l'intera struttura, includendo meccanismi di difesa sia fisica sia digitale. Di fatto, questo livello è focalizzato sulla prevenzione dell'accesso fisico non autorizzato a infrastrutture critiche, adottando sia misure di sicurezza tradizionali – quali il controllo sicuro degli ingressi agli edifici - sia metodi più avanzati – quali i sistemi di chiavi magnetiche - per le aree particolarmente sensibili.
  È doveroso evidenziare che gli operatori degli impianti a idrogeno, con l'aumento delle esigenze di sicurezza industriale, devono fronteggiare limitazioni in termini di tempo e di risorse, richiedendo un supporto esperto. Attualmente, sono disponibili sul mercato servizi di sicurezza personalizzati che offrono l'analisi dei rischi, l'implementazione delle misure di sicurezza, il monitoraggio continuo e aggiornamenti regolari per garantire la massima protezione degli impianti.
  Inoltre, è importante evidenziare che le valutazioni della sicurezza sono fondamentali a questo livello, dato che forniscono un'analisi dettagliata delle minacce, delle vulnerabilità e dei rischi, unitamente a raccomandazioni per colmare le lacune di sicurezza identificate. Ancora, tali valutazioni possono includere audit in loco o controlli completi basati su standard come l'IEC 62443 (i.e., lo standard internazionale per la sicurezza dei sistemi di controllo dell'automazione industriale) per garantire che i controlli di sicurezza fisica – quali il controllo degli accessi – e le misure di sicurezza organizzativa -quali politiche e formazione - siano solide ed efficaci;
- **livello di sicurezza della rete** - L'obiettivo di questo livello è salvaguardare le reti di automazione da accessi non autorizzati attraverso un attento monitoraggio di tutte le interfacce, sia tra reti IT e OT sia per l'accesso remoto. La segmentazione della rete, l'uso di comunicazioni crittografate e l'adozione di principi zero-trust assicurano un'architettura sicura che isola le aree critiche e controlla l'accesso tramite firewall e protocolli di autenticazione sicuri. Inoltre, la segmentazione delle zone di sicurezza e la protezione delle comunicazioni tra queste zone sono

fondamentali per prevenire accessi non autorizzati ai dati e mantenere l'integrità del sistema. Inoltre, con l'aumento del lavoro a distanza, questo livello permette di stabilire connessioni sicure alle aree di sviluppo e produzione, utilizzando comunicazioni basate su certificati e autenticazione secondo i principi zero-trust;

- **livello di integrità del sistema** - L'integrità del sistema è volta a impedire l'accesso non autorizzato ai sistemi di automazione, ai relativi dati e ai canali di comunicazione, oltre a prevenirne la manipolazione. L'obiettivo principale è evitare tempi di inattività imprevisti e salvaguardare la proprietà intellettuale. Ciò è reso possibile attraverso funzionalità di sicurezza integrate che bloccano modifiche non autorizzate alla configurazione e proteggono l'accesso alla rete e ai dati di configurazione da copie o da manipolazioni, assicurando così l'affidabilità e la sicurezza dell'ambiente produttivo.

Il ruolo del fattore umano per la cybersecurity del settore dell'idrogeno

La sicurezza degli impianti di produzione di idrogeno richiede non solo misure tecniche, ma anche un significativo coinvolgimento umano. È fondamentale un approccio olistico che unisca formazione qualificata del personale, rigidi controlli di accesso e avanzati meccanismi di autenticazione. Ovvero, un approccio che mira a: promuovere una cultura della sicurezza robusta; minimizzare il rischio di errori umani; garantire la protezione dei dati sensibili e delle infrastrutture critiche.

Di fatto, un programma di formazione esaustivo deve dotare i dipendenti degli strumenti e delle conoscenze per riconoscere e affrontare le minacce, oltre a diffondere una consapevolezza della sicurezza informatica a livello aziendale. Inoltre, l'implementazione del principio del privilegio minimo - che consente l'accesso ai dati sensibili solo a chi ne ha necessità per il proprio ruolo, come nel controllo degli accessi basato sui ruoli (Role Based Access Control - RBAC) - è cruciale dato che consente di ridurre significativamente il rischio di violazioni dei dati sia per errore sia intenzionali.

Ancora, audit regolari e controlli di conformità rinforzano questo framework, assicurando la corretta assegnazione dei diritti di accesso. Senza dimenticare che l'autenticazione robusta è quanto mai essenziale per prevenire accessi non autorizzati e, in particolare, l'autenticazione a più fattori (Multi Factor Authentication - MFA) aumenta la sicurezza, richiedendo agli utenti di fornire diverse forme di verifica, quali password, token di sicurezza e di identificazione biometrica, offrendo, così, una protezione superiore rispetto ai soli metodi basati su password.

Inoltre, come sottolinea Gaetano Sanacore, Direttore Scientifico dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici,

"un rischio aggiuntivo può manifestarsi al confine tra le architetture IT e OT, in un contesto di cyber-resilienza, nel punto di convergenza IT/OT nei settori di produzione e distribuzione dell'idrogeno e nelle loro architetture produttive. Il pericolo è che il personale addetto alla sicurezza possa introdurre tecnologie e/o servizi con un'impronta più IT che OT al confine tra questi due ambiti. Questo potrebbe portare a una '*ITizzazione*' dell'ambiente OT, rendendolo più suscettibile agli attacchi degli hacker che, una volta entrati nell'infrastruttura IT, possono muoversi facilmente all'interno dell'infrastruttura OT, sfruttando le vulnerabilità comuni dell'IT (CVE - Common Vulnerabilities and Exposures) che possono causare gravi interruzioni nei processi OT, fino a bloccarli completamente".

Normative e standard di sicurezza che impattano sul settore energetico dell'idrogeno

La protezione delle infrastrutture energetiche dell'idrogeno è supportata da diverse normative e standard di sicurezza - quali NIS2, IEC 62443 e CER (Critical Entities Resilience) - che forniscono un quadro normativo per proteggere le infrastrutture critiche del settore energetico - incluso quello dell'idrogeno - da minacce fisiche e cibernetiche, assicurando la resilienza dei servizi essenziali, oltre a promuovere pratiche di sicurezza avanzate. Vediamo di seguito di che si tratta.

Direttiva NIS2 - La direttiva mira a garantire un livello comune elevato di sicurezza informatica nell'Unione Europea per i settori critici - come l'energia - e richiede agli Stati membri di migliorare la loro preparazione, collaborazione e cultura della sicurezza. Essa si basa su misure tecniche e organizzative per gestire i rischi legati alla sicurezza dei sistemi informatici e impone obblighi di notifica degli incidenti.

IEC 62443 - Uno standard internazionale che fornisce un framework applicativo per le misure di sicurezza richieste dalla Direttiva NIS2. È specifico per i sistemi di automazione e controllo industriale, fornendo strumenti pratici per implementare misure di cybersecurity ed è particolarmente rilevante per settori come l'energia, dove i sistemi di controllo industriale sono ampiamente utilizzati.

Sinergia e complementarità NIS2 e IEC 62443 - Nonostante le due normative operino su livelli e contesti diversi, lo standard internazionale IEC 62443 fornisce un supporto concreto e tecnicamente specifico per attuare i requisiti generali della Direttiva NIS2, creata per proteggere le reti e i sistemi informativi nei settori critici europei. Dato che molti dei settori coperti dalla NIS2, incluso il settore energetico, fanno largo uso di sistemi di controllo industriale, l'IEC 62443 può aiutare a soddisfare gli obblighi di sicurezza stabiliti dalla direttiva in questi ambiti specifici. In sostanza, la sinergia tra le due normative permette alle organizzazioni di assicurare la conformità

dei sistemi industriali, migliorando allo stesso tempo la continuità operativa dei servizi essenziali.

In pratica, si osservano:

- Un allineamento degli obiettivi di sicurezza delle due norme, che punta a rafforzare la resilienza complessiva contro le minacce informatiche.
- Un approccio strutturato alla gestione del rischio, in cui le best practices dell'IEC 62443 forniscono una guida fondamentale per affrontare correttamente la valutazione del rischio informatico.
- L'integrazione nei processi di conformità, dove audit e certificazioni secondo gli standard IEC 62443 possono dimostrare la conformità con i requisiti NIS2, se inseriti in un programma complessivo di cybersecurity.

Punti di implementazione specifici della direttiva NIS per le infrastrutture strategiche

È doveroso evidenziare che, per soddisfare i requisiti elencati all'Articolo 21, comma 2, della Direttiva NIS2, si può fare riferimento alla parte 2-1 dello standard IEC, ovvero l'IEC 62443-2-1.

Inoltre, come suggerisce sempre Gaetano Sanacore, "è importante comprendere che la parte IEC 62443-3.2 permette di impostare un Security Risk Assessment per la progettazione/adeguamento dei sistemi di Supervisione e Controllo (ICS/SCADA/RTU/PLC) allo standard, oltre a definire il livello di sicurezza target (SL-T) degli impianti produttivi, anche per i sistemi di produzione/trasmissione e distribuzione dell'Idrogeno. Pertanto, è necessario prendere in considerazione anche le fasi dell'intero ciclo di vita degli IASC (Industrial Automation and Control Systems). E, precisamente:

- **fase di specifica -** Asset/sistema per cui si definisce il livello di sicurezza target, SLT (62443-3-2) che costituisce il requisito di sicurezza per l'integrazione e il funzionamento dell'impianto;
- **fase di integrazione e messa in servizio -** Questa fase implementa la soluzione di automazione sicura e appropriata, richiesta dal proprietario dell'asset e secondo il SL-T (Security Level-Target) che è stato definito. Inoltre, l'integratore di sistema deve garantire che tutte le misure implementate per il SL-A (Security Level - Achieved) siano efficienti, adeguate e corrispondano al SL-T;
- **l'esercizio di impianto e la fase di manutenzione -** Le capacità di sicurezza dell'IACS devono essere mantenute sui livelli di sicurezza raggiunti e approvati in tutte le sue zone e condotti. Inoltre, il rischio di violazioni della sicurezza e delle relative conseguenze deve essere mantenuto a un livello accettabile. Ancora,

le proprietà di sicurezza rilevanti per l'IACS devono essere verificate e/o testate a intervalli regolari o ogni volta che viene scoperta una nuova vulnerabilità per garantire che SL-A corrisponda a SL-T.

Sanacore sottolinea, inoltre, l'importanza dei seguenti 4 SL specifici per la mitigazione del rischio previsti dallo standard tecnico IEC 62443 e, precisamente (in ordine crescente di complessità):

- **Security Level 1 (SL1)** - Protezione contro la violazione occasionale o casuale.
- **Security Level 2 (SL2)** - Protezione contro la violazione intenzionale con mezzi scarsi, con risorse scarse, competenze generiche del sistema e motivazione scarsa.
- **Security Level 3** (**SL3**) - Protezione contro la violazione intenzionale con mezzi sofisticati, con risorse moderate, competenze specifiche del sistema e motivazione moderata.
- **Security Level 4** (**SL4**) - Protezione contro la violazione intenzionale con mezzi sofisticati con risorse ingenti, competenze specifiche del sistema e forte motivazione.

Inoltre, Sanacore aggiunge: "i requisiti di sicurezza per ogni installazione variano, a seconda della criticità dell'impianto industriale, e adempiono agli eventuali cogenti di legge (es. NIS2)".

Obiettivi NIS2 e Riferimenti 62443-2-1

Di seguito un'esamina dei riferimenti normativi per tipologia di sfide relative al settore dell'energia a idrogeno per quanto riguarda la NIS2 e IEC 62443-2-1.

Politiche di analisi dei rischi e di sicurezza dei sistemi informatici

Obiettivo NIS 2: si tratta di adottare misure proporzionate ai rischi che devono essere valutati in relazione al servizio essenziale, per implementare un approccio "risk-based".

Riferimenti IEC 62443-2-1:
4.2.2 Business Rationale
4.2.3 Risk identification, classification, and assessment
4.3.2.3 Organizing for security
4.3.2.6 Security policies and procedures
4.3.4.2 Risk management and implementation
4.3.4.3 System development and maintenance

4.4.3 Review, improve and maintain the Cyber Security Management System

Inoltre, in questo caso, Sanacore afferma che "è importante evidenziare che la parte IEC 62443-3.2 permette di impostare un Security Risk Assessment per la progettazione/adeguamento dei sistemi di Supervisione e Controllo (ICS/SCADA/RTU/PLC) e definisce il livello di sicurezza target - SLT degli impianti produttivi - anche per i sistemi di produzione/trasmissione e distribuzione dell'Idrogeno".

Gestione degli incidenti, procedure e strumenti per la notifica

Obiettivo NIS 2 - Si tratta di adottare un piano per il contenimento di eventuali incidenti, coordinandosi con le autorità preposte.

Riferimento IEC 62443-2-1 - Si fa riferimento al 4.3.4.5 Incident planning and response

Continuità operativa, gestione del backup in caso di disastro

Obiettivo NIS 2 - Si tratta di avere un piano per riprendere al meglio l'erogazione del servizio.

Riferimento IEC 62443-2-1 – Si fa riferimento al 4.3.2.5 Business Continuity Plan

Sicurezza della supply chain

Obiettivo NIS 2: è necessario gestire in sicurezza la catena dei fornitori per minimizzare il rischio di attacco.

Riferimenti IEC 62443-2-1 - Si fa riferimento a:
4.3.2.2 Cyber Security Management System scope
4.3.2.3 Organizing for security
4.3.2.6 Security policies and procedures
4.3.4.3 System development and maintenance
4.4.3 Review, improve and maintain the Cyber Security Management System

Sicurezza dell'acquisto, dello sviluppo e della manutenzione dei sistemi, compresa la gestione e la divulgazione delle vulnerabilità

Obiettivo NIS 2: si tratta di garantire la gestione della sicurezza nel cambiamento, nella gestione delle vulnerabilità e nell'aggiornamento dei sistemi.

Riferimenti IEC 62443-2-1:
4.2.3 Risk identification, classification, and assessment
4.3.2.2 Cyber Security Management System scope

4.3.2.6 Security policies and procedures
4.3.4.3 System development and maintenance.
4.4.3 Review, improve and maintain the Cyber Security Management System

È importante sottolineare che la Direttiva NIS2 include anche requisiti per la gestione dei rischi, la formazione del personale, le politiche di crittografia, il controllo degli accessi e l 'autenticazione, con riferimenti nell'IEC 62443 che supportano il soddisfacimento consapevole di tali requisiti attraverso analisi, training e piani di formazione mirati.

Le direttive CER e NIS2: leve per la resilienza del settore energia dell'idrogeno

La nuova direttiva CER sostituisce la direttiva europea sulle infrastrutture critiche del 2008 e, insieme alla NIS2, mira a rafforzare la resilienza delle infrastrutture critiche - incluso il settore dell'energia a idrogeno - che devono adottare misure tecniche, di sicurezza e organizzative per rafforzare la loro resilienza.

In particolare, il settore dell'energia a idrogeno dovrà garantire la propria resilienza in termini di: produzione di idrogeno (operatori della produzione di idrogeno); stoccaggio di idrogeno (operatori dello stoccaggio di idrogeno); trasporto di idrogeno (operatori del trasporto di idrogeno).

È doveroso evidenziare che la direttiva CER si sovrappone in parte alla NIS2, dato che è più orientata alla protezione fisica delle infrastrutture, evidenziando, così, che la resilienza non dovrebbe essere limitata alla sicurezza informatica, ma deve estendersi anche alle minacce fisiche quali: reati terroristici, sabotaggi e calamità naturali.

Di fatto, a differenza della direttiva NIS2, la direttiva CER non distingue tra entità "essenziali" e "importanti", utilizzando invece la terminologia generale di "entità critiche" per i fornitori di servizi essenziali identificati come tali, sulla base della valutazione del rischio.

Inoltre, le entità identificate come critiche ai sensi della Direttiva CER dovrebbero essere considerate essenziali anche ai sensi della Direttiva NIS2. Pertanto, entrambe le normative sono applicabili a queste entità. Ancora, le entità critiche ai sensi della Direttiva CER devono rispettare le misure di gestione del rischio di sicurezza informatica e gli obblighi di segnalazione imposti dalla Direttiva NIS2.
Si ritiene che, per semplificare le attività di vigilanza e ridurre al minimo l'onere amministrativo, le autorità competenti dovrebbero armonizzare i modelli di notifica degli incidenti e i processi di vigilanza.

Cyber Resilience Act (CRA) e AI Act nel settore dell'energia a idrogeno

Le organizzazioni coinvolte nella fornitura di hardware e software critici al settore dell'energia a idrogeno devono porre attenzione anche al Cyber Resiliency Act (CRA), che introduce requisiti di sicurezza informatica per i prodotti con elementi digitali (prodotti e dispositivi IoT).

È doveroso ricordare che il CRA si applica a tutti i prodotti IoT, oltre a stabilire misure migliorate per l'hardware utilizzato all'interno di infrastrutture critiche. Pertanto, per quanto riguarda il settore dell'energia a idrogeno, i sistemi di automazione e controllo industriali, i sistemi di gestione di rete, le interfacce di rete fisiche, i firewall e router, i modem e gli switch saranno tutti sottoposti a un attento esame. Inoltre, nei casi in cui i sistemi AI sono utilizzati nel settore dell'energia a idrogeno, le organizzazioni del settore devono conformarsi non solo a NIS2, CER, ma anche all'AI Act, sfruttando misure di sicurezza informatica anche per supportare la gestione del rischio AI. Ovvero, le organizzazioni del settore dell'energia a idrogeno necessitano di attuare un approccio olistico alla conformità, integrando le pratiche di sicurezza informatica e la gestione del rischio AI.

Network Code on Cybersecurity (NCCS) Standard – È entrato in vigore a marzo 2024 e fornisce norme per il settore dell'energia elettrica dell'UE (i.e. codice di rete) per affrontare gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica al fine di contribuire a rendere il sistema elettrico dell'UE più resiliente e sicuro. In particolare, stabilisce norme riguardanti: la valutazione dei rischi per la sicurezza informatica; i requisiti minimi comuni di cibersicurezza; la pianificazione, la reportistica e il monitoraggio; la gestione delle crisi. Esso è destinato a impattare anche il settore dell'energia a idrogeno, considerando che l'energia dell'idrogeno è collegata al sistema elettrico tramite un processo di elettrificazione come vettore energetico; l'elettrificazione dell'idrogeno è solitamente realizzata sotto forma di conversione da gas a elettricità per rilasciare energia.

Risk Preparedness Regulation nel settore energetico – Si tratta di una regolamentazione per la cooperazione degli Stati membri che è in vigore da giugno 2019 e sarà revisionata entro settembre 2025. Essa mira a: identificare meglio le possibili crisi elettriche; predisporre piani di gestione delle crisi; gestire le crisi quando si verificano. Inoltre, stabilisce una metodologia comune e le norme per la cooperazione tra i paesi dell'UE al fine di prevenire, di prepararsi e di gestire le crisi dell'energia elettrica in uno spirito di solidarietà e trasparenza, nel rispetto dei requisiti per un mercato interno competitivo dell'energia.

ISO/IEC 27019:2024"Information security controls for the energy utility industry" – Questo standard, recentemente pubblicato, stabilisce requisiti specifici per il funzionamento sicuro dei sistemi di controllo dei processi e le misure di sicurezza per il settore dell'energia, ampliando i controlli per includere vari aspetti specifici del settore energetico rispetto ai controlli della ISO 27001:2022 e della ISO 27002:2022.

Governance del settore energetico in Europa: Istituzioni, organi consultivi e reti degli Stati membri

Tra le istituzioni dell'UE, ci sono quattro principali entità con compiti diversi. E, precisamente:

European Network And Information Security Agency (ENISA) – È l'agenzia dell'UE dedicata a raggiungere un alto livello comune di cybersecurity in tutta Europa. P

Computer Emergency Response Team for EU (CERT-EU) – È l'ente di sicurezza informatica che lavora per proteggere i dati e i sistemi delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione e garantisce le risposte alle emergenze.

European Cybersecurity Competence Centre (ECCC)- È un'agenzia esecutiva europea che mira ad aumentare le capacità e la competitività nel campo della cybersecurity.

European Defence Agency (EDA) - È l'agenzia che lavora con la difesa complessiva dell'Unione, inclusa la resilienza cibernetica.

Oltre alle istituzioni sopra menzionate, esistono quattro organi consultivi e quattro diverse reti di Stati membri che lavorano sulla cybersecurity a livello dell'UE. In particolare, nel campo intersecante dell'energia e del cyber, la Commissione Europea ha costituito un cosiddetto Smart Energy Expert Group (SEEG), la cui missione è accelerare la digitalizzazione del sistema energetico. Il gruppo di esperti è stato formalmente creato nell'ambito del Piano d'Azione per la digitalizzazione dell'energia. Il sottogruppo del SEEG – denominato Working Group Cybersecurity - fornirà raccomandazioni e orientamenti alla Commissione in termini di cybersecurity per i sistemi energetici. Ciò comprende sia la valutazione delle ramificazioni di nuove iniziative legislative nel campo sia l'esplorazione delle migliori modalità per affrontare le sfide correlate.

Stato dell'arte dell'energia a idrogeno in Italia

L'Europa ha integrato l'idrogeno come elemento centrale della sua politica energetica, e l'Italia, supportata dai fondi del PNRR, ha seguito questa direzione. A gennaio 2024, la Commissione Europea ha approvato un aiuto di 550 milioni di euro per

sostenere l'uso dell'idrogeno nei processi industriali, con l'obiettivo di accelerare la transizione verde e ridurre la dipendenza dai combustibili fossili.

In Italia, il piano prevede la creazione di 54 Hydrogen Valley per riqualificare aree industriali dismesse, lo sviluppo di progetti nei settori industriali difficili da decarbonizzare, e la costruzione di stazioni per il trasporto su strada e ferroviario entro il 2026. Attualmente, sono in corso 54 progetti finanziati, con il 50% dei fondi destinato al Sud Italia. L'iniziativa mira a promuovere la produzione e l'uso di idrogeno verde, creando hub per la produzione, tracciamento, stoccaggio e distribuzione dell'idrogeno. Inoltre, il 26 novembre 2024, il Ministero dell'Ambiente e della Sicurezza Energetica ha introdotto la Strategia Nazionale Idrogeno 2024 che identifica l'idrogeno come una soluzione chiave per raggiungere gli obiettivi di decarbonizzazione, in linea con gli impegni del Piano Nazionale Integrato Energia e Clima (PNIEC) per il 2030 e il traguardo del Net Zero entro il 2050.

Come afferma Sanacore "è quanto mai importante e strategico garantire la cyber resilience di questo settore strategico anche in considerazione del quadro normativo europeo vigente e che richiede sempre più un approccio risk-based e resilience based, utilizzando a supporto i più calzanti standard internazionali di sicurezza (es. IEC 62443, IEC 62351, ecc)".

Raccomandazioni

È essenziale concedere al settore dell'energia – incluso quella a idrogeno - il tempo necessario per implementare completamente il quadro normativo dell'UE attuale, prima di introdurre nuove regolamentazioni, considerando le sfide contingenti. Di fatto, i miglioramenti normativi dovrebbero essere proposti solo quando strettamente necessari, evitando sovrapposizioni con regolamenti esistenti, data l'importanza crescente di questo settore per l'Europa.
Inoltre, è fondamentale promuovere lo sviluppo di una forza lavoro qualificata, dato che l'industria della sicurezza informatica richiede un incremento di personale qualificato per affrontare le minacce in evoluzione e, in quest' ottica, l'UE ha istituito la Skills Academy da parte dell'UE. Ancora, è cruciale abilitare investimenti che permettano al settore di gestire efficacemente i rischi cyber crescenti, riconoscendo e compensando i costi aggiuntivi delle misure di sicurezza e della conformità normativa.

Conclusioni

La cyber resilience è fondamentale per il futuro del settore dell'energia a idrogeno, e le organizzazioni in queste aree specifiche devono potenziare notevolmente le loro difese informatiche per contrastare attacchi hacker sempre più sofisticati e distruttivi.

Proteggere le infrastrutture dalle minacce informatiche non è solo una necessità operativa, ma un imperativo per garantire l'affidabilità e la sostenibilità dell'energia pulita. Le direttive europee che riguardano il settore energetico richiedono l'implementazione di principi di risk management, business continuity e cybersecurity, adottando un approccio basato sul rischio e sulla resilienza. Guardando al futuro, sarà essenziale che le organizzazioni continuino a innovare e collaborare per rafforzare la sicurezza informatica e promuovere la resilienza delle infrastrutture critiche in Europa, senza dimenticare l'importanza di promuovere una formazione continua ed esercitazioni periodiche per consolidare la cultura della cyber resilience nel settore.

Fonti

- Rapporto Clusit – marzo 2024 - https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2024-Approfondimento-energy-e-utilities-Q1.pdf
- NIS2 Directive - https://digital-strategy.ec.europa.eu/it/policies/nis2-directive
- Critical Entities Resilience (CER) Directive https://www.critical-entities-resilience-directive.com/
- Cyber Resilience Act (CRA) - https://www.european-cyber-resilience-act.com/
- Eurelectric snapshot of cybersecurity 2024 - https://www.eurelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf
- Network Code Cybersecurity (NCCS) - EU electricity supply – sector-specific rules on cybersecurity (network code)
- EU regulation on risk-preparedness in the electricity sector - Regulation - 2019/941 - EN - EUR-Lex
- Gaetano Sanacore, Direttore Scientifico dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici - Contributo autorizzato sotto forma di virgolettati.

Proteggere la Supply Chain: strategie di difesa per MSP e MSSP in un panorama di minacce globali

(A cura di Irina Artioli, Acronis)

Escalation delle minacce Cyber: implicazioni per l'Europa e l'Italia

Gli attacchi informatici continuano ad aumentare su scala globale ed europea, e l'Italia non fa eccezione. L'impennata delle campagne ransomware e delle compromissioni della supply chain ha attirato l'attenzione dei policymaker, spingendo l'Unione Europea a adottare misure più stringenti. La Direttiva NIS2 rappresenta un progresso significativo nella strategia di cybersecurity europea, imponendo requisiti di sicurezza più rigorosi ed estendendo il proprio perimetro per proteggere meglio infrastrutture critiche e servizi digitali. Uno dei cambiamenti più rilevanti introdotti dalla NIS2 riguarda l'ampliamento del campo di applicazione: non più limitata alle grandi imprese, la direttiva ora coinvolge anche le aziende di medie dimensioni, aumentando sensibilmente gli obblighi di conformità. Questa trasformazione riflette una consapevolezza crescente: le minacce cyber non fanno distinzioni in base alle dimensioni aziendali. Qualsiasi organizzazione con dipendenze digitali può diventare un bersaglio.

NIS2: quali settori sono coinvolti?

Per molte aziende, una delle sfide principali è determinare se rientrano nel perimetro di applicazione della direttiva. La NIS2 estende la propria copertura ben oltre le infrastrutture critiche tradizionali, includendo fornitori di servizi IT, piattaforme cloud, marketplace online e data center, tra gli altri. Per chi è incerto sulla propria classificazione, una domanda chiave da porsi è: *Se i nostri sistemi venissero compromessi, chi ne subirebbe le conseguenze?* Un attacco informatico a un singolo ente può avere ripercussioni su tutta la supply chain, rendendo la gestione del rischio di terze parti una priorità. Identificare proattivamente le proprie esposizioni e dipendenze sarà fondamentale per affrontare le nuove normative.

Attacchi alla Supply Chain: una minaccia in crescita

Gli attacchi alla supply chain continuano a rappresentare una minaccia significativa, sfruttando le vulnerabilità nei sistemi interconnessi per colpire simultaneamente più organizzazioni.

I Managed Service Provider (MSP), i Managed Security Service Provider (MSSP) e le aziende di telecomunicazioni (Telco) svolgono un ruolo centrale nell'ecosistema IT moderno, rendendoli obiettivi privilegiati per i cybercriminali. Gli attaccanti mirano a sfruttare l'accesso privilegiato di questi fornitori ai sistemi dei loro clienti, moltiplicando l'impatto delle intrusioni.

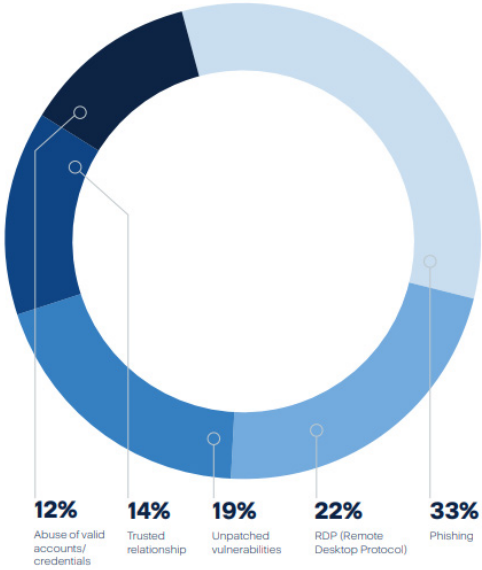
Le campagne di attacco stanno diventando sempre più sofisticate, con un uso crescente del social engineering e del phishing per ottenere accessi non autorizzati a sistemi sensibili. L'ascesa degli attacchi alimentati dall'Intelligenza Artificiale ha ulteriormente aggravato la situazione, permettendo agli attori delle minacce di automatizzare campagne di phishing, aggirare le difese tradizionali e individuare vulnerabilità con precisione allarmante. Una violazione riuscita all'interno di un MSP o di un MSSP può generare effetti a catena devastanti, compromettendo intere supply chain e causando interruzioni in settori critici a livello globale.

I dati parlano chiaro: le tendenze del 2024

Il monitoraggio di Acronis TRU (TRU) degli attacchi contro MSP, MSSP e Telco tra gennaio e dicembre 2024 ha rivelato 185 incidenti rivendicati. Dall'analisi emerge che i cybercriminali hanno fatto ampio uso di campagne di phishing via e-mail, seguite dallo sfruttamento di strumenti di accesso remoto compromessi, con password RDP deboli come principale punto d'ingresso. Le debolezze nelle credenziali hanno inoltre compromesso VPN e firewall, consentendo agli attaccanti di aggirare i controlli di autenticazione e infiltrarsi nei sistemi critici.

Vettori di attacco iniziali

Gli MSP, in particolare, sono diventati bersagli prioritari, subendo attacchi attraverso gli stessi vettori di compromissione osservati in altri settori. La nostra analisi ha evidenziato che il phishing è rimasto il metodo più diffuso, con 62 attacchi documentati, seguito dall'abuso di RDP, dallo sfruttamento di vulnerabilità non risolte, e dalle compromissioni della supply chain. Queste tecniche, pur non essendo nuove, continuano a dimostrarsi sorprendentemente efficaci, segnalando carenze persistenti nelle pratiche di sicurezza di base.



La consapevolezza e la gestione del rischio

Phishing e furto di credenziali sono particolarmente insidiosi perché sfruttano l'errore umano e la fiducia intrinseca nei processi aziendali. Per questo motivo, la formazione sulla sicurezza non è più un'opzione, ma un elemento imprescindibile per una strategia di difesa efficace. Con la NIS2, la Security Awareness Training[1] diventa un requisito normativo e un pilastro essenziale di una postura di sicurezza robusta.

Gli attacchi RDP e le vulnerabilità non risolte evidenziano i pericoli di un'infrastruttura mal gestita, offrendo agli attaccanti un accesso diretto ai sistemi critici. Inoltre, lo sfruttamento delle relazioni di fiducia tra aziende dimostra come l'interconnessione dei moderni ecosistemi digitali possa amplificare il rischio, trasformando un singolo punto debole in un varco aperto per gli aggressori.

[1] Acronis può supportare i partner nel rispetto dei requisiti grazie al SAT integrato nella console. Servizio gestito Security Awareness Training di Acronis, progettato per gli MSP

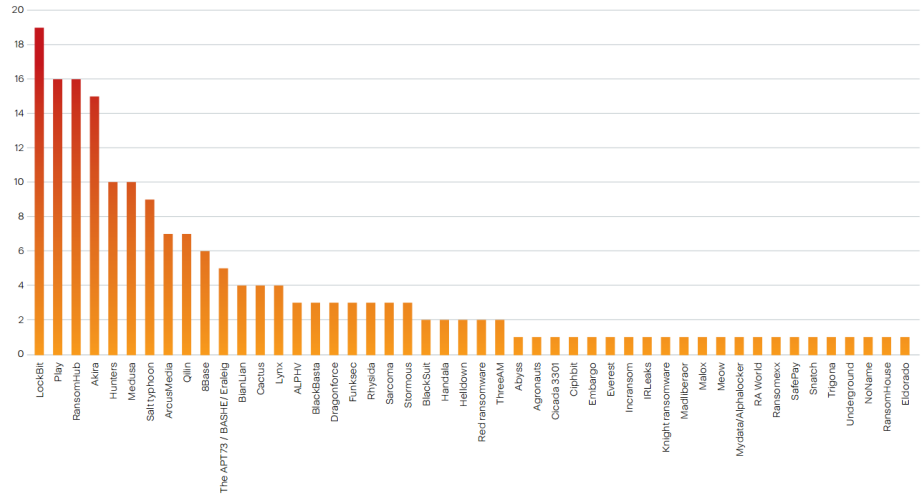
Per mitigare queste minacce, MSP e MSSP devono adottare una strategia di sicurezza proattiva, basata su:

- gestione continua delle vulnerabilità, per ridurre la superficie di attacco;
- visibilità costante sui sistemi, per rilevare e rispondere rapidamente alle minacce;
- approccio Zero Trust, per limitare l'accesso e minimizzare i danni in caso di compromissione.

Le sfide imposte dalla NIS2 e dall'evoluzione delle minacce cyber richiedono un cambiamento di paradigma: non basta più difendersi, occorre anticipare, individuare e neutralizzare le minacce.

MSP e MSSP nel mirino degli APT: una minaccia in evoluzione

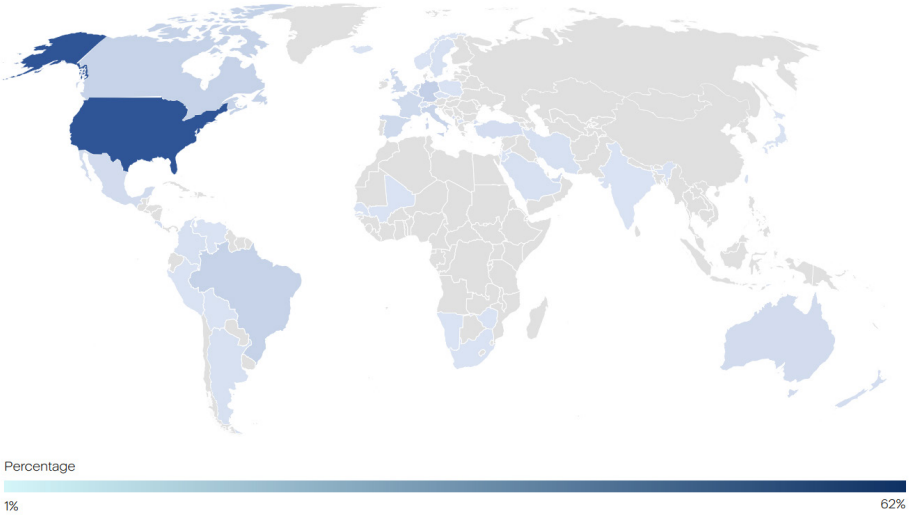
Distribuzione degli attacchi Ransomware per gruppo



Una tendenza emergente, e ancor più preoccupante, è il crescente coinvolgimento di gruppi ransomware legati agli Advanced Persistent Threats (APT) negli attacchi contro MSP, MSSP e operatori telco. Sebbene questi attori sofisticati utilizzino tattiche consolidate, come lo sfruttamento di dispositivi di rete vulnerabili e l'uso di tecniche "Living-off-the-Land" (LotL) per garantire accessi persistenti ai sistemi critici, la motivazione si estende oltre il semplice guadagno economico, arrivando a includere attività di spionaggio. Un esempio eclatante è rappresentato dagli attacchi condotti da Salt Typhoon, gruppo APT noto per aver preso di mira le infrastrutture di

telecomunicazione commerciali degli Stati Uniti[2]. Questa evoluzione del panorama delle minacce sottolinea come gli MSP non siano più solo obiettivi opportunistici, ma vettori strategici per attacchi ad alto impatto. Per mitigare questi rischi in continua evoluzione, gli MSP, MSSP devono rafforzare le proprie difese adottando strumenti avanzati di rilevamento delle minacce, gestione continua delle patch e monitoraggio rigoroso delle credenziali di accesso. L'implicazione diretta della crescente presenza di gruppi APT è la necessità di un approccio immediato e più robusto alla sicurezza delle infrastrutture MSP.

I paesi più colpiti dagli attacchi contro MSP, MSSP e Telco



Secondo le analisi condotte da TRU, il numero di attacchi informatici contro MSP e MSSP è aumentato del 16% rispetto al 2023, consolidando ulteriormente il loro status di bersagli di alto valore per i cybercriminali. Nel 2024, su 5.264 incidenti segnalati a livello globale, 185 hanno coinvolto MSP, MSSP e operatori Telco, confermando come gli attaccanti continuino a sfruttare il ruolo centrale di questi fornitori nella gestione delle infrastrutture IT dei clienti.

[2] https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

In Italia gli attacchi contro MSP e società di consulenza IT hanno rappresentato il 4% degli incidenti segnalati (7 su 185 a livello globale) nel 2024. Se confrontiamo la percentuale di aziende colpite da attacchi ransomware in Italia nel 2023 (11 su 184) con quella del 2024 (7 su 146), il valore complessivo si mantiene intorno al 5-6%.

Con l'entrata in vigore della Direttiva NIS2, MSP e MSSP devono affrontare responsabilità di conformità più stringenti, che li obbligano a implementare misure di sicurezza più avanzate e a segnalare tempestivamente eventuali incidenti. L'obiettivo è migliorare la resilienza complessiva dei settori critici, innalzando gli standard di sicurezza lungo tutta la supply chain.

L'abuso degli strumenti RMM negli attacchi cyber

Una delle tendenze più allarmanti nel panorama delle minacce informatiche è lo sfruttamento degli strumenti di Remote Monitoring and Management (RMM) da parte degli attaccanti per condurre intrusioni stealth e persistenti. Gli strumenti RMM sono una componente essenziale delle moderne operazioni IT, consentendo a MSP, MSSP e team IT interni di gestire da remoto sistemi distribuiti, applicare patch e aggiornamenti di sicurezza, e risolvere problemi senza interventi in presenza. Tuttavia, le stesse funzionalità che rendono gli RMM strumenti indispensabili li trasformano in obiettivi altamente appetibili per i cybercriminali. L'accesso remoto, se mal gestito, diventa un'arma a doppio taglio: mentre migliora l'efficienza operativa, introduce anche rischi di sicurezza significativi.

Oggi, gli RMM vengono armati dagli attaccanti per eludere i controlli di sicurezza, muoversi lateralmente all'interno delle reti e distribuire payload ransomware. Piuttosto che introdurre codice malevolo che potrebbe attivare alert di sicurezza, gli attori delle minacce abusano di applicazioni fidate già presenti nell'ambiente target—a riprova dell'efficacia delle tecniche LotL precedentemente menzionate.

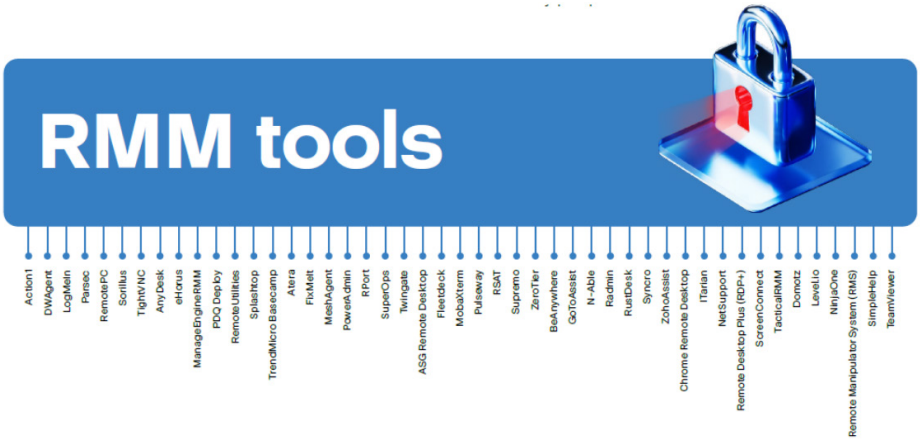
Questo approccio consente agli aggressori di bypassare le misure di protezione degli endpoint, mimetizzarsi con l'attività amministrativa legittima e mantenere la persistenza a lungo termine. I cybercriminali sfruttano autenticazioni deboli, configurazioni errate o vulnerabilità irrisolte negli RMM per infiltrarsi nelle reti, aumentare i privilegi e condurre operazioni malevole mascherandole da attività legittime.

Dopo aver ottenuto l'accesso iniziale, gli attaccanti possono anche installare agenti RMM non autorizzati attraverso tecniche come phishing, ingegneria sociale ed exploit su software vulnerabili. Attori delle minacce hanno inoltre utilizzato social engineering per convincere utenti a scaricare e avviare strumenti RMM portatili, garantendosi un accesso remoto persistente ai sistemi compromessi.

La comparsa di strumenti RMM non riconosciuti all'interno di una rete è spesso un indicatore chiave di compromissione.

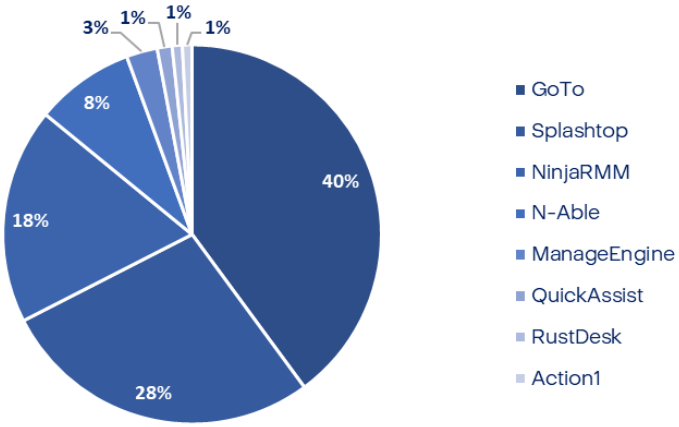
Nel nuovo report Acronis CyberThreats H2[3], abbiamo analizzato i sistemi RMM a livello globale e i dati della nostra telemetria mostrano che, in molte organizzazioni, vengono utilizzati più pacchetti software contemporaneamente, spesso senza un chiaro vantaggio. Questa frammentazione facilita ulteriormente gli attaccanti, permettendo loro di introdurre i propri strumenti senza destare sospetti.

Attualmente, oltre 47 strumenti RMM noti rappresentano un vero e proprio "tallone di Achille" della sicurezza aziendale, spaziando da piattaforme commerciali ampiamente utilizzate a soluzioni meno conosciute.



RMM più conosciuti

[3] https://www.acronis.com/en-us/resource-center/resource/acronis-cyberthreats-report-h2-2024/



RMM più utilizzati in Italia secondo la telemetria di Acronis (H2 2024)

I gruppi Ransomware e il loro abuso degli strumenti RMM

Considerando la frequenza degli attacchi ransomware, è essenziale evidenziare alcuni dei principali attori delle minacce e il loro utilizzo degli RMM per massimizzare l'impatto degli attacchi.

RMMs/RaaS	Cactus	BianLian	ALPHV	LockBit	Medusa	Royal	RansomHub	BlackBasta	Akira	PLAY
Action1				©						
Atera		©	©	©		©		©		
ConnectWise ScreenConnect			©	©		©	©	©		©
GoTo								©		
LogMeIn						©				
ManageEngine										
N-Able					©		©			
NinjaRMM										
QuickAssist								©		©
RustDesk									©	©
Splashtop	©	©	©	©			©	©		©
SuperOps	©									
Teamviewer		©	©	©					©	©

RMM abusati dai gruppi ransomware

1. Cactus Ransomware

Gli operatori di Cactus adottano un approccio diverso, basandosi su tecniche LotL per evitare il rilevamento. Utilizzano strumenti di rete legittimi come PowerShell, Chisel e Rclone, evitando di generare allerte di sicurezza. Nel 2023, Cactus ha iniziato ad abusare di Qlik Sense per l'accesso iniziale e di strumenti come ManageEngine UEMS e AnyDesk per la persistenza. Il gruppo ha anche incorporato Splashtop e SuperOps RMM per il controllo remoto, oltre a Cobalt Strike per il movimento laterale.

2. LockBit Ransomware

LockBit si è confermato uno dei gruppi ransomware più attivi ed efficaci nel 2024. Nel primo trimestre, i suoi affiliati hanno sfruttato zero-day in ConnectWise ScreenConnect, un RMM ampiamente utilizzato. Le vulnerabilità CVE-2024-1709 e CVE-2024-1708, con punteggi CVSS rispettivamente di 10/10 e 8,4/10, hanno permesso agli attaccanti di bypassare l'autenticazione e ottenere accesso non autorizzato, esponendo oltre 8.000 istanze a livello globale. LockBit ha inoltre sfruttato TeamViewer per infiltrarsi nelle reti target, dimostrando una notevole capacità di adattamento nello sfruttare strumenti RMM di fiducia per portare a termine le proprie operazioni.

3. Play Ransomware

Nel 2024, il gruppo Play è stato responsabile del 7,5% degli attacchi ransomware globali (355 casi), di cui 16 mirati agli MSP. Dopo essersi inizialmente concentrato sull'America Latina (soprattutto Brasile), il gruppo ha ampliato il proprio raggio d'azione per colpire fornitori di servizi in Nord America ed Europa. Play ha sfruttato strumenti RMM per compromettere più reti di clienti attraverso un singolo punto di accesso, amplificando notevolmente l'impatto delle violazioni.

Le tecniche MITRE più utilizzate

Con l'evoluzione sempre più rapida delle minacce informatiche, la protezione delle reti aziendali richiede una priorità strategica sulle tecniche più frequentemente utilizzate dagli avversari. Basandosi sul framework MITRE ATT&CK, che classifica le azioni degli attaccanti in tattiche, tecniche e procedure (TTPs), sono state identificate cinque tecniche critiche che si sono dimostrate altamente efficaci e particolarmente difficili da rilevare. Le aziende, e in particolare gli MSP e gli MSSP, devono monitorare con estrema attenzione queste metodologie per rafforzare le proprie difese e proteggere le infrastrutture dei clienti.

Uno dei dati più significativi emersi nel 2024 è stato l'aumento dell'uso dei **BITS Jobs (Background Intelligent Transfer Service – T1197)**, una tecnica che consente ai cybercriminali di programmare ed eseguire download malevoli in background senza destare sospetti.

In Italia, i BITS Jobs sono stati osservati come una delle tecniche più frequentemente sfruttate dagli attaccanti; tuttavia, il primo posto è ancora occupato dagli script PowerShell (T1059.001), utilizzati per mantenere la persistenza e lanciare ulteriori azioni malevole senza attivare i tradizionali sistemi di sicurezza. Per migliorare il proprio livello di sicurezza, MSP e MSSP devono comprendere a fondo queste tecniche chiave, che giocano un ruolo fondamentale nei cyberattacchi moderni. Dare priorità al rilevamento e alla mitigazione di queste tattiche ad alto rischio, soprattutto quelle che sfruttano strumenti di sistema legittimi come BITS Jobs e PowerShell, permette agli MSP di anticipare le minacce emergenti e rafforzare le difese contro avversari sempre più sofisticati. Grazie a questa conoscenza, le organizzazioni possono implementare strategie di monitoraggio più avanzate, attività di ricerca delle minacce (threat hunting) e misure di sicurezza più efficaci, riducendo il rischio di compromissione dovuto all'utilizzo di tecniche di attacco avanzate.

BITS Jobs (T1197)

Descrizione: Il BITS è uno strumento a riga di comando deprecato, comunemente abusato per scaricare ed eseguire payload malevoli sotto la copertura di un legittimo servizio di Windows.

Rilevamento: Monitorare la creazione e l'esecuzione di BITS Jobs, soprattutto se contengono parametri insoliti o fanno riferimento a URL esterni sospetti. Prestare attenzione all'uso inaspettato di bitsadmin o dei comandi PowerShell legati a BITS.

Mitigazione: Disabilitare BITS e sostituirlo con cmdlet PowerShell più sicuri, applicare restrizioni di rete per impedire download non autorizzati, implementare soluzioni EDR (Endpoint Detection and Response) per monitorare i processi di sistema e l'attività di rete.

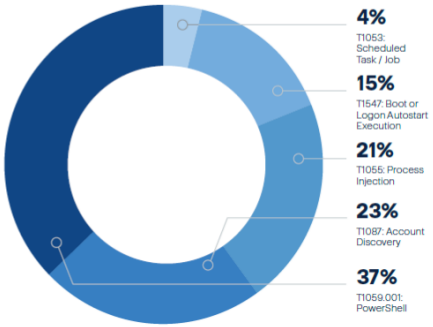
I dati di telemetria globale, raccolti da Acronis Cyber Protect Advanced Security + XDR tra il 1° aprile e il 31 dicembre 2024, hanno identificato le cinque tecniche di attacco più frequentemente utilizzate dai cybercriminali. Questi risultati evidenziano l'evoluzione delle tattiche adottate dagli attaccanti in varie regioni e settori, sottolineando l'importanza di adottare una difesa proattiva e adattiva.

Tecniche MITRE ATT&CK più frequenti, Q2-Q4 2024

The collected information is based on Acronis telemetry from Acronis XDR from April, 1 2024 to December 31, 2024.

No.	Technique ID	Technique name
1	T1059.001	PowerShell
2	T1087	Account Discovery
3	T1055	Process Injection
4	T1547	Boot or Logon Autostart Execution
5	T1053	Scheduled Task / Job

Top 5 most frequently seen mitre att&ck techiques, Q2-Q4 2024



1. PowerShell (T1059.001)

Descrizione: Gli attori delle minacce sfruttano PowerShell, un potente strumento di scripting, per eseguire script malevoli, scaricare payload dannosi o offuscare comandi, mascherandosi tra le normali attività di sistema.

Rilevamento: Monitorare i log di PowerShell per individuare argomenti sospetti nella riga di comando, payload codificati in base64 o connessioni di rete anomale avviate dagli script. Le soluzioni EDR (Endpoint Detection and Response) possono segnalare comportamenti sospetti.

Contenimento: Limitare e monitorare l'uso di PowerShell (ad esempio, impedendo l'esecuzione da percorsi insoliti come C:/Temp). Attivare logging avanzato e script block logging per una maggiore visibilità.

2. Account discovery (T1087)

Descrizione: Gli attaccanti interrogano informazioni sugli utenti e sugli account per comprendere l'ambiente target e individuare account privilegiati per il movimento laterale. Ciò può includere comandi come net user o query LDAP in ambienti Active Directory.

Rilevamento: Monitorare i log per attività di enumerazione degli account eccessive o insolite. Prestare attenzione ai sistemi che eseguono comandi amministrativi inaspettati o che interrogano i controller di dominio.

Contenimento: Limitare la visibilità delle informazioni sugli account tramite il principio del privilegio minimo. Disabilitare gli account non necessari e utilizzare strumenti come honeypot accounts per rilevare tentativi di enumerazione.

3. Process injection (T1055)

Descrizione: Questa tecnica consente agli attaccanti di iniettare codice malevolo in processi legittimi, evitando il rilevamento ed eseguendo il codice in modo stealth. Esempi includono DLL injection e APC (Asynchronous Procedure Call) injection.

Rilevamento: Monitorare le chiamate API sospette (es. CreateRemoteThread). Controllare i processi per modifiche inaspettate alla memoria o comportamenti anomali. Le soluzioni EDR possono fornire un rilevamento in tempo reale.

Contenimento: Implementare EDR con rilevamento basato sul comportamento. Abilitare funzionalità di integrità della memoria. Applicare rigide policy di controllo delle applicazioni per ridurre le opportunità di sfruttamento.

4. Boot or logon autostart execution (T1547)

Descrizione: Gli avversari ottengono persistenza **aggiungendo entries malevole nei Registry Run keys, nelle cartelle di avvio o nei task schedulati**, assicurando l'esecuzione all'avvio del sistema o al login dell'utente.

Rilevamento: Monitorare **modifiche ai Registry Run keys**, alla cartella di avvio e ai task schedulati. Utilizzare analisi comportamentale per rilevare **programmi inaspettati che si avviano automaticamente**.

Contenimento: Implementare la "whitelist delle applicazioni" per consentire solo l'esecuzione di software autorizzato. Limitare i permessi relativi alla modifica delle impostazioni di avvio. Utilizzare i Group Policy Objects (GPO) per applicare restrizioni sulle configurazioni di avvio.

5. Scheduled task / Job (T1053)

Descrizione: Questa tecnica, ampiamente sfruttata, consente agli attaccanti di abusare delle funzionalità di programmazione delle attività di Windows (Task Scheduler) per eseguire codice malevolo in modo persistente o a intervalli specifici. Questi task si mimetizzano tra le normali attività di sistema, facilitando l'evasione dal rilevamento.

Rilevamento: Monitorare la creazione e la modifica dei task schedulati, ponendo particolare attenzione a: nomi insoliti, orari di esecuzione anomali, argomenti sospetti nella riga di comando. Analizzare i log di sistema per individuare task avviati da account inattesi o fuori dagli orari operativi normali.

Contenimento: Limitare i permessi per la creazione o modifica dei task schedulati solo a utenti autorizzati. Effettuare audit regolari dei task programmati per identificare e rimuovere entries non autorizzate. Implementare strumenti EDR per rilevare e bloccare comportamenti malevoli associati ai task. Applicare policy per prevenire l'esecuzione non autorizzata di script.

È fondamentale concentrare gli sforzi sul rilevamento delle tecniche più pericolose, come l'abuso di PowerShell, l'estrazione delle credenziali (credential dumping) e lo sfruttamento dei servizi remoti, per rafforzare la protezione contro attacchi sempre più avanzati e complessi.

Prevenzione: applicare policy di sicurezza rigorose; implementare segmentazione della rete; utilizzare la "whitelist delle applicazioni" per bloccare l'esecuzione di software non autorizzato.

Rilevamento: sfruttare strumenti avanzati come EDR e SIEM (Security Information and Event Management) per il monitoraggio in tempo reale e l'analisi comportamentale.

Risposta: collaborare con un SOC gestito per garantire un monitoraggio 24/7 e una risposta rapida agli incidenti. Automatizzare le risposte dove possibile per reagire più velocemente e limitare l'impatto iniziale degli attacchi.

Migliorare la sicurezza degli MSP in conformità con la NIS2: una strategia completa

Combinando misure proattive con capacità avanzate di rilevamento, gli MSP possono anticipare meglio le tattiche avversarie e creare un ecosistema di sicurezza che renda significativamente più difficile per gli attaccanti muoversi lateralmente e mantenere la persistenza. La recente Direttiva NIS2 sottolinea la necessità per le organizzazioni di adottare pratiche di cybersecurity solide e implementare misure adeguate a proteggere le infrastrutture critiche. Con questo obiettivo, ecco alcune raccomandazioni allineate alla NIS2.

10 azioni fondamentali per garantire la conformità alla NIS2

Prevenzione: rafforzare le difese di base

1. **Formazione sulla consapevolezza della sicurezza:** poiché i criminali informatici si affidano sempre più a tecniche di social engineering e phishing, è fondamentale formare i dipendenti degli MSP a riconoscere attività sospette e adottare le migliori pratiche di cybersecurity. La formazione regolare garantisce che il personale sia in grado di individuare i tentativi malevoli prima che si trasformino in incidenti di sicurezza. La Direttiva NIS2 richiede alle aziende di formare regolarmente il personale sulla consapevolezza della sicurezza informatica, in particolare coloro che hanno accesso a sistemi critici.
2. **Autenticazione a più fattori (MFA):** l'implementazione dell'MFA su account privilegiati e sistemi critici garantisce che gli attaccanti non possano facilmente compromettere le credenziali. Questo metodo di autenticazione multistrato rappresenta una difesa cruciale contro gli accessi non autorizzati. NIS2 sottolinea l'importanza di implementare solidi meccanismi di controllo degli accessi, in particolare per i sistemi che trattano dati sensibili o critici.
3. **Segmentazione della rete:** segmentare le reti degli MSP in zone isolate assicura che una violazione in una parte della rete non si traduca in una compromissione su larga scala. Questa tecnica limita il movimento laterale, rendendo significativamente più difficile per gli attaccanti accedere ad altre aree della rete una volta all'interno. Secondo la NIS2, le aziende devono implementare misure per limitare l'estensione delle violazioni e ridurre i danni in caso di attacco.
4. **Gestione delle patch di aggiornamento:** è fondamentale implementare un programma efficace per garantire l'applicazione tempestiva degli aggiornamenti di sicurezza ai sistemi vulnerabili. L'applicazione tempestiva delle patch aiuta a ridurre l'esposizione alle vulnerabilità note, diminuendo la superficie di attacco. La NIS2 impone alle organizzazioni di mantenere i sistemi e le applicazioni aggiornati con le ultime patch di sicurezza per mitigare il rischio di sfruttamento.
5. **Crittografia dei dati e prevenzione della perdita di dati:** la crittografia dei dati sensibili in transito e a riposo garantisce che, anche se intercettati, i dati rimangano protetti. Inoltre, l'implementazione di soluzioni di Data Loss Prevention (DLP) aiuta a prevenire l'esfiltrazione non autorizzata di informazioni critiche. NIS2 richiede alle aziende di proteggere le informazioni critiche garantendone la riservatezza, l'integrità e la disponibilità, anche attraverso tecniche di crittografia.

Rilevamento: monitoraggio proattivo delle minacce

6. **Monitoraggio continuo e threat intelligence**: l'implementazione di un monitoraggio di rete in tempo reale e l'integrazione della threat intelligence consentono agli MSP di anticipare le minacce emergenti. Grazie a feed di minacce e analisi di sicurezza, le organizzazioni possono identificare precocemente gli indicatori di compromissione (IoC) e contrastare metodi di attacco in evoluzione. NIS2 enfatizza la necessità di adottare sistemi di monitoraggio continuo per rilevare rapidamente anomalie e potenziali minacce.
7. **Sicurezza degli endpoint con EDR/XDR:** le soluzioni di Endpoint Detection and Response (EDR) ed Extended Detection and Response (XDR), dotate di AI e analisi comportamentale, sono essenziali per rilevare malware, movimenti laterali e altre attività malevole. Queste tecnologie avanzate forniscono una visione più dettagliata del comportamento degli endpoint e aiutano a individuare le minacce nascoste in fase precoce. La NIS2 sottolinea la necessità di sistemi avanzati di rilevamento delle minacce come parte di una strategia di difesa completa.

Risposta: azioni rapide ed efficaci

8. **Pianificazione della risposta agli incidenti:** sviluppare e testare regolarmente un piano di risposta agli incidenti garantisce che gli MSP possano reagire rapidamente ed efficacemente a un incidente di sicurezza. Avere ruoli e procedure predefinite riduce la confusione durante un attacco e assicura un contenimento rapido. NIS2 sottolinea l'importanza di una chiara strategia di risposta agli incidenti per consentire alle organizzazioni di riprendersi da violazioni di sicurezza mantenendo la continuità operativa.
9. **Correzione (Remediation) automatizzata:** l'uso di strumenti EDR/XDR con funzionalità di correzione (remediation) integrata permette agli MSP di neutralizzare automaticamente le minacce, riducendo i tempi di risposta e minimizzando le interruzioni operative. Questa automazione è cruciale per impedire agli attaccanti di mantenere la persistenza o intensificare i loro attacchi. Inoltre, la Direttiva NIS2 richiede l'adozione di meccanismi di risposta automatizzati per limitare la durata e l'impatto degli incidenti di sicurezza.
10. **Analisi post-incidente:** dopo un incidente di sicurezza, è fondamentale eseguire un'analisi approfondita per identificare la causa principale e implementare miglioramenti nelle difese. Questa analisi dovrebbe includere l'esame dei metodi utilizzati dall'attaccante per ottenere l'accesso, la valutazione dell'efficacia dei controlli esistenti e la misurazione dell'impatto complessivo dell'inci-

dente. La Direttiva NIS2 impone la segnalazione post-incidente e l'adozione di misure correttive per prevenire future violazioni simili.

Conclusione

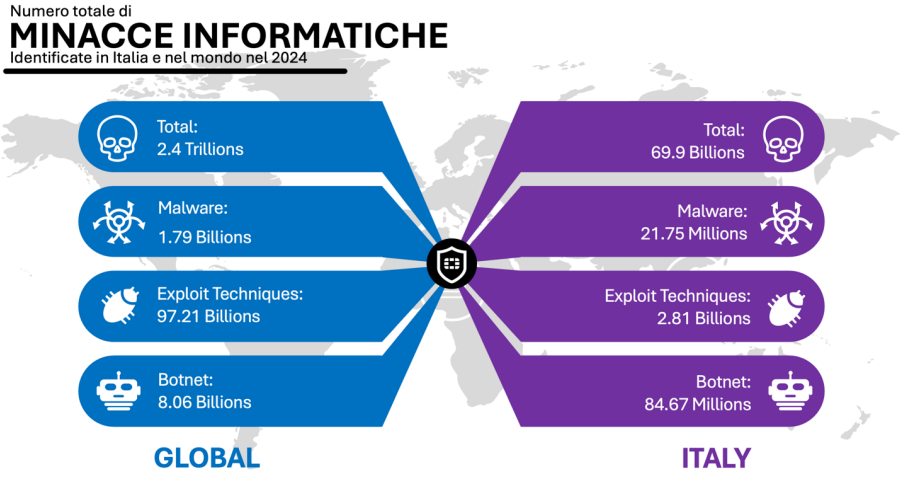
Sebbene la conformità alla NIS2 possa sembrare un onere normativo, deve essere vista come un'opportunità per elevare la maturità della cybersecurity. La direttiva rafforza l'idea che la sicurezza informatica non sia solo un problema IT, ma un pilastro fondamentale della resilienza operativa, della stabilità economica e della sicurezza nazionale. Le aziende italiane devono agire ora per valutare la loro esposizione, migliorare i protocolli di sicurezza e promuovere una cultura della consapevolezza informatica. Coloro che abbracciano questo cambiamento non solo soddisferanno le aspettative normative, ma otterranno anche un vantaggio strategico in un'era in cui la resilienza informatica definisce il successo a lungo termine. La collaborazione e l'innovazione, unite a un impegno continuo nella cybersecurity, permetteranno agli MSP/MSSP e alle aziende che forniscono servizi di sicurezza informatica di mantenere il ruolo di partner affidabili, assicurando la protezione del panorama digitale per i propri clienti.

Infrastrutture critiche sotto attacco

(A cura di Aldo Di Mattia, Fortinet)

Nel corso del 2024 i cyber criminali hanno intensificato gli attacchi informatici alle infrastrutture critiche italiani e globali prendendo di mira in modo specifico i distinti settori di cui sono composte. Le infrastrutture critiche risultano sempre più appetibili a tutte le categorie di attaccanti informatici, dai cyber criminali ai quali permettono di massimizzare i proventi illeciti, agli attacchi sponsorizzati dai governi nei contesti di spionaggio e competitività, fino agli hacktivisti. Analizzando i dati estratti dai FortiGuard Labs di Fortinet, emerge che l'**Italia è stata colpita dal 2,91% delle minacce globali, rispetto allo 0,79% dell'anno precedente**. Esaminando le minacce specifiche, si osservano le seguenti percentuali per l'Italia rispetto ai dati globali:

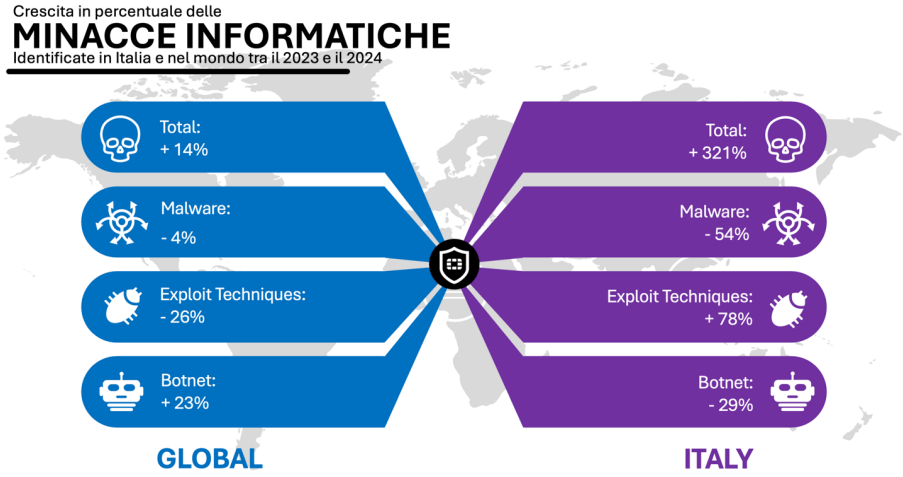
- **1,22% dei malware** individuati complessivamente (2,5% nel 2023)
- **2,89% dei tentativi di exploit** globali (1,18% nel 2023)
- **1,05% delle botnet** intercettate nel mondo (1,81% nel 2023)



Minacce totali riscontrate in Italia e nel mondo nel corso del 2024

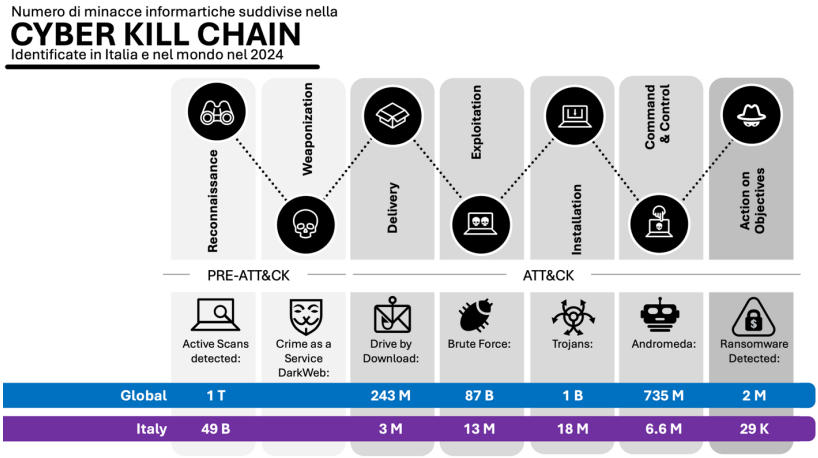
Come di seguito riportato, se già nel 2023 si era registrata una significativa crescita delle minacce totali individuate in Italia e nel mondo, nel corso del 2024 tale incremento è stato ancora più marcato a livello italiano. Inoltre, tra gli aspetti che più pre-

occupano nel 2024 si segnala il cospicuo aumento di **Active Scanning Techniques**, che In **Italia** hanno avuto un incremento del **1.076%,** passando da 4,21 miliardi a 49,46 miliardi. Va precisato che l'incremento totale risulta legato a un picco significativo raggiunto nel mese di Febbraio 2024, laddove nel resto dell'anno il dato resta di poco superiore rispetto l'anno precedente. La crescita a livello **globale** delle stesse attività è stata del **16,71%**, passando da 993 miliardi a 1,16 trilioni. Anche gli attacchi **Denial of Service (DoS)** hanno fatto registrare un forte aumento, passando da 576,63 miliardi a 1,07 trilioni a livello **globale (+85,25%)** e da 657,06 milioni a 4,22 miliardi in **Italia (+542,52%).**



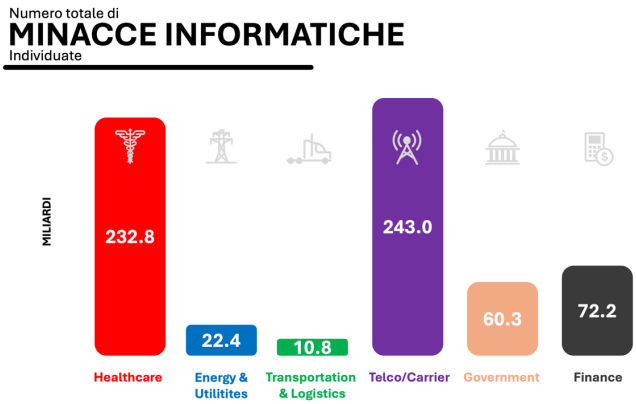
Crescita delle minacce riscontrate in Italia e nel mondo nel 2024 rispetto al 2023

Tutti i dati mostrati sono estratti dai **FortiGuard Labs** e offrono un punto di osservazione peculiare, in quanto indicano le **minacce** informatiche totali **individuate** da Fortinet. I dati includono attacchi, malware e tutte le attività di scansione e intelligence comprese nella fase di Pre-Att&ck ed evidenziano la numerosità dei tentativi di azioni malevole condotte dagli attaccanti in Italia e nel mondo. Andando a collocare le minacce identificate nella Cyber Kill Chain, si hanno i seguenti risultati. I dati sono espressi con l'abbreviazione angloamericana: B=miliardi, M=milioni, K=migliaia.



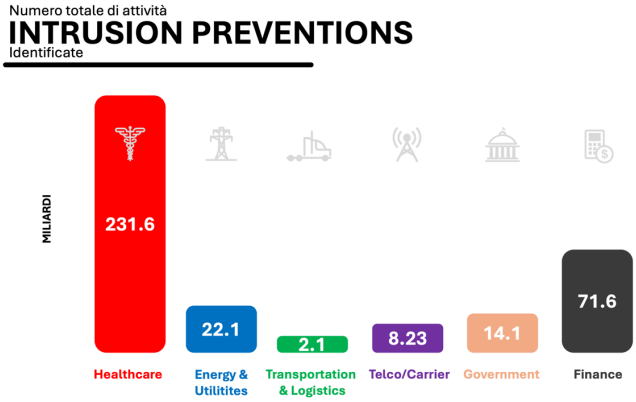
Minacce informatiche suddivise nella Cyber Kill Chain in Italia e nel mondo nel corso del 2024

Come già sottolineato lo scorso anno, il dato relativo alle attività di "Reconnaissance" suscita particolare attenzione sia a livello globale che a livello italiano. La ricognizione comprende tutte le tecniche utilizzate dagli avversari per raccogliere, in modo attivo o passivo, informazioni utili a supportare un attacco. Queste informazioni possono includere dettagli sull'organizzazione, sull'infrastruttura o sul personale della vittima. Per ottimizzare le strategie di difesa, è fondamentale sfruttare al massimo le potenzialità offerte da tecnologie come Deception, Intelligence e AI. Questi strumenti, sebbene essenziali per contrastare le minacce, vengono ancora troppo spesso messi in secondo piano o utilizzati in modo limitato. Andando a suddividere gli attacchi per alcuni mercati specifici delle Infrastrutture Critiche, abbiamo un'importante evidenza di come il settore Sanitario e quello Telco, siano stati specificamente presi d'assalto anche nel corso del 2024.



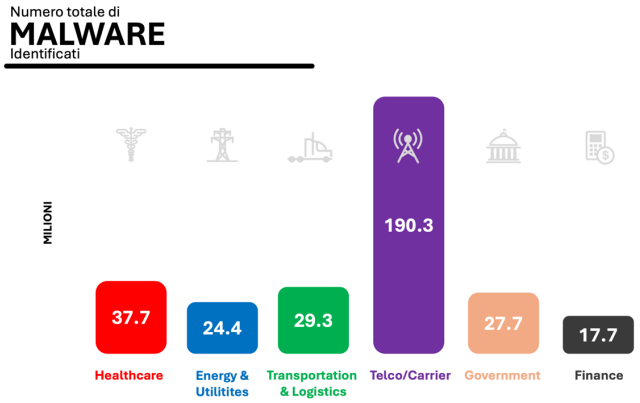
Minacce Informatiche totali nel corso del 2024 per settore

Andando a suddividere le minacce nei distinti mercati delle Infrastrutture Critiche emerge che Sanità e Telco sono i settori più colpiti in termini assoluti.



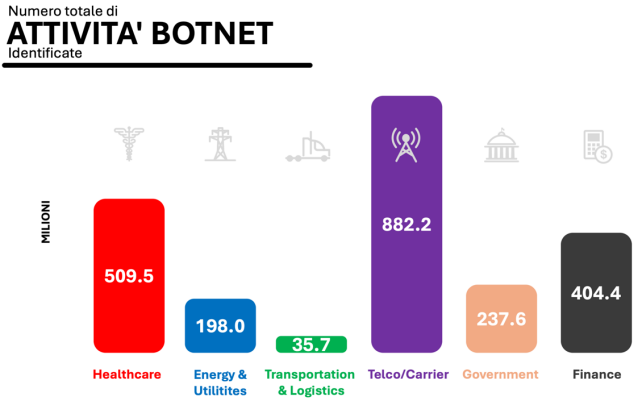
Minacce Informatiche di tipo IPS nel corso del 2024 per settore

Dal punto di vista degli attacchi informatici identificati da sistemi IPS, la Sanità è risultata quella maggiormente colpita. Le scansioni effettuate nella fase "Pre-Att&ck" sono state quelle maggiormente utilizzate dagli attaccanti.



Minacce Informatiche di tipo Malware nel corso del 2024 per settore

Dal punto di vista dei Malware e degli attacchi botnet, sono state le Telco a risultare maggiormente impattate, seguite ancora una volta dalla Sanità.



Minacce Informatiche di tipo Botnet nel corso del 2024 per settore

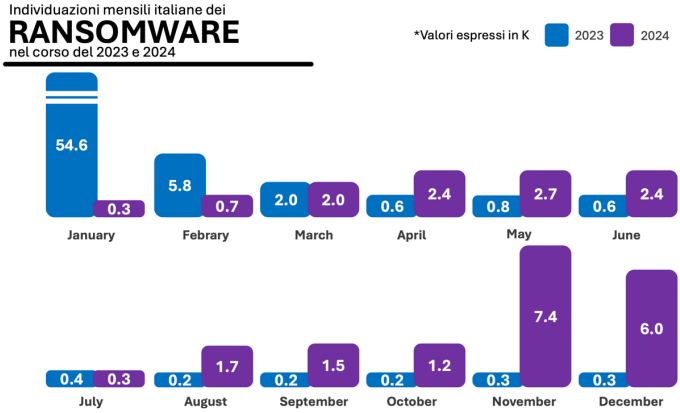
Per meglio esaminare quanto accaduto alle Infrastrutture Critiche nel corso del 2024 cerchiamo di analizzare minacce e dati statistici che inquadrano i settori indicati nei contesti:

- Secure Access Service Edge
- Security Operations

- Operational Technology
- Cloud

Secure Access Service Edge

L'evoluzione del mondo digitale, ogni giorno più connesso e dinamico, deve far fronte sempre più al tema della sicurezza informatica, diventata una priorità assoluta per le aziende e per i singoli individui. I dispositivi connessi, siano essi laptop aziendali, smartphone personali o dispositivi IoT, sono oggi i principali custodi delle informazioni, trovandosi a gestire spesso dati sensibili e privati di importanza rilevante. Questo rende i dispositivi il punto di accesso più vulnerabile alle minacce informatiche, dati confermati anche dalle analisi dei FortiGuard Labs che evidenziano il proliferare di diverse tipologie di attacchi in continua crescita, favoriti dalla scarsa adeguatezza dei sistemi di protezione. Il modello Ransomware-as-a-Service (RaaS) ad esempio, consente ai criminali informatici di affittare o acquistare kit di ransomware pronti all'uso, facilitando la diffusione di attacchi ransomware anche da parte di individui con competenze tecniche limitate. Nell'ultimo trimestre del 2024 in Italia sono stati individuati **14.600 attacchi di tipo ransomware** (a fronte degli **800 dello stesso trimestre nel 2023**).



Ransomware individuato mensilmente durante il 2023 e il 2024 in Italia

Allo stesso modo anche il **Cybercrime-as-a-Service (CaaS)** sta crescendo vertiginosamente, con un'offerta sempre più varia e completa e con servizi offerti nel dark

web contenenti malware, phishing e strumenti di ricognizione. Questo fenomeno amplia le possibilità per i criminali informatici di lanciare attacchi complessi senza dover sviluppare autonomamente gli strumenti necessari. Un tipico esempio di CaaS è legato al trojan TrickBot (come riportato anche nel threat report pubblicato da CSIRT Italia), ancora oggi identificato come target delle botnet più diffuse in Italia (**6.8M di detection di TrickBot nel 2024 in Italia**, pari al 10,1% del totale dei tentativi di Exploit). Un malware identificato per la prima nel 2016 come trojan bancario ma che si è evoluto negli anni cambiando le modalità di attacco negli anni incrementando sempre più il suo volume.

In questo contesto, quindi, risulta essenziale introdurre delle soluzioni in grado di proteggere i dispositivi utente, aziendali e/o personali, in particolare per quanto concerne la navigazione internet, tradizionalmente vettore d'attacco principale per un cybercriminale. Il framework SASE rappresenta un modello implementativo ideale per questi scenari, combinando in un'unica soluzione funzionalità di rete come il Software-Defined Wide Area Network (SD-WAN) e servizi di sicurezza avanzati come il Secure Web Gateway (SWG), il Cloud Access Security Broker (CASB), la protezione firewall-as-a-service (FWaaS) e lo Zero Trust Network Access (ZTNA). Queste componenti, fornite in modalità SaaS, consentono alle organizzazioni di gestire e proteggere in modo centralizzato l'accesso ai dati e alle applicazioni, indipendentemente da dove si trovino gli utenti o i dispositivi, garantendo un'esperienza utente costante e una postura di sicurezza sempre attiva. Nello specifico quello che il framework SASE introduce è una rivoluzione nell'approccio alla sicurezza attraverso il modello Zero-Trust, dove ogni accesso è rigorosamente controllato per garantire che solo utenti e dispositivi autorizzati possano accedere alle risorse aziendali dove è necessario verificare costantemente l'identità e l'integrità degli utenti e dei dispositivi stessi, limitando l'accesso alle risorse solo a quelli autorizzati ed eliminando il concetto di trusted-network attraverso la logica del "mai fidarsi, verificare sempre".

Adottando un'architettura SASE, le organizzazioni possono rafforzare il proprio livello di sicurezza, proteggendo efficacemente utenti, dispositivi e dati dalle minacce informatiche in continua evoluzione. Le aziende possono ridurre i rischi provenienti da Malware e Ransomware, controllando in maniera adeguata gli scenari di Phishing, e implementando soluzioni basate su agent in grado di identificare eventuali vulnerabilità del software a bordo dei dispositivi. Il tutto garantendo un controllo dei flussi di traffico da e verso le applicazioni corporate e un'esperienza utente di navigazione sicura, sostenuta dall'intelligence di sicurezza fornita dai principali centri di ricerca.

Security Operations

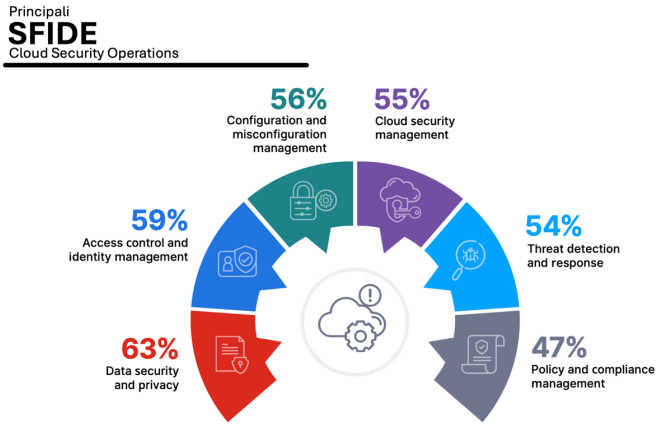
L'analisi dei dati relativi alle attività criminali informatiche del 2024 disegna uno scenario in fase altamente evolutiva dal punto di vista sia della tipologia che della quantità delle minacce. A livello globale, come già anticipato nelle previsioni Fortinet riportate nell'ultima edizione del rapporto Clusit 2024, sono stati rilevati aumenti a doppia cifra di attacchi di tipo **Reconnaissance (+16,71%)**, **Botnet (+ 15,10%)** e **Denial of Service (+85,25%).** Le motivazioni più plausibili dietro questi numeri sono naturalmente diverse, ma un elemento comune è sicuramente l'aumento esponenziale dell'utilizzo dell'**Intelligenza Artificiale** (**AI**) quale strumento avanzato a disposizione dei gruppi criminali. Con una nuova vulnerabilità identificata e pubblicata in media ogni 17 minuti (dato 2024), gli aggressori beneficiano delle grandi capacità di automazione offerte dall'Intelligenza Artificiale per aumentare di diversi ordini di grandezza la portata delle campagne, avvalendosi di uno strumento che copre tutto il ciclo-vita dell'attacco, dalla Reconnaissance all'esfiltrazione dei dati. L'Intelligenza Artificiale sta sempre di più ridefinendo il panorama delle minacce informatiche, rendendo gli attacchi più sofisticati, scalabili e accessibili. L'AI non solo potenzia gli attacchi, ma "democratizza" il cybercrime, consentendo a un maggior numero di individui con competenze tecniche limitate di sferrare attacchi sofisticati. I numeri di seguito riportati provengono dalle rilevazioni di FortiGuard Labs, l'organizzazione globale di Threat Intelligence e Ricerca di Fortinet sulle minacce. Il 2024 ha fatto registrare un numero di attività malevole, a livello globale, pari a **2,4 Trilioni**, con un incremento del **14,29% rispetto l'anno precedente**. Il numero di rilevazioni "Reconnaissance" è pari al **46,02%** del totale (**1,16 Trilioni**) con un incremento del **+16,71%** sul 2023, mentre la quantità di DoS registrati è del **43,86%** (**1,07 Trilioni**) con un incremento del **+85,25%** sull'anno precedente. In linea con la tendenza globale, i numeri relativi alle attività di cybercrime in Italia nel 2024 confermano un trend, purtroppo, in ascesa. Il numero totale delle minacce rilevate è di **69,9 Miliardi** (**2,91%** del totale con un incremento annuale del **+268,35%**). Il dato relativo alle attività di **Reconnaissance** è particolarmente significativo, poiché esso costituisce il **69,60%** del totale con un incremento annuale del **+1.075,90%.** A seguire le attività di **Credential Access/Brute Force**, con il **19%** del totale e un incremento sul 2023 di **+102,87%.** Nonostante la flessione YoY (Year over Year) di **Malware Distribution** (**-53,83%**) **Ransomware** (**-56,73%**) e **Botnet** (**-31,51%**), si rileva un sostanziale incremento di attacchi **DoS** (**+542,52%**) e la crescita esponenziale di una nuova famiglia di attacchi, ovvero **Cryptojacking** con **+778,28%.** Il **Cryptojacking** è un attacco informatico subdolo che sfrutta la potenza di calcolo del dispositivo vittima per "minare" criptovalute. In sostanza si fa uso dei vettori classici di propagazione malware, instal-

lando codice malevolo sul sistema violato, che invece di produrre attività di controllo remoto o cifratura dei dati, lavora in background consumando risorse e generando criptovaluta per l'attaccante. Questo tipo di attacco, vista la diffusione sempre maggiore delle criptovalute, è in aumento principalmente poiché è più redditizio e meno rischioso rispetto ad altri attacchi come i ransomware. Inoltre, il Cryptojacking è più difficile da individuare e permette ai cyber criminali di generare profitti costanti senza attirare troppa attenzione.

In conclusione, il 2024 ha visto una crescita esponenziale delle minacce informatiche, alimentate dall'uso dell'AI nel cybercrime. L'aumento degli attacchi di Reconnaissance, DoS e la comparsa del Cryptojacking evidenziano la necessità di strategie di difesa avanzate. Per contrastare efficacemente queste minacce, è fondamentale adottare soluzioni di sicurezza integrate con forte presenza AI, in grado di rilevare e contenere anomalie e pattern sospetti in tempo reale. Investire in sistemi di protezione, analisi e orchestrazione, e piattaforme di Threat Intelligence è cruciale. Soluzioni come SIEM, SOAR e sistemi di Deception rappresentano senz'altro la base essenziale di un moderno SOC. La formazione continua del personale sulle nuove minacce e l'implementazione di politiche di sicurezza robuste completano un approccio olistico per proteggere le aziende nel panorama digitale in continua evoluzione.

Cloud

Dati interessanti relativi agli ambienti Cloud ci vengono forniti dal rapporto Fortinet 2025 "State of Cloud Security Report", pubblicato da Cybersecurity Insiders, che ha coinvolto 873 professionisti a livello globale. Il rapporto, basato su sondaggi, fotografa in maniera chiara la crescita delle strategie di adozione del Cloud, ponendo a 78% il valore del modello MultiCloud, valore continuamente in crescita già da diversi anni. Andando a esaminare le principali sfide di sicurezza in ambito Cloud troviamo al primo posto le tematiche di **Data Security**, menzionata come priorità dal **63% degli intervistati**, valore in crescita rispetto al 58% del 2024. Subito dopo, con il **59% e 56%** troviamo invece la **gestione degli accessi** e della **configurazione degli asset Cloud**, tematiche inerenti agli ambienti Cloud e perfettamente in linea con le minacce informatiche legate alle **Active Scanning Techniques/Reconnaissance** menzionate in precedenza.



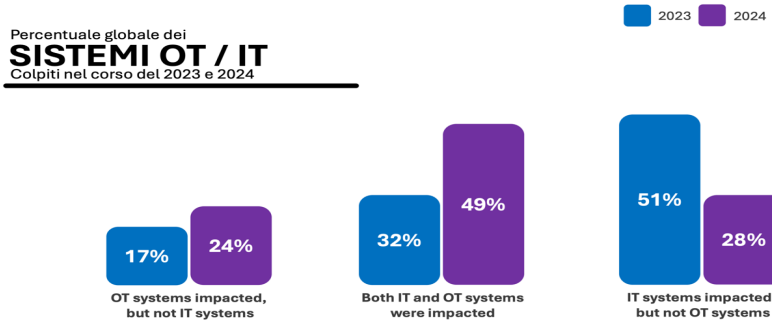
Principali sfide relative alle Cloud Security Operations

Il **59%** dei partecipanti ha dunque indicato tra le sfide principali la **Gestione degli accessi inefficace**, che riguarda l'inadeguatezza nella creazione e gestione delle identità e degli accessi. Elementi che possono portare a permessi eccessivi, impersonificazione e una gestione crittografica debole, aumentando il rischio di accessi non autorizzati e di conseguenza allo sviluppo di attività illecite di Activity Scanning da parte di risorse o identità fuori controllo. Questo dato risulta leggermente in crescita con il rapporto dello scorso anno, dove la gestione degli accessi è stata menzionata dal 54% degli intervistati. Il **56%** infine ha indicato le **Configurazioni errate e controllo delle modifiche inadeguato** tra le sfide più importanti, riferendosi alla configurazione impropria delle risorse cloud, la gestione inefficace delle modifiche e in generale la mancanza di rispetto delle best practices nel cloud. Tutti elementi che possono a loro volta esporre le organizzazioni a rischi di violazione dei dati e a una non conformità normativa. Questo dato è in linea con il valore di 55% dello scorso anno.

Operation Technology

Negli ultimi anni è stato sempre più evidente come l'Operational Technology (OT) sia essenziale per governi e aziende di tutto il mondo, conseguentemente alla convergenza tra IT e OT. Le minacce volte a compromettere le infrastrutture critiche sono sempre più frequenti. Analizzando i risultati Fortinet riportati nel '**2024 State of Operational Technology and Cybersecurity Report**' che rappresentano lo stato attuale

della sicurezza OT a livello mondiale, condotto su oltre 550 professionisti di diversi settori dell'OT, vengono messe in evidenza le opportunità di miglioramento continue per le organizzazioni per proteggersi in un panorama di minacce IT/OT in continua espansione. Nonostante negli ultimi 12 mesi le organizzazioni abbiano compiuto progressi nell'ottimizzazione della propria strategia di cybersecurity, ci sono ancora aree critiche da migliorare, poiché le infrastrutture IT e OT continuano a convergere in modo esponenziale. **Gli attacchi informatici che compromettono le infrastrutture critiche sono in aumento.** Nel 2024, quasi tre quarti (73%) delle organizzazioni sono state colpite subendo un'intrusione che ha avuto un impatto sui sistemi OT o su entrambi i sistemi IT/OT. I dati del sondaggio mostrano un aumento, anno su anno, delle intrusioni che hanno avuto un impatto solo sui sistemi OT **(dal 17% al 24%).**



Percentuale Globale dei sistemi OT e IT colpiti nel corso del 2023 e 2024

Le intrusioni sono aumentate. Quasi un terzo (**31%**) degli intervistati ha segnalato **più di sei intrusioni**. Tutti i tipi di intrusione sono aumentati rispetto al 2023, a eccezione di un calo dei malware. Le intrusioni tramite tecniche di phishing e tramite compromissione di posta elettronica aziendale sono state le più comuni, tra le tecniche più utilizzate le violazioni della sicurezza su smartphone e la compromissione tramite web. Fortunatamente anche la responsabilità per la cybersecurity nell'OT sta aumentando. La percentuale di organizzazioni che stanno trasferendo la **sicurezza OT nelle responsabilità del CISO** continua a crescere, passando dal **17% nel 2023 al 27% nel 2024**. Allo stesso tempo, si nota un aumento nello spostamento della responsabilità delle infrastrutture OT ad altri ruoli C-level, tra cui CIO, CTO e COO, evidenziando chiaramente una preoccupazione per questo ambito specifico della sicurezza.

Predictions 2025

L'intelligenza artificiale (IA) sta trasformando il mondo della cybersecurity, offrendo sia nuove difese che nuove minacce. Sul piano difensivo, IA può migliorare enormemente le capacità di rilevamento e risposta agli attacchi. Gli algoritmi di machine learning analizzano enormi quantità di dati, identificando schemi anomali e rilevando attacchi informatici in modo più rapido ed efficiente, e possono aiutare i SOC a rispondere in modo più efficace agli incidenti di sicurezza. Tuttavia, l'IA è oramai ampiamente sfruttata dai criminali informatici per attacchi sempre più sofisticati e automatizzati. L'IA può, tra le altre attività criminali, creare deepfake convincenti, generare e-mail di phishing personalizzate, scrivere codice malevolo e automatizzare attacchi di social engineering.

Un'altra area critica è l'uso dell'IA per manipolare le infrastrutture fisiche/OT, considerata la sempre maggiore sovrapposizione degli ambiti OT nel tradizionale perimetro IT. I criminali possono utilizzare modelli linguistici di grandi dimensioni (LLM) per generare script che compromettono le infrastrutture critiche come il governo del traffico terrestre, aereo e marittimo, i veicoli, reti elettriche e impianti industriali. Inoltre, l'IA può essere utilizzata per aggirare i controlli di verifica dell'identità, creare identità sintetiche e manipolare i sistemi finanziari.

È fondamentale quindi adottare un approccio equilibrato allo sviluppo e all'implementazione dell'IA nella cybersecurity, riconoscendone tanto il potenziale positivo, quanto quello negativo.

Un'altra tendenza importante è l'emergere dell'**IA Agentiva (Agentive AI)**, ovvero l'IA in grado di prendere decisioni e agire in modo autonomo perseguendo uno specifico obiettivo. L'IA agentiva offre nuove opportunità, ma presenta anche nuove sfide per la sicurezza. Gli aggressori possono sfruttare l'IA agentiva per automatizzare gli attacchi informatici, il Reconnaissance e lo sfruttamento delle vulnerabilità. La sicurezza dell'IA agentiva sarà quindi un elemento cruciale per la cybersecurity nel 2025.

Inoltre, gli aggressori stanno diventando sempre più sofisticati nello sviluppo di nuove tecniche e strategie per violare i sistemi di sicurezza. Gli attacchi informatici sono sempre più rapidi e silenziosi, sfruttando credenziali valide e strumenti legittimi per eludere i sistemi di rilevamento. Gli attacchi basati sull'identità sono in aumento, con l'IA generativa che aiuta gli aggressori a utilizzare nuove tecniche come il phishing, il social engineering e l'acquisto di credenziali legittime da broker di accesso.

La gestione proattiva dell'esposizione al rischio per ottimizzare la sicurezza aziendale

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

Gestione proattiva dell'esposizione al rischio

Nell'attuale panorama della sicurezza informatica e dal proliferare di minacce in continua evoluzione e superfici d'attacco sempre più ampie, le aziende devono adottare strategie avanzate per ridurre il rischio di subire una compromissione. Una gestione realmente efficace dell'esposizione al rischio consente di identificare, valutare e mitigare in maniera proattiva le vulnerabilità prima che possano essere sfruttate da attori malevoli.

Il concetto di gestione dell'esposizione al rischio

La gestione dell'esposizione alle minacce informatiche è un approccio non si limita alla rilevazione e risposta agli incidenti di sicurezza. Lo scopo principale è infatti prevenire le opportunità di attacco analizzando in maniera continua e costante le superfici d'attacco di una azienda, comprendendo a fondo le tecniche utilizzate dagli attori malevoli e applicando misure di correzione atte alla riduzione del rischio.

Una efficace gestione dell'esposizione al rischio deve garantire una visione completa e aggiornata delle risorse esposte, sia all'interno della rete aziendale tradizionale che su infrastrutture cloud e ambienti esterni. Questa raccolta di informazioni include la valutazione delle vulnerabilità, delle configurazioni errate, delle credenziali compromesse e altre problematiche di sicurezza che potrebbero semplificare il lavoro da parte degli attaccanti.

Limiti delle soluzioni tradizionali

Le strategie tradizionali di gestione delle vulnerabilità si basano spesso su scansioni periodiche e su modelli di prioritizzazione del rischio che non tengono conto del reale contesto delle minacce.

Tra le principali limitazioni si possono evidenziare:

- estensione della superficie di attacco: con l'aumento degli asset, l'infrastruttura IT diventa sempre via via più complessa, rendendo complessa l'identificazione tempestiva delle esposizioni critiche;

- frammentazione e segmentazione delle informazioni: l'uso di soluzioni separate per la gestione delle vulnerabilità, l'analisi delle minacce e la protezione degli endpoint può generare falle di sicurezza e difficoltà nella integrazione dei diversi componenti, estendendo il tempo di esposizione al rischio;
- mancanza di una efficace prioritizzazione: le tradizionali metodologie di valutazione del rischio non sono in grado di riflettere sempre il modo in cui un attore malevolo potrebbe sfruttare una determinata vulnerabilità o problematica di sicurezza in senso lato, fuorviando dall'adozione di strategie di difesa che sarebbero realmente efficaci.

Un approccio moderno alla sicurezza proattiva

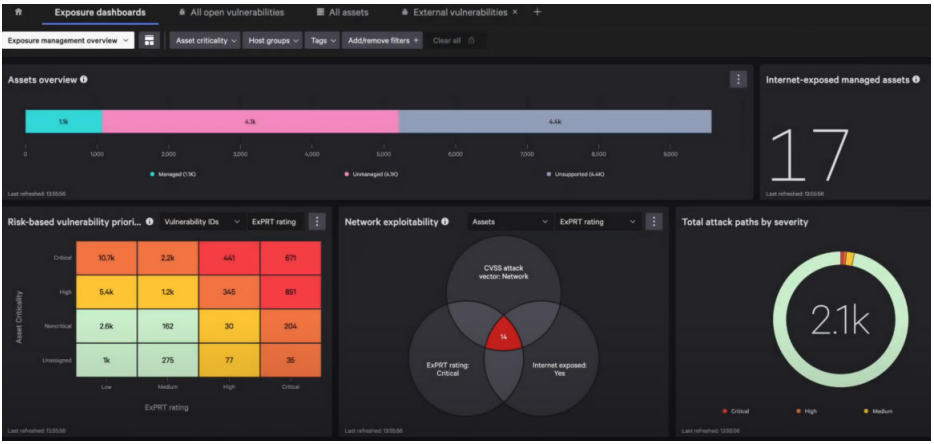
Per contrastare e superare queste limitazioni, è necessario adottare un approccio dinamico e basato sulle informazioni di intelligence relative alle minacce. Una strategia realmente efficace di gestione dell'esposizione al rischio dovrebbe includere:

- monitoraggio continuo: analisi in tempo reale degli asset per rilevare nuove vulnerabilità, esposizioni al rischio e modifiche nell'infrastruttura;
- contestualizzazione del rischio: valutazione delle vulnerabilità non solo in base alla livello di severità dal punto di vista tecnico ma anche in considerazione del loro utilizzo reale e alla probabilità di sfruttamento da parte degli attaccanti;
- automazione e capacità di intervento: utilizzo di strumenti avanzati per automatizzare la prioritizzazione delle minacce e implementare rapidamente efficaci azioni di mitigazione;
- integrazione con soluzioni di sicurezza di terze parti: la sinergia con altre soluzioni di sicurezza è vitale per creare un ecosistema unificato e collaborativo, migliorando la risposta agli incidenti.

Benefici di una gestione proattiva dell'esposizione ai rischi

L'adozione di un modello proattivo di gestione dell'esposizione ai rischi offre numerosi vantaggi. La riduzione del rischio di attacco è possibile grazie a una mitigazione mirata delle vulnerabilità realmente critiche e che richiedono quindi maggiore attenzione. Il miglioramento della visibilità relativa alle superfici d'attacco permette di avere una maggiore consapevolezza delle minacce potenziali e l'ottimizzazione delle risorse di sicurezza consente di concentrare gli sforzi sui rischi con un potenziale maggiore impatto.

Infine, l'aumento della resistenza delle infrastrutture aziendali riduce il tempo di reazione agli eventi critici, migliorando la capacità delle aziende nell'affrontare situazioni di emergenza.



Vista centralizzata delle esposizioni ai differenti rischi con relativa prioritizzazione

Vista unificata degli asset esposti su Internet e relative problematiche di sicurezza

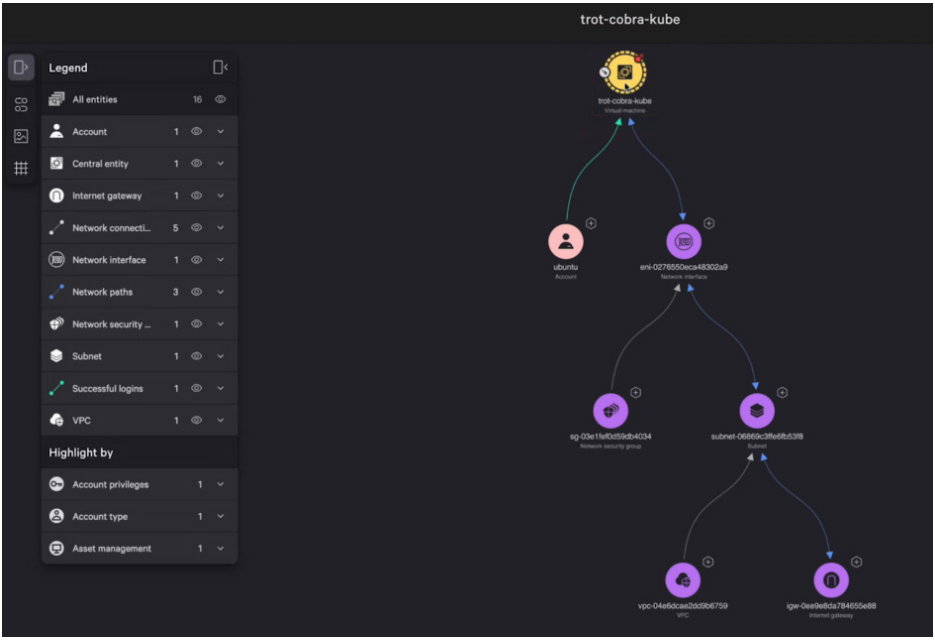
Prioritizzazione delle vulnerabilità

Per rendere ancora più efficace la gestione proattiva dell'esposizione alle minacce informatiche, è fondamentale implementare una prioritizzazione del rischio basata su analisi e dati avanzati. L'adozione di modelli predittivi consente di anticipare quali

vulnerabilità potrebbero essere sfruttate, in che modo e in quali contesti, permettendo ai team di sicurezza di concentrarsi sulle minacce realmente più rilevanti, mitigando i rischi in modo più efficace.
L'integrazione di una telemetria completa e aggiornata, arricchita informazioni specifiche relative alle diverse minacce, offre una visione completa relativa all'ecosistema dei rischi di attacco. Questo approccio fornisce una valutazione puntuale e approfondita di ciascun rischio, facilitando una gestione efficace delle vulnerabilità senza spreco di tempo e risorse per comprendere cosa prioritizzare.

Adottando una gestione proattiva dell'esposizione ai rischi, una gestione in grado di adattarsi in modo dinamico alle informazioni di sfruttamento delle diverse vulnerabilità in tempo reale, le aziende possono prevenire gli attacchi e migliorare la propria postura di sicurezza.

Queste strategie permettono alle aziende di anticipare le mosse degli attori malevoli, di ottimizzare l'adozione e l'utilizzo delle risorse di sicurezza e garantire una protezione più efficace della propria infrastruttura.



Rappresentazione di un asset e dei componenti con cui interagisce

Informazioni di threat intelligence relative alle vulnerabilità

Per migliorare ulteriormente la gestione dell'esposizione ai rischi, le aziende possono integrare informazioni di threat intelligence sulle vulnerabilità in grado di fornire dati aggiornati e in tempo reale relativi alle minacce attuali. Questa metodologia consente di identificare rapidamente le vulnerabilità critiche e di attuare misure di mitigazione efficaci.

Un elemento chiave è la comprensione approfondita degli avversari. Disporre di informazioni dettagliate sui diversi attori malevoli, permette alle aziende di sapere chi si cela dietro agli attacchi, identificare gli attori che prendono di mira specifici settori e comprendere le tecniche adottate. Questa conoscenza approfondita facilita una risposta ancora più precisa e mirata alle diverse minacce.

L'integrazione delle informazioni di threat intelligence sulle vulnerabilità con gli automatismi operativi, arricchiti da dati costantemente aggiornati sugli attaccanti, assicura che le aziende non si limitino alla sola reazione alle minacce ma riescano a trovarsi un passo avanti rispetto agli attaccanti stessi.

Le informazioni disponibili e le modalità di fruizione, devono comprendere tanto aspetti tattici quanto strategici, spaziando dagli indicatori atomici, come gli IOC, corredati da informazioni di contesto estese, fino a report dettagliati sulle tendenze delle minacce e sulla loro evoluzione. Devono inoltre essere disponibili analisi tecniche approfondite inclusive di tutti gli elementi necessari per supportare efficacemente i team responsabili sia delle attività di remediation che di threat hunting.

La sicurezza della Gestione Documentale nei sistemi di acquisizione e stampa

(A cura di Sara Bonini e Stefan Dawid, ASSOIT)

I sistemi di acquisizione e stampa svolgono un ruolo fondamentale nella gestione documentale, offrendo un ponte tra il mondo fisico e quello digitale. Sebbene i documenti cartacei offrano un'accessibilità immediata, i vantaggi della gestione documentale digitale sono innegabili. Quest'ultima consente una ricerca rapida ed efficiente dei documenti, facilita la condivisione e riduce in modo significativo lo spazio fisico necessario per archiviare i documenti. Inoltre, l'integrazione con i sistemi aziendali e le funzionalità di sicurezza e protezione dei documenti rappresentano un ulteriore vantaggio offerto dalla gestione documentale digitale.

La protezione dei dati diventa sempre di più una priorità essenziale per le aziende.

Ogni anello della catena è fondamentale: ogni punto di accesso e ogni connessione; ogni protocollo, impostazione e funzione; ogni stampa, copia e scansione.
Mentre sono i ransomware, gli schemi di phishing, i trojan e altri attacchi malware che attirano la maggior parte dell'attenzione, la sicurezza dei dati nella sua globalità va oltre le violazioni della rete e gli attori esterni malevoli.

Riguarda i documenti stessi, che una volta stampati o scansionati possono finire nelle mani sbagliate, anche accidentalmente. Si tratta in particolare di limitare l'accesso alle funzionalità del dispositivo, per impedire duplicazioni o condivisioni da parte di utenti non autorizzati.

I moderni dispositivi professionali, stampanti, multifunzione e scanner, consentono tipicamente di proteggere opportunamente i 3 ambiti coinvolti: sicurezza della periferica, dei documenti e di rete.

La sicurezza dei dispositivi di acquisizione e stampa

Ogni giorno si producono e si distribuiscono milioni di documenti riservati. I sistemi multifunzione, le stampanti e gli scanner fanno parte integrante delle reti aziendali, proprio per la loro capacità di memorizzare elevate quantità di dati sul loro disco fisso, e rappresentano dunque dei punti critici di vulnerabilità. Inoltre, la maggior parte dei sistemi di stampa è accessibile anche tramite dispositivi mobili e piattaforme cloud, il che li rende ancora più vulnerabili agli attacchi esterni.

Per rendere inattaccabili questi dispositivi chi deve avere accesso per impostare le funzioni di sicurezza? Quali funzioni devono essere disponibili; e quali per lo specifico utente?
Stampanti, multifunzione e scanner possono implementare limitazioni di accesso al dispositivo per gruppi o individui specifici, incluso il limitare particolari funzioni.
Tipicamente queste funzionalità di sicurezza possono essere anche integrate nelle più diffuse soluzioni software di gestione del settore.

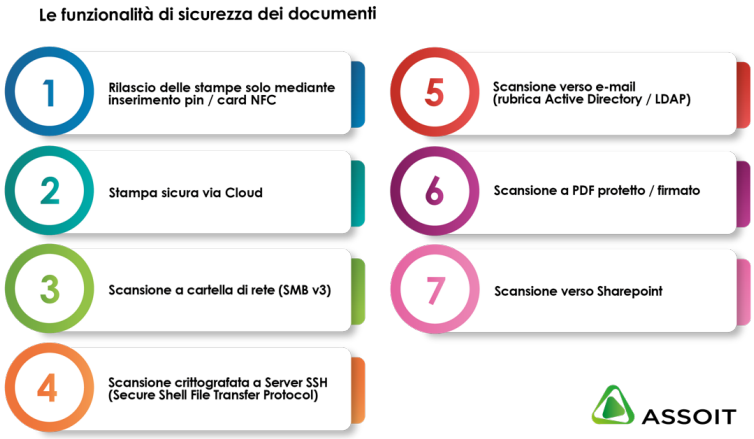
Le principali funzioni di sicurezza sui dispositivi di acquisizione e stampa:

- Firmware firmati digitalmente
- Accesso alla periferica solo mediante password o card NFC
- Autenticazione tramite Active Directory e LDAP
- Interfaccia Pannello utente personalizzabile

Sicurezza dei documenti

Quando un documento viene stampato, chi può recuperarlo?
Quando un documento è scansito, dove può essere inviato?

Anche in questo caso le funzionalità specifiche sono compatibili con molte soluzioni di sicurezza dei documenti sviluppate da terze parti.



Sicurezza di rete

Proteggere la rete aziendale da attori esterni malevoli è fondamentale per il piano sicurezza di ogni organizzazione. I dispositivi di stampa non sicuri possono divenire un punto di accesso per gli hacker.

Le periferiche professionali attuali sono tipicamente dotate di tutti i più recenti protocolli e possono facilmente essere configurate per soddisfare le esigenze e le policy in ambito sicurezza e, in combinazione con gli strumenti software di gestione e monitoraggio forniti dai produttori, consentono di mantenere la sicurezza della rete sempre aggiornata.

Principali protocolli e strumenti in questo ambito sono:

- HTTPS
- IPPS
- SMBv3
- SNMPv3
- Certificati TLS
- Filtro IPv4
- IPv6 Internet Protocol
- IEEE 802.1X
- IPSec (IP Security)
- Software di gestione fornito dal produttore

Sicurezza e fattore umano

Oltre agli ambiti già elencati, così come per il phishing, per la sicurezza dei documenti non vanno dimenticati i fattori comportamentali. Pur implementando tutte le politiche di sicurezza dei dispositivi, permangono infatti vulnerabilità derivanti da errori umani nel loro utilizzo.

Spesso infatti i documenti, anche importanti, vengono stampati senza utilizzare le funzioni che richiedono, ad esempio, PIN per il rilascio. Il risultato è che vengono lasciati abbandonati documenti cartacei sulla periferica di stampa, accessibili a chiunque che possono violare le politiche di privacy e potenzialmente utilizzabili per scopi impropri all'esterno dell'azienda.

Varie indagini effettuate stimano che dal 10 al 30% dei documenti non viene mai prelevato dalla stampante.
Una specifica formazione e regole per gli utenti consentono di evitare la condivisione ed eventuale esfiltrazione di informazioni riservate o confidenziali.

Uno degli incidenti più significativi che ha attirato molta attenzione mediatica riguarda la fuga di informazioni relative ai documenti top-secret del governo statunitense, avvenuta nel 2004. Questo caso ha avuto un forte impatto per il clamore che ha suscitato, anche perché ha coinvolto direttamente documenti estremamente sensibili e la negligenza in un ambiente ad alta sicurezza.

Il caso: Fuga di informazioni dalla stampa governativa negli USA (2004)

Nel 2004, un'inchiesta giornalistica del Washington Post rivelò che alcuni documenti classificati, riguardanti la sicurezza nazionale e operazioni militari, erano stati lasciati su una stampante in un'area pubblica di un ufficio governativo. La stampa non solo non era stata recuperata tempestivamente, ma era stata anche vista da persone non autorizzate che avevano avuto accesso all'area. I documenti riguardavano operazioni sensibili in Medio Oriente, e la loro esposizione a persone esterne avrebbe potuto compromettere operazioni in corso e mettere a rischio la vita di agenti sul campo.

La rivelazione della fuga di informazioni fece scalpore, non solo perché riguardava documenti riservati, ma anche per il modo in cui la negligenza si verificò in un ambiente che teoricamente avrebbe dovuto avere protocolli di sicurezza molto più rigidi.

Il caso portò a un'inchiesta interna da parte delle agenzie governative americane, con discussioni sui protocolli di gestione dei documenti riservati. Si pose anche l'attenzione sulle vulnerabilità nei processi di stampa e distribuzione dei documenti all'interno delle diverse agenzie.
Il caso contribuì a mettere in evidenza la necessità di migliorare la sicurezza dei dispositivi di stampa e a rivedere le politiche di gestione dei documenti all'interno delle agenzie governative e aziendali.

Questo caso è emblematico per il modo in cui un errore relativamente semplice, come dimenticare un documento su una stampante, possa portare a una fuga di informazioni estremamente riservate e potenzialmente dannose. Il clamore derivante da questo incidente ha messo sotto la lente l'inadeguatezza dei protocolli di sicurezza fisica (come la gestione dei documenti stampati) che, seppur molto forti in altri ambiti (come la crittografia dei dati), possono essere facilmente aggirati da negligenze quotidiane.

Questo incidente evidenziò anche quanto fosse facile per qualcuno, senza intenzioni malevole, ottenere accesso a informazioni riservate semplicemente approfittando di un errore umano. La sua rilevanza mediatica fu forte anche perché avvenne in un

periodo di intensa attenzione sulla sicurezza nazionale, dopo gli attentati dell'11 settembre, e la sua diffusione contribuì a sollevare il tema della sicurezza fisica nell'ambito della gestione delle informazioni sensibili.

Non trascurabile, per la piccola come per la grande impresa, financo per i cittadini, il ricorso a soluzioni che si avvalgono di una comunità solida e di prossimità di partner, rivenditori, system integrator e consulenti per implementare procedure, assicurare formazione e consulenza per la protezione e la sicurezza dei sistemi di stampa, digitalizzazione e gestione documentale presenti nelle aziende, nelle istituzioni e nelle case dei privati cittadini.

Per aiutare le aziende a creare strategie a lungo termine che includano l'utilizzo di tecnologia finalizzata ad alimentare la produttività e ridurre i costi, ASSOIT ha realizzato diverse ricerche, una delle quali è dedicata alla sicurezza delle informazioni che può essere scaricata dal sito dell'associazione.

ASSOIT è l'Associazione Produttori Soluzioni di Stampa, Digitalizzazione e Gestione Documentale, cui sono associate tutte le principali aziende presenti in Italia che producono
sistemi di acquisizione e stampa. I suoi associati rappresentano un mercato
di 70.000 addetti, 11 milioni di dispositivi e 3 miliardi di euro di fatturato.

https://www.assoit.it/

Autismo e Cyber Security

(A cura di Lorenzo J.S e Andrea Mazzola)

Negli ultimi anni sono apparsi diversi articoli[1] e studi in merito alla possibilità di utilizzare nell'ambito della cybersecurity persone autistiche (o più in generale appartenenti all'area della neuro diversità), un insieme molto ampio di individui, con caratteristiche molto diverse fra loro e soprattutto con livelli e capacità intellettive alquanto differenziati[2].

Più recentemente sono state presentate diverse iniziative in questo senso, come una semplice ricerca con i termini "autismo and cybesecurity" ben evidenzia.

Lo stesso CLUSIT, nell'ambito di un paio di edizioni del Security Summit, ha affiancato alla tradizionale attività istituzionale, eventi legati al mondo dell'autismo presidiati dalla Dott.ssa Raffaella Faggioli (con la quale ho pubblicato il mio primo libro su questo tema: ***Dentro l'autismo. L'esperienza di un clinico, la testimonianza di un Asperger***, FrancoAngeli 2014).

Considerando che la mia attività professionale mi porta a incrociare spesso persone che si occupano di informatica, sicurezza e cybersecurity, ho ritenuto opportuno esprimere il punto di vista di una persona autistica (il mio) su questo argomento.

Per farlo utilizzerò in parte anche alcuni stralci del libro sopra citato (riportati in corsivo nel testo).

---

[1] **Autistic People Can Solve Our Cybersecurity Crisis** - Kevin Pelphrey is (Carbonell Family Professor and director of the Autism and Neuro developmental Disorders Institute at George Washington University in Washington, DC.),
An Alan Turing-Inspired Solution to the Cybersecurity Labor Shortage - Xuyen Bowles - Sentek Global
Neurodiversity & Cybersecurity Careers: Recruiting & Retaining Autistic Cybersecurity Professionals - Eleanor Dallaway Editor & Publisher, Infosecurity Magazine.
https://www.redhotcyber.com/post/la-neuro-diversita-allinterno-dei-team-di-cybersecurity-e-un-bene-prezioso/
https://www.economymagazine.it/la-neurodiversita-e-unarma-in-piu-per-contrastare-i-reati-informatici/

[2] Come il resto della popolazione anche le persone autistiche possono avere un livello di QI molto diverso gli uni dagli altri. Un altro elemento che distingue fra loro i soggetti autistici è la severità dei sintomi, che viene misurata con una scala di 3 valori che indica quanto significativo debba essere l'attività a loro supporto. Ad esempio un livello di severità 2 indica la necessità di supporto sostanziale.

Lo spettro autistico

il termine autismo è ancora sempre legato all'immagine di un bambino solitario o al personaggio di Rain Man (il celebre film con protagonista l'attore Dustin Hoffman) e non si concepisce l'idea che anche un affermato professionista, un dirigente d'azienda, un dipendente statale, un impiegato, un docente universitario, uno scienziato, possano rientrare fra quanti abbiamo una diagnosi di ASD.

In realtà il numero delle persone è molto più alto di quanto ci si potrebbe aspettare e le stime variano dall'1% al 4% della popolazione mondiale (l'affinamento degli strumenti di diagnosi e l'ampliamento dei criteri diagnostici ha portato a un radicale aumento dei casi diagnosticati negli ultimi anni)[3].

Settori particolari, come quello dell'IT, presentano un elevato numero di persone autistiche, anche se in molti casi queste non hanno mai ricevuto una diagnosi.

Molto interessante era al riguardo l'approccio della pubblicazione **Autism and careers in cyber security: A short guide for employers4**, redatta congiuntamente dall' **Information Assurance Advisory Council** (IAAC) e dal **Cyber Security Challenge UK** (https://cybersecuritychallenge.org.uk/about).

Questa era a tutti gli effetti una guida per quanti desiderassero impiegare persone autistiche e cita nella sua introduzione:

The inspiration for this guide comes from two commonly expressed views in the cyber security community.

- *Firstly, there is the idea that autistic people often have skills that are particularly suited to working in cyber security and IT more generally.*
- *Secondly, that the IT sector already has a large number of autistic people working in it, many of whom have gone undiagnosed or not disclosed their condition.*

Il perché le persone autistiche siano considerate particolarmente adatte a svolgere attività legate agli ambiti della sicurezza verrà chiarito nei prossimi paragrafi.

Le caratteristiche delle persone a funzionamento autistico

le ricerche prima citate, riportano alcune delle particolarità delle persone autistiche. Fra queste in ambito tecnico evidenziano:

- l'essere molto analitici

[3] Secondo l'ISS, in Italia tra 1 e il 2 %.

[4] Attualmente non più disponibile.

- avere un approccio metodologico
- avere una buona memoria per i fatti concreti
- avere elevate capacità di *problem solving*
- avere elevate abilità numeriche
- acquisire con facilità conoscenze e competenze specialistiche
- essere abili nel riconoscimento di modelli e di pattern
- avere una attenzione minuziosa ai dettagli
- avere una elevata capacità di attenzione su un problema specifico.

In effetti tutte queste caratteristiche ben si sposano con quanto è richiesto in ambito informatico ad esempio nel controllo della qualità del software[5], nell'analisi del codice sorgente di un'applicazione e, nell'ambito della sicurezza, nell'analisi e predisposizione della configurazione di apparati di sicurezza, nell'individuare vulnerabilità, nell'identificare schemi di attacco...

Le persone autistiche hanno inoltre una ulteriore caratteristica molto importante: un modo diverso di pensare.

Le persone autistiche per nascita "vedono le cose in maniera differente" e per tale motivo sono spesso incomprese; tuttavia, se adeguatamente indirizzate, supportate e motivate, possono sfruttare adeguatamente le loro peculiari caratteristiche. Io ne ho fatto dei plus delle mie numerose attività professionali.

Lo stesso Hans Asperger, come riporta Tony Attwood nel suo libro Guida alla sindrome di Asperger aveva ipotizzato: "Sembra che per avere successo nelle scienze e nell'arte, un pizzico di autismo sia essenziale. Per il successo, l'ingrediente necessario potrebbe essere la capacità di allontanarsi dal mondo di ogni giorno, dal semplicemente pratico, una capacità di pensare di nuovo a qualcosa in modo originale, per creare strade non ancora percorse, con tutte le abilità canalizzate nell'unica specialità".

Questo consente loro, ad esempio, di analizzare e anche ipotizzare nuovi schemi di attacco e predisporre anticipatamente nuove modalità di difesa.

Le caratteristiche sopra menzionate non devono tuttavia considerarsi limitate agli ambiti di sicurezza puramente IT. Le capacità di analisi e correlazione hanno importanti risvolti anche nella redazione di procedure e policy di sicurezza, nella esecuzione di verifiche ispettive in ambito sicurezza e qualità, nell'analisi delle normative che abbiano impatti sulla sicurezza, nell'analisi e formulazione di accordi contrattuali e

[5] Una grande azienda di software gestionale ha dichiarato di arrivare di voler includere persone autistiche in numero pari all'1% dei propri addetti.

SLA; in sintesi riguarda tutti gli aspetti tecnici, organizzativi e legali legati al mondo della sicurezza.

Inoltre la capacità di cogliere, analizzare e correlare particolari che ai più possono sfuggire, rende particolarmente utile l'impiego di persone autistiche anche in attività di intelligence estese all'ambito economico, politico o energetico.

Al riguardo l'uso delle peculiarità delle persone neurodiverse[6] sono state già oggetto di attenzione ad esempio dei servizi segreti britannici[7] o di altri Stati[8].

Alle caratteristiche "tecniche" si aggiungono quelle che personalmente ritengo essere le doti morali di cui le persone autistiche sono dotate:

- un forte senso etico
- onestà
- affidabilità
- rispetto delle regole.

Personalmente do molto peso a queste caratteristiche e proprio per questo considero che questo *modo di essere, considerato da molti semplicemente una disabilità9* sia un privilegio.

Io do una mia particolare interpretazione alla presenza di queste caratteristiche:

È inoltre a mio avviso strettamente connessa all'interpretazione letterale (nel senso più esteso del termine, quali il rispetto delle regole) l'elevato senso etico e morale che contraddistingue solitamente le persone autistiche.

Difficilmente inoltre una persona autistica è in grado di mentire (ma questo in molte situazioni non è affatto positivo) o di smussare la propria posizione (rigidità).
Sono troppe le caratteristiche dei così detti neuro tipici che mi lasciano perplesso, smarrito. Prima di tutte la facilità con cui mentono, spesso a fin di bene, dicono, per non ferire, per mediare...

---

6 Le persone autistiche definiscono con il termine neurotipiche le persone non autistiche.

7 Spooky London: how Britain's spy agencies are using new and unexpected methods to recruit the next generation https://www.standard.co.uk/lifestyle/esmagazine/spooky-london-the-new-methods-of-britains-spies-a3189396.html
I spy with my little eye … someone on the spectrum
http://www.telegraph.co.uk/education/educationnews/11113540/I-spy-with-my-little-eye...-someone-on-the-spectrum.html

8 The Israeli Army Unit That Recruits Teens With Autism
https://www.theatlantic.com/health/archive/2016/01/israeli-army-autism/422850/

9 https://iterdigital.it/autismo-studiare-lavorare-socializzare/#1724944901665-b44cfc1f-4d40
https://static.francoangeli.it/fa-contenuti/area_pdfdemo/1305.205_demo.pdf

Una cosa che reputo eticamente e moralmente inaccettabile.

Sono state realizzate anche alcune serie televisive che hanno come protagoniste persone dichiaratamente autistiche e, personalmente, trovo molto realistica e ben fatta la serie poliziesca "Astrid e Raphaëlle", nella quale la protagonista, utilizza le sue capacità, in quanto autistica, nello svolgimento di indagini.

La serie mi piace in quanto ho molte analogie con le caratteristiche che ha il personaggio di Astrid.

Fra gli altri svolgiamo un lavoro per certi versi molto simile e quindi questo accentua le analogie.
Debbo dire che in realtà questa è anche l'unica serie che ho seguito e quindi non sono in grado di dare un giudizio sulla veridicità di altri personaggi.

Sheldon Cooper nella serie Big Bang Theory[10] rappresenta molte caratteristiche di una persona autistica e molte delle mie caratteristiche, ma in nessuna delle quasi 300 puntate della serie (delle quali ho la raccolta completa) si fa esplicita menzione di una sua specifica neuro diversità.

Essere preparati

È evidente che pur con tutte le qualità che la rendono un candidato ideale per svolgere un lavoro nell'ambito della sicurezza, una persona autistica è tale perché presenta delle caratteristiche che vengono facilmente viste come negative o spesso fraintese. Se così non fosse l'autismo non sarebbe considerata una disabilità. Non è quindi possibile limitarsi a considerare i benefici derivanti dall'impiego di una persona autistica senza valutare anche l'impegno che ciò può comportare.

Si deve infatti avere l'accortezza da un lato, di predisporre un ambiente idoneo dove la persona possa lavorare, anche se relativamente a questo aspetto l'uso dello smart working può fortunatamente risolvere alla radice il problema e dall'altro, di essere consapevoli delle particolari modalità di essere, di comunicare e di interagire che tali persone hanno.

Le persone neuro tipiche devono prendere coscienza che non esistono solo persone di razze diverse, ma anche persone con un funzionamento diverso nel modo di pensare e di relazionarsi con gli altri. Persone per le quali la comunicazione (di per sé scarsa) è basata più sul contenuto del messaggio che sulla forma o sul modo (inconsapevole) di atteggiarsi. Persone per cui gli occhi non sono lo specchio dell'anima,

[10] Probabilmente la serie televisiva più premiata di sempre.

perché il loro sguardo può non essere in linea con le loro parole. Persone che non ti stanno giudicando o rifiutando semplicemente perché ti osservano tenendo incrociate le braccia (tutti elementi questi che portano spesso a pesanti fraintendimenti).

Le persone autistiche sono solitamente molto rigide, hanno interessi ristretti, danno una interpretazione letterale a quanto si dice (o si scrive) e hanno spesso un linguaggio monotonico che può apparire (involontariamente) assertivo…

L'uso del linguaggio monotonico è assolutamente naturale e spontaneo e pertanto è quello che richiede il minor impegno.

Può apparire eccessivamente assertivo e imperativo e in parte questo è legato al fatto che ritengo vero ciò che affermo, nel senso che non ne dubito11.

Per questi motivi il modo di essere e comportarsi di una persona autistica può essere (è il mio caso) anche particolarmente irritante. Io ne sono consapevole e spesso istruisco al riguardo un nuovo collega con il quale devo lavorare. A volte però mi dimentico o non ho voglia di farlo e quindi si creano anche pesanti fraintendimenti.
Non va inoltre mai dimenticato che quotidianamente le persone autistiche devono affrontare una serie di sfide e problemi, che si assommano a quelli tipici dell'attività lavorativa.

…le difficoltà non mancano12. In particolare la incapacità di interazione e di relazione con gli altri, i fraintendimenti, l'essere esclusi, il sentirsi catapultati in un mondo che non ci appartiene, il non sapere cosa è giusto fare (e quindi non fare nulla)... Sarebbe utile riuscire a valorizzare le caratteristiche che possono avere risvolti positivi e temperare quelle che hanno dei possibili risvolti negativi, ma questo discorso vale per tutti gli esseri umani. La differenza probabilmente sta nel fatto che di queste ultime e delle loro conseguenze non ci rendiamo conto, se non ci vengono esplicitamente (e verbalmente) evidenziate.

È importante essere consapevoli del diverso modo di reagire di una persona autistica che può, ad esempio, non capire di avere offeso o irritato qualcuno.

Fortunatamente la natura ci ha dato delle potenti difese, non permettendoci di cogliere gli aspetti negativi delle reazioni degli altri, salvo che la reiterazione dei loro modi di fare non porti a capire (per deduzione logica, quindi razionalmente e non

---

[11] La mimica facciale, spesso poco espressiva, rafforza questo stile comunicativo

[12] Molte persone autistiche risentono pesantemente di alcuni fattori ambientali, quali luci al neon, rumori… Io ad esempio sono molto condizionato dal posizionamento della mia postazione nel locale in cui lavoro, da quanto mi circonda, dalle dimensioni dei locali, da rumori e voci…

emotivamente) che qualcosa non va: comportamenti inaspettati, reazioni inattese e inspiegabili, fino al risentimento e al disprezzo nei miei confronti.

Non va inoltre confusa la capacità di risolvere brillantemente un problema tecnico con la capacità assoluta di comprendere rapidamente qualunque cosa o qualunque situazione.

Le persone autistiche sono spesso molte lente nel capire e nel rispondere, sommerse come sono dall'eccesso di informazioni dell'ambiente che le circonda (a differenza dei neuro tipici queste informazioni sono elaborate scientemente). Le particolari capacità intellettive delle quali sono dotate emergono infatti solitamente quando, pur in mezzo agli altri, riescono a rifugiarsi nel loro mondo.

Mi viene spontaneo paragonarci a delle lumache o a delle tartarughe; è curioso il fatto che entrambi questi animali "lenti" abbiano anche un'altra caratteristica molto autistica: un guscio nel quale rifugiarsi.

È quindi importante comunicare correttamente, ma considerando che la comunicazione è uno degli aspetti più carenti delle persone autistiche è importante dare il giusto peso a questo tipo di attività.

Comunicare non è facile, non è indolore. Decidere di comunicare comporta l'attivazione di un processo complesso, comporta l'abbassare le proprie difese, spesso uscire dal proprio mondo, dalla propria sicurezza. Comunicare è una scelta che costa e quindi quando si decide di farlo non è per una banalità. Ci si aspetta però che sia così anche per la controparte e si rimane frustrati quando ci si accorge che molto spesso non è così, che per gli altri comunicare è una convenzione, un gesto di "educazione", è fatto per abitudine.

Me ne accorgo in particolare quando ad esempio un terzo si introduce in un colloquio che sto avendo con qualcuno. Quando riprendiamo a parlare a volte provo volutamente a non proseguire il discorso che è stato interrotto e molto spesso il mio interlocutore non si ricorda nemmeno di cosa stavamo parlando.

Mi permetto di aggiungere di non limitarsi a chiedere, ma anche di verbalizzare ciò che si prova, fosse anche un profondo disagio che la persona che ci sta di fronte ci provoca. La mancanza di comunicazione, il dare per scontato che l'altro capisca, sta alla base di fraintendimenti che, reiterati nel tempo, possono avere conseguenze anche gravi.

Singoli gesti, che per una persona neuro tipica sono insignificanti, in quanto inseriti in un contesto comunicativo più ampio, possono essere vissuti e interpretati in modo

totalmente diverso da una persona a funzionamento autistico, che probabilmente in futuro ben difficilmente riuscirà a chiarire e capire le reciproche posizioni. È quindi indispensabile parlare, chiedere e non dare nulla per scontato, non fermarsi all'apparenza.

Non offendetevi o stupitevi se una persona autistica non verrà a prendere il caffè con voi o non verrà a pranzo con il gruppo di colleghi (o nel caso in cui venga a pranzo se ne stia zitta). Né stupitevi se invece si relaziona solo con una persona in particolare. È probabile che quella persona sia la sola ad avere il giusto livello di interazione. Nel mio caso interagisco solo con un paio di colleghi che mi tollerano, anche se io me ne sto quasi sempre zitto e in ascolto. Del resto io al parlato privilegio la scrittura.

La comunicazione scritta presenta una serie di vantaggi considerevoli rispetto a quella orale:

- *può essere asincrona (non è necessaria la contemporanea presenza di altri interlocutori);*
- *può essere indirizzata a più interlocutori;*
- *può essere facilmente integrata;*
- *il messaggio può essere rivisto anche da terze parti prima di essere inoltrato;*
- *può contenere domande, risposte, testi, immagini;*
- *non costringe l'interlocutore a una risposta immediata.*

Inoltre la forma scritta costituisce anche una forma di tutela o viceversa una prova a proprio sfavore.

Questo secondo aspetto fa sì che molte persone sono restie a lasciare traccia scritta delle proprie affermazioni; di norma si tratta di chi desidera riservarsi la facoltà di negare quanto ha in precedenza affermato. È per questo motivo che con il tempo ho imparato a diffidare di chi ha difficoltà a comunicare per iscritto (di norma trincerandosi dietro la scusa di non voler essere formali)...

Il tema delle problematiche legate al mondo del lavoro e di quali difficoltà o strategie una persona autistica possa adottare per far fronte alle difficoltà che incontra è molto ampio e ho descritto le strategie che ho adottato nel corso della mia vita nel mio libro: ***"Autismo: studiare, lavorare, socializzare"***, ITER 2024 realizzato con il Dott. Andrea Mazzola.

Personalmente ho la necessità di avere una postazione in un luogo il più possibile protetto (un angolo ad esempio, possibilmente vicino a una finestra), ma in un locale molto ampio, posto al piano terra o comunque di un grande edificio.

Non posso stare in ogni caso in un ambiente che percepisco come circoscritto e quindi claustrofobico.

Accanto all'impossibilità di accettare un contenimento fisico si affianca il contenimento temporale e quindi, durante la mia vita lavorativa ho dovuto ideare soluzioni basate su part time o più recentemente, smartworking o comunque soluzioni che consentissero di stare chiuso in ufficio per il minor tempo possibile.

La mia vita lavorativa è stata un continuo compromesso fra necessità del non sentirmi "ingabbiato" e la garanzia e continuità di un lavoro stabile, realizzata portando avanti contemporaneamente più attività sia come dipendente, sia come professionista, part time e smart working, affrontando situazioni e ambienti molto diversi fra loro in quanto a comprensione delle esigenze e disponibilità.

Conclusioni

Personalmente condivido completamente la tesi secondo la quale molte persone autistiche hanno caratteristiche che le rendono risorse preziose nell'ambito della sicurezza e delle attività di analisi legate alle attività di intelligence. Tuttavia mi chiedo quanto siano preparate le aziende o gli enti pubblici nel gestire adeguatamente queste risorse senza penalizzarle per il loro particolare modo di essere.

Sicuramente io ho subito discriminazioni per il mio essere autistico, in particolare quando mi sono trovato, mio malgrado, in ambienti particolarmente competitivi, dove non sono assolutamente in grado di muovermi, non capendo le logiche relazionali in essere fra gli individui.
Il fraintendimento circa il mio modo di essere è una costante; solo in rare occasioni ho trovato chi ha saputo valorizzare le mie peculiarità.

È quindi assolutamente fondamentale che le aziende che desiderino avvalersi di persone autistiche, per avvantaggiarsi delle loro caratteristiche uniche, siano realmente preparate per farlo e questo implica diversi aspetti, fra i quali:

- un ambiente spazio/temporale idoneo
- la formazione di tutto il personale in merito a cosa significhi lavorare con una persona autistica
- un progetto ben definito su quali siano le aspettative e le modalità per perseguirle
- una costante analisi di quali siano le caratteristiche specifiche dei soggetti interessati, al fine di poterle indirizzare al meglio
- il ricorso a specialisti che possano mediare la relazione e indirizzare le scelte reciproche.

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 per 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.
Agentive AI	AI in grado di prendere decisioni e agire in modo autonomo perseguendo uno specifico obiettivo.
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.
APA (Attack Path Analysis)	Tecnica utilizzata nel campo della sicurezza informatica per identificare e valutare i percorsi potenziali attraverso i quali un attaccante potrebbe violare un sistema o una rete.
Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	Vulnerabilità che consente a un attaccante di accedere a file tramite richieste Web remote.

Assume breach	Approccio secondo cui gli operatori di sicurezza partono dal presupposto che, prima o poi, un attacco andrà a buon fine, e dunque strutturano processi, strumenti e competenze per rilevare, investigare e contenere rapidamente qualsiasi compromissione.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
Backdoor	Soluzione tecnica che consente l'accesso a un sistema superando i normali meccanismi di protezione.
BEC fraud (Business e-mail compromise)	Tipi di attacco phishing mirati verso figure aziendali al fine di convincere le vittime a trasferire somme di denaro o rilevare dati personali. (Vedi anche ***CEO fraud***)
BITS Jobs (Background Intelligent Transfer Service)	Tecnica che consente ai cybercriminali di programmare ed eseguire download malevoli in background senza destare sospetti.
Blocj	Tecnica utilizzata nell'ambito dell'***e-voting***. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.
Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi ***DDOS.***
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo ***DDOS***.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.

CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CDR (Cloud Detection and Response)	Approccio alla sicurezza che nasce per fornire ai team di SecOps, in particolare SOC (Security Operations Center) e IR (Incident Response), le capacità di cui hanno bisogno per monitorare, individuare e bloccare attacchi specifici per il Cloud.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.
CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): • fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; • incrementare la consapevolezza e la cultura della sicurezza; • cooperare con istituzioni analoghe, nazionali 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.
CNAPP (Cloud-Native Application Protection Platform)	Categoria di soluzioni che riunisce diverse funzionalità di sicurezza in un'unica piattaforma, per proteggere le applicazioni in cloud.
CNOs (Computer Network Operations)	Tipologia di ***Information warfare*** finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.
CoA (Courses of Action)	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della ***Cyber Intelligence*** rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali a un attacco cyber.
Constituency	Nell'ambito di un ***CERT*** indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).
Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.

C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: • due azioni passive: *Discover* e *Detect* • cinque attive - *Deny*, *Disrupt*, *Degrade*, *Deceive*, *Destroy*).
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito ***IRU*** a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.

CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. *(*https://www.first.org/cvss/specification-document*)*
CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o a 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…).
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 a 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 a un host vulnerabile inducendolo a indirizzare le risposte alla vittima dell'attacco. Questa tipologia di ***DDOS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.
Dropper	Codice che installa il ***malware*** sul computer della vittima.
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni
eBPF (Extended Berkeley Packet Filter)	Tecnologia integrata nel kernel di Linux, che consente di monitorare e filtrare il traffico di rete in tempo reale senza impattare negativamente sulle prestazioni, offrendo un livello di protezione granulare e adattivo, capace di rispondere automaticamente ai cambiamenti dell'infrastruttura.
EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.
Enterprise Architecture	Sistema informativo che, raccogliendo dati da tutte le funzioni dell'organizzazione, li collega in un unico modello informativo consentendo di visualizzare complessivamente lo stato dell'organizzazione e contemporaneamente di immaginarne la possibile evoluzione futura, rinforzandone la capacità di reagire a eventi esterni.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.

Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Facing applications	Applicazioni rivolte al pubblico, quali ad esempio siti web.
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro a una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997

Harvest now, decrypt later	Tecnica che consiste nel raccogliere i dati crittografati per una successiva decrittazione, quando la potenza di calcolo quantistico diventerà più accessibile.
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia a inviare il corpo del messaggio a 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 e 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.
IoB (Internet of Bodies)	IoT applicato ai sistemi biologici. Dispositivi che raccolgono dati biometrici, fisiologici e comportamentali.
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	***Malware*** finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.

Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti e 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 a 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 e ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
ITDR (Identity Threat Detection and Response)	Insieme di strategie, processi, tecnologie utilizzati per rilevare, analizzare e rispondere alle minacce che prendono di mira le identità digitali.

Jamming	Interferenza intenzionale o volontaria di un segnale elettromagnetico al fine di disturbare, bloccare o impedire la ricezione corretta del segnale da parte dei dispositivi destinatari.
LOTL (Living Off The Land)	Tipo di attacco basato su strumenti nativi preinstallati nel sistema operativo.
LOTS (Living Off Trusted Sites)	Tecnica di attacco che permette agli attori di sfruttare strumenti presenti nei sistemi attaccati per eseguire attività malevole senza essere scoperti.
MAAS (Malware as a Service)	Modello di erogazione del codice malevole dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Meaconing	Interferenza con i segnali di navigazione, come quelli provenienti dai sistemi GPS, al fine di alterare le informazioni di posizione e indirizzare in modo errato i dispositivi di navigazione o di localizzazione.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.
MFA (Multi-Factor Authentication)	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
MFU (Malicious File Upload)	Attacco a 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 a una rete.
OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. *(https://www.poliziadistato.it)*
OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla ***blockchain*** per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio e alla gestione di asset fisici in ambito industriale, trasporti…

Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… e i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una ***botnet***, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.
Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.

Pretexting	Tecnica di ingegneria sociale nella quale l'attaccante usa una storia inventata, ad esempio una carta di credito bloccata, per carpire la fiducia della vittima e manipolarla fino a farle condividere informazioni sensibili, scaricare malware, inviare denaro a criminali o arrecare danni alla propria organizzazione.
PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*
Pulse Wave (o Hit & Run)	Hit & Run (o Pulse wave)
QKD (Quatum Key Distribution)	Tecnologia che utilizza i principi della meccanica quantistica per creare canali di comunicazione sicuri; permettendo di condividere chiavi crittografiche con totale sicurezza, poiché qualsiasi tentativo di intercettazione verrebbe immediatamente rilevato.
QTSP (Qualified Trust Service Provider)	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
Quishing/QRishing	Tecnica di attacco che utilizza QR code malevoli per indurre le vittime a visitare siti web fraudolenti o scaricare malware.
Ransomware	***Malware*** che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware).
RDP (Remote Desktop Protocol)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi a un contesto in continua evoluzione". *Definizione da* ISO 22316:2017
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.

Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività ***OSINT***. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
SASE (Secure Access Service Edge)	Approccio alla sicurezza attraverso il modello Zero-Trust, dove ogni accesso è rigorosamente controllato per garantire che solo utenti e dispositivi autorizzati possano accedere alle risorse aziendali.
SAST (Static Application Security Testing)	Analisi statica del codice finalizzata alla individuazione di vulnerabilità.
SBOM (Software Bill of Materials)	Inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.
Security Architecture (NIST)	Insieme di rappresentazioni logiche e fisiche di un'architettura di sistema rilevanti dal punto di vista della sicurezza, che raccoglie le informazioni su come il complessivo sistema sia organizzato in domini di sicurezza, e ne fa uso per rinforzare le policy che prescrivono come dati e informazioni debbano essere protetti all'interno di un dominio di sicurezza e nelle relazioni tra i domini.
Self-sovereign Identity	Modello di identità digitale dove la gestione dei dati non è affidata a provider esterni o Identity Provider, ma lascia agli utenti il pieno controllo sui propri dati.
Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.

SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. *(*Tratto da: *Glossario intelligence – Il linguaggio degli Organismi informativi* - www.sicurezzanazionale.gov.it*)*
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
SMB (Server Message Block)	Protocollo per la condivisione di file e stampanti nelle reti locali. Se esposto su internet può essere utilizzato per accedere a documenti e file condivisi.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.
SOAR (Security Orchestration Automation and Response)	Approccio che consente di orchestrare le tecnologie di sicurezza al fine di avere una gestione il più possibile automatizzata della raccolta, analisi e risposta agli eventi di sicurezza.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.

SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini ***OSINT***, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
Spear phishing	***Phishing*** mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SL-A (Security Level - Achieved)	Livello di sicurezza effettivamente raggiunto.
SL-T (Security Level-Target)	Livello di sicurezza richiesto.
SSDLC (Secure Software Development Life Cycle)	Programma che indirizza la sicurezza sin dalle prime fasi di progettazione di un'applicazione software e non si conclude con la fase di delivery, ma segue tutto il ciclo di vita dell'applicazione.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	***Protocollo*** cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
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 a 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 a un host vulnerabile inducendolo a 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 a una rete.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti a una ***blockchain***.
VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del ***phishing***.

Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
WEF Quantum Readiness Toolkit	Kit che fornisce cinque principi per aiutare le organizzazioni a prepararsi per l'economia quantistica sicura, valutando la loro prontezza quantistica e identificando le azioni prioritarie.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello ***spearphishing*** che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
Wiper	Tipologia di virus che hanno come unico scopo quello di distruggere il sistema target (IT e OT).
XDR (Extended Detection and Response)	Dispositivi che integrano tutte le componenti della soluzione di sicurezza in un'unica piattaforma di individuazione (detection) e risposta agli incidenti (Incident Response) portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone.
XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.

Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.
Zoom bombing	Irruzione virtuale in una videoconferenza finalizzata a creare disturbo.

Gli autori del Rapporto Clusit 2025

Alessio Aceti, vanta oltre 20 anni di esperienza internazionale in cybersecurity e digital transformation, con un focus su innovazione e sicurezza OT. Come CEO di HWG Sababa, guida lo sviluppo del Security Operations Center (SOC), promuovendo strategie avanzate per la protezione delle infrastrutture critiche. Il suo impegno ha contribuito a rafforzare la sicurezza di settori strategici come manifatturiero, trasporti, energia e utilities. Con uno sguardo sempre rivolto al futuro, Alessio continua a innovare nella protezione degli ambienti industriali, affrontando le minacce emergenti con soluzioni all'avanguardia.

Irina Artioli, lavora in Acronis dal 2017, dove oggi ricopre il ruolo di Cyber Protection Evangelist. La sua missione è analizzare le ultime minacce informatiche, gli attacchi emergenti e l'evoluzione del malware, contribuendo alle ricerche della Threat Research Unit (TRU). Grazie a un background consolidato nello sviluppo del Canale e delle Vendite IT, ha portato la sua esperienza all'interno del TRU, collaborando con partner e clienti in tutto il mondo per rafforzare la consapevolezza sulla cyber protection. Con una laurea magistrale in Economia e Commercio Internazionale e certificazioni Security+, e IT Management presso SDA Bocconi, ha trasformato la sua passione in una carriera, credendo che la vera fortuna sia poter coniugare Cybersecurity e Vendite per offrire soluzioni innovative e strategiche.

Domenico Barresi, la sua passione per l'informatica nasce fin dall'infanzia, quando rimase affascinato dal potenziale dei primi PC. Da quel momento ha coltivato un interesse instancabile per la tecnologia, attraversando ogni fase evolutiva del settore informatico. Con oltre 20 anni di esperienza professionale nel campo dell'ICT, ha maturato esperienze come System Administrator, ICT Consultant e Cyber Security Consultant, sviluppando competenze trasversali che spaziano dalla

gestione infrastrutturale alla sicurezza dei sistemi. Da più di 10 anni lavora nel campo della Cyber Security, ricoprendo diversi ruoli. Ha iniziato lavorando nel SOC Corporate di Fastweb, dove ha affinato le sue competenze nella gestione degli incidenti e nella protezione delle infrastrutture aziendali, per poi passare al gruppo Security Eng & Ops, dove ha contribuito all'ottimizzazione dei sistemi di sicurezza. La sua evoluzione professionale lo ha condotto al SOC Enterprise, dove, come Enterprise Security Engineer per i servizi di Cyber Security e Architetture di sicurezza, si occupa principalmente di progettazione, delivery e manutenzione di soluzioni SIEM e SOAR per i clienti Enterprise e Pubbliche Amministrazioni di Fastweb. Il suo lavoro include anche un contributo come L3 Security Analyst.

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, 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.

Mario Boemi, ha conseguito la Laurea Magistrale in Informatica presso l'Università degli Studi di Messina nel 2012. Vanta un'esperienza di oltre 10 anni nel settore della Sicurezza Informatica, durante i quali si è specializzato in tematiche di Cyber Security in contesti CERT e SOC e acquisito certificazioni in ambito di gestione e risposta agli incidenti di sicurezza e Threat Intelligence. Dal 2023 svolge il ruolo di Cyber Security Coordinator del CSIRT&SOC di Fastweb, gruppo responsabile delle attività di monitoraggio e risposta agli incidenti di sicurezza dell'infrastruttura Corporate dell'azienda.

Laura Bongiorno, Laureata in Fisica, è entrata in Fastweb nel 2000. Lavora nella funzione Security & Real Estate dal 2018, dove ha assunto prima la responsabilità della funzione Security by Design, poi anche la responsabilità della funzione Fraud Management. Da ottobre 2021 ha la reponsabilità di Incident e Fraud Management. Il mondo della gestione delle frodi la entusiasma e le permette di conciliare molte delle competenze acquisite e sviluppate in questi anni, dall'analisi dei casi all'analisi dei processi, alla valutazione del rischio frode, alla definizione dei controlli, insieme al suo team. Rilevante è la collaborazione con le funzioni aziendali impattate e con gli omologhi team antifrode del settore. Le esperienze sviluppate nell'ambito della Sicurezza Informatica la aiutano nella detection di fenomeni sempre più evoluti e che sfruttano modalità di attacco e strumenti propri del mondo cyber.

Sara Bonini, ha oltre 35 anni di esperienza nell'IT, attualmente è responsabile della comunicazione di ASSOIT, l'Associazione Produttori Soluzioni di Stampa, Digitalizzazione e Gestione Documentale, per la quale coordina anche la redazione e la produzione delle guide dedicate alle tematiche di interesse dell'associazione tra le quali la cyber security. Nelle sue precedenti esperienze professionali è stata addetta stampa presso la Direzione Comunicazioni di IBM Italia occupandosi della tematica di sicurezza IT.

Giancarlo Butti, ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 170 corsi e seminari tenuti presso ISACA/ AIEA, ORACLE/CLUSIT, ITER, Informa Banca, CONVENIA, CETIF, IKN, 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

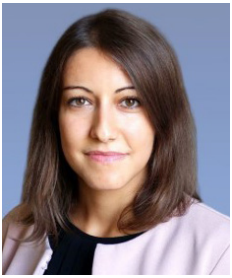
white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 30 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT. Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di ACFE, di DFA e del BCI e partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni (LA BS 7799), (LA ISO IEC 27001:2005/2013/2022), (LA ISO 20000-1), (LA ISO IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI

Georgia Cesarone, membro del Comitato Scientifico del Clusit, 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.

Martina D'Agnolo, da sempre affascinata dal mondo dell'informatica, ha conseguito una laurea in Economics, Management and Computer Science presso l'Università Bocconi e la laurea magistrale in Cyber Risk, Strategy and Governance presso l'Università Bocconi e il Politecnico di Milano. Attualmente, riveste il ruolo di Cyber Security Professional presso il CSIRT di Fastweb, dove mette in pratica le sue competenze multidisciplinari.

Stefan Dawid, è Responsabile in Brother Italia della Unit che si occupa di sviluppare il business a valore sul mercato della Pubblica Amministrazione, gestendo i partner specializzati e sviluppando e promuovendo soluzioni verticali dedicate. Con una laurea quinquennale in Ingegneria Meccanica conseguita al Politecnico di Milano, Stefan Dawid entra in Brother nel 2010 dopo aver maturato un'esperienza ventennale in multinazionali del settore Printing ricoprendo ruoli di crescente responsabilità in ambito marketing e vendite, sviluppando relazioni costanti con headquarter europei e worldwide.

Aldo Di Mattia, è entrato in Fortinet nel 2012 con il titolo di System Engineer per poi diventare nel 2018 Principal System Engineer & team leader, nel 2020 Manager Systems Engineering e nel 2022 Senior Manager Systems Engineering. Oggi è il responsabile di un team di sistemisti che supportano in tutta Italia le pubbliche amministrazioni centrali e locali, la difesa e le infrastrutture critiche. Nel 2005 si è laureato in informatica all'università La Sapienza di Roma con una tesi sperimentale sulla sicurezza di rete, lavorando tra il 2004 e il 2012 per due tra i più importanti System Integrator italiani nella sicurezza informatica in qualità di Systems Engineer, Security Consultant, Sr. Systems Engineer and Team Leader. In questi anni di lavoro ha maturato importanti competenze ed esperienze nel settore, conseguendo nel tempo più di venticinque certificazioni specialistiche sui principali vendor di sicurezza informatica, la certificazione indipendente CISSP di ISC2 e ha depositato quattro brevetti con Fortinet presso USPTO (United States Patent and Trademark Office's) contenti innovazioni tecnologiche nella cybersecurity in relazione a: API Cooperation; End-point protection and smart working; Deception; SD-WAN.



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.

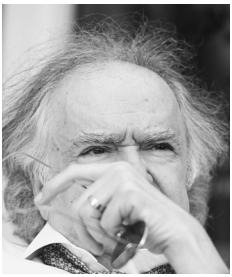
Guglielmo Duccoli, è un pubblicista, autore televisivo e divulgatore milanese, residente a Genova. Ha diretto alcuni dei periodici di informazione storica e culturale più diffusi in edicola, come "Civiltà", "Civiltà Romana", "L'Illustrazione Italiana", "Vivere con filosofia", "Guerre e Guerrieri", "Medioevo misterioso", "Far West Gazette", firmando anche diversi saggi di argomento culturale e artistico. Attualmente dirige i periodici per ragazzi "History Kids" e "Scienze Kids" (Sprea Editori). E' stato autore, insieme ad Alfredo Castelli e Giorgio Schottler, della docufiction in sei puntate "Alex" per l'emittente Italia 1 (Fininvest). Appassionato del mondo dei giochi, ha pubblicato alcuni board game di tema storico con editori nazionali e internazionali. Insieme con Nicola Lepetit ha scritto il saggio "In the Mind of ChatGPT" (ed. Dumas). E' fondatore e amministratore di Dumas srl, casa editrice e agenzia di editing specializzata in opere di divulgazione culturale.

Cinzia Ercolano, fondatrice e amministratore delegato di Astrea, agenzia nata e cresciuta nel mondo della tecnologia e, in particolare, della Sicurezza Informatica, si occupa del format del Clusit "Security Summit", uno degli eventi di Sicurezza Informatica di riferimento in Italia da oltre 15 anni. Dal 2015 si occupa attivamente della comunicazione del CLUSIT, coordinando le attività di ufficio stampa, social media e relazioni con le aziende. Nel 2020 ha ideato e creato, insieme a un gruppo di specialiste della cybersecurity, Women For Security, community tutta al femminile, che si pone l'obiettivo di mettere a fattor comune le competenze delle donne in ambito information security. Partecipa a diversi eventi di divulgazione del digitale in generale e della cybersecurity in particolare verso le nuove generazioni, inoltre contribuisce con la community a sostenere le campagne di diffusione delle discipline STEM e delle professioni cyber verso il mondo femminile in particolare e adolescenziale in generale.

Raffaele Fazio, è il Responsabile del Defense Center presso HWG Sababa. Con una solida esperienza nel settore della cybersecurity, Raffaele guida un team di oltre 70 analisti certificati, garantendo un monitoraggio continuo 24/7, rilevamento e risposta agli incidenti, intelligence e threat hunting. Il Defense Center, organizzato su tre livelli, protegge i sistemi critici dei clienti dalle minacce informatiche più avanzate, assicurando la resilienza degli ecosistemi complessi.

Ivano Gabrielli, laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, entra a far parte della Polizia Postale e delle Comunicazioni nel 2006. Assegnato inizialmente al Compartimento Polizia Postale e delle Comunicazioni di Genova, dal 2009 è trasferito al Servizio Polizia Postale del Dipartimento della PS. Nel maggio 2012 riceve l'incarico di Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Nel luglio 2017 è nominato Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, coordinando le attività di indagine del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC, della Sezione Cyber Terrorismo e della Sezione per il contrasto al Financial Cyber Crime. Dal gennaio 2022 è Direttore del Servizio Polizia Postale e delle Comunicazioni. Dal luglio 2024, nominato Dirigente Superiore della Polizia di Stato, assume l'incarico di Direttore del Servizio Polizia Postale e per la sicurezza cibernetica, incardinato nella neoistituita Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica e che ha ereditato anche le storiche competenze del Servizio Polizia Postale e delle Comunicazioni.

Paola Girdinio, membro del Comitato Direttivo del Clusit, è professore ordinario di elettrotecnica presso l'Università degli Studi di Genova, è stata preside della facoltà di ingegneria e membro del consiglio di amministrazione di Ateneo. È stata consigliere di amministrazione di Enel, di Ansaldo STS, del Distretto ligure delle tecnologie marine, di Banca Carige, della società D'Appolonia, di Fondazione Carige, di Banca Popolare di Bari, ricopre attualmente analogo incarico in Ansaldo Energia, Ansaldo Nucleare, in Wsense, in Fondazione Costa Crociere e in Fondazione Amga. È presidente del Centro di Competenza sulla sicurezza e ottimizzazione delle infrastrutture strategiche 4.0 e presidente dell'Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici. L'attività di ricerca di Paola Girdinio riguarda i settori della superconduttività applicata, dei materiali dielettrici a basse temperature, del calcolo di campi elettrici e magnetici con metodi numerici e della progettazione assistita da calcolatore di dispositivi elettrici e magnetici, compatibilità elettromagnetica industriale, cybersecurity per le infrastrutture.



Paolo Giudice, è segretario generale del Clusit. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto a interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi, membro del Comitato Scientifico di Clusit, è fondatore e senior partner di Rexilience. Già esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale/CERT-AGID (2015-2020) con la responsabilità dello sviluppo del CERT della Pubblica Amministrazione, già membro (mandati 2010-12, 2012-15, 2015-17 e 2017-20) dell'Advisory Board dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). In oltre trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di audit 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 Team Leader, 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.

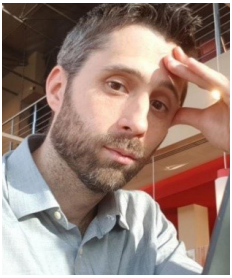
Sergio Inglima Modica, ha conseguito la Laurea Magistrale in Scienze Informatiche presso l'Università degli Studi di Palermo. Da sempre appassionato di sicurezza Informatica, oggi ricopre il ruolo di Technical Analyst presso il gruppo CSIRT di Fastweb, annoverando 9 anni di esperienza nel settore. Certificato nella gestione degli incidenti e delle minacce cyber, segue e monitora eventi notevoli e nuovi vettori di attacco. Si occupa altresì delle tematiche di Threat Intelligence strutturando il processo di raccolta e verifica delle fonti d'intelligence.

Lorenzo J.S. è impegnato in diversi ambiti professionali nei quali, grazie anche alle specifiche capacità legate al suo essere autistico, ha ottenuto risultati di notevole rilievo. Ad esempio la necessità di documentare (per sapere cosa sa…) lo ha portato a una intensa attività pubblicistica, la necessità di ordinare, elencare, schematizzare (per avere dei punti di riferimento in una realtà altrimenti caotica ed eccessivamente ricca di informazioni…) lo ha portato a occuparsi di organizzazione, la capacità di visualizzare soluzioni e di associazione logica, lo ha portato a introdurre innovazioni in numerosi ambiti… Ha pubblicato: con Raffaella Faggioli, Dentro l'autismo. L'esperienza di un clinico, la testimonianza di un Asperger, FrancoAngeli 2014 e con Andrea Mazzola, Autismo: studiare, lavorare, socializzare, ITER 2024.

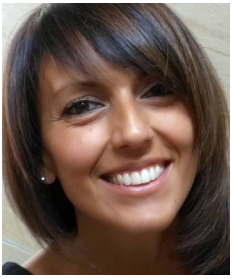
Federica Maria Rita Livelli, Certificata in Risk Management (FERMA/RIMAP certificazioni Iso 3100:2018) & Business Continuity (AMBCI Certification – BCI UK; CBCP Certification – DRI Usa), svolge consulenze in Risk Management & Business Continuity, oltre a effettuare un'attività di diffusione e di sviluppo 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.

Andrea Mazzola, è Psicologo e Psicoterapeuta con specializzazioni in ambito terapeutico (CBT, EMDR, DBT e Analisi del comportamento) e in ambito della Psicologia dello Sport. Dopo alcune esperienze nell'intervento precoce con i giovani e nella psichiatria, lavora prevalentemente con persone autistiche dall'adolescenza all'età adulta in contesti pubblici (ASST-Lecco) e privati (equipe AspergerLab Milano). È socio dell'AIAMC (Associazione Italiana di Analisi e Modificazione del Comportamento e Terapia Comportamentale e Cognitiva) e dell'AIPP Italia (Associazione Italiana per la Prevenzione e l'Intervento Precoce nella Salute Mentale) per cui ha contribuito a uno studio pubblicato nel 2023 volto a indagare lo stato dei servizi clinici di intervento precoce nel contesto nazionale (https://onlinelibrary.wiley.com/doi/10.1111/eip.13380). Ha pubblicato con Lorenzo J.S., Autismo: studiare, lavorare, socializzare, ITER 2024



Luca Memini, appassionato di informatica dalla tenera età grazie al Commodore 64, oggi ricopre il ruolo di Cyber Security Professional presso il gruppo CSIRT di Fastweb. Specializzato nella gestione degli incidenti e delle minacce cyber afferenti al mondo APT. Si occupa inoltre dello sviluppo di nuovi strumenti per migliorare le capacità di rilevamento e di risposta alle minacce da parte dell'azienda.



Sonia Montegiove, è informatica e giornalista; coordinatrice del progetto Cybertrials del Cybersecurity National Lab del CINI, programma **gratuito di gaming e formazione per le ragazze delle scuole superiori.** Ha fatto parte del gruppo di esperti nominati dal Ministero dell'Innovazione per individuare misure di contrasto all'hate speech. Fa parte del Comitato Direttivo di Women for Security dal 2021. Ha pubblicato: "Valentina nello spazio", favola rivolta a bambini e bambine per avvicinarli alle STEAM, "#gnomeide salvate le mamme e i papà" e "#gnomeide2 manuale di sopravvivenza ai social network", il cui intento è quello di guidare i genitori nella corretta costruzione di percorsi di consapevolezza digitale da intraprendere insieme ai ragazzi e alle ragazze. Ha condotto insieme a Chiara Lalli l'inchiesta giornalistica "Mai dati, dati aperti (sulla 194) perché sono nostri e perché ci servono per scegliere", diventata libro per Fandango editore.

Vincenzo Muratore, Laureato in Informatica per le Telecomunicazioni presso l'Università degli Studi di Milano, vanta 18 anni di esperienza nel settore della sicurezza informatica. Dal 2011 lavora in Fastweb, dove nel 2013 ha contribuito alla creazione e allo sviluppo del Security Operation Center Enterprise. Attualmente ricopre il ruolo di Managed Security Operation Coordinator, guidando un gruppo dedicato all'erogazione di servizi di sicurezza gestita assicurando che siano efficienti ed efficaci.

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. Alessio è inoltre membro del Comitato Scientifico di Clusit.

Corrado Pezzella, laureato in Ingegneria delle Telecomunicazioni, vanta oltre 15 anni di esperienza professionale in ambito ICT. Dopo 11 anni trascorsi nella consulenza manageriale presso multinazionali quali Accenture, Bip e KPMG, da circa 4 anni lavora in Fastweb, nel team di Product Design & Delivery, dove si occupa di Marketing per soluzioni B2B innovative, con un focus su prodotti e servizi in ambito Cloud e Cybersecurity. Le sue attività includono la ricerca di mercato per identificare esigenze dei Clienti e opportunità competitive, la collaborazione con i team di sviluppo prodotto per garantire soluzioni

allineate al mercato, la gestione di incontri con clienti chiave per la raccolta di needs e la creazione di materiali di marketing a supporto delle vendite. Inoltre, è impegnato nell'ottimizzazione dei processi, applicando metodologie come Design Thinking e Service Design per migliorare l'esperienza Cliente.

Umberto Pirovano, ha più di 25 anni di esperienza nelle Telecommunications e Cyber Security, con ruoli differenti in ambito prevendita, consulenza e people management. Attualmente ricopre il ruolo di Direttore tecnico e membro del CSO Office in PaloAlto Networks e aiuta i clienti nei loro percorsi di trasformazione verso il Multi-Cloud/DevSecOps, IoT/5G, SOC Automation e Digitalizzazione.

Luciano Pomelli, ha iniziato la sua carriera professionale lavorando sui sistemi IBM Mainframe, per poi ampliare la sua esperienza nel campo delle reti e delle tecnologie emergenti, con particolare focus sulla sicurezza, i data center e il cloud. Entrato in Cisco nel 1996, ha ricoperto diversi ruoli nell'ambito dell'organizzazione tecnica di vendita, maturando una solida esperienza nell'implementazione di soluzioni tecnologiche avanzate. Attualmente, ricopre il ruolo di responsabile tecnico per l'offerta di cybersecurity, dove guida l'innovazione e la protezione delle infrastrutture aziendali.

Luca Pupillo, Responsabile dei servizi di Cybersecurity e Architetture di sicurezza all'interno del SOC Enterprise di Fastweb, segue lo sviluppo dei servizi per i clienti Enterprise e Pubbliche Amministrazioni. Con oltre 22 anni di esperienza in ambito cyber e una passione nelle tecnologie ha lavorato in precedenza presso realtà nazionali come I.NET e internazionali come British Telecom. Nel corso della sua carriera è stato insegnante presso AFOL Metropolitana Centro Vigorelli, tenendo corsi di Network Security. Oltre ad aver maturato certificazione e competenze tecnologiche ha ottenuto certificazioni indipendenti coma la CISSP di ISC2.

Corrado Righetti, è Head of Security Operations Center (SOC) di HWG Sababa. Vanta un'ampia esperienza in cybersecurity, con un focus sulle operazioni di sicurezza e sulla gestione degli incidenti. Le sue competenze spaziano dalla gestione dei team SOC allo sviluppo di strategie di sicurezza e all'implementazione di avanzati sistemi di rilevamento delle minacce. Da oltre 15 anni guida l'evoluzione del SOC di HWG Sababa.

Pier Luigi Rotondo, è Advanced Technical Leader per i prodotti e le soluzioni IBM. Ha contribuito a molti progetti, nazionali e internazionali, su soluzioni per il Threat Management, Threat Intelligence, Attack Surface Management, Identity e Access Governance, e Single Sign-on. Con una laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Scrive articoli divulgativi, e contribuisce dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia su temi di cybercrime nel settore finanziario, presentando le tendenze del mercato della cyber security. È stato membro del Comitato Scientifico del CLUSIT dal 2021, ora è membro del Comitato Direttivo.

Manuela Santini, è Information & Cyber Security Advisor, con esperienza di oltre 10 anni sulle tematiche ICT e sicurezza delle informazioni. Si occupa di consulenza in ambito cyber security, supportando le aziende, in ottica risk-based, nella progettazione, gestione e verifica di sistemi e servizi coerentemente con le esigenze operative, di business e le normative nazionali ed europee in tema di Data Protection e Cybersecurity. Fa parte del Comitato Direttivo di Women For Security. È relatrice in webinar e convegni, nonché in corsi di formazione sulle tematiche di competenza e autrice di articoli in materia di sicurezza delle informazioni.

Mirko Santocono, nato nel 1975, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Torino e l'università ParisTech in Francia. Ha iniziato la sua carriera nell'ambito della consulenza IT per poi orientare la sua attività nel Product Marketing, dopo un Master in Germania. Ha lavorato presso importanti player ICT dove ha maturato competenze sia in ambito tecnologico che business, principalmente per il segmento Enterprise. Entrato in Fastweb nel 2008, ricopre oggi il ruolo di responsabile Marketing nel team Product Design & Delivery per lo sviluppo dei servizi Security, Cloud e IoT.

Dirk Schrader, è VP of Security Research presso Netwrix. Dirk è un veterano con ben 25 anni di esperienza nel campo della sicurezza IT che lavora per promuovere la resilienza informatica come approccio moderno alla lotta alle minacce informatiche. Possiede le certificazioni CISSP (ISC²) e CISM (ISACA). Oltre alla ricerca generale sulla sicurezza e alla scoperta delle vulnerabilità, Dirk è interessato alla ricerca mirata ai settori come sanità, energia e finanza. Inoltre, ha segnalato centinaia di dispositivi medici vulnerabili alle autorità e agli operatori sanitari di tutto il mondo. Dirk ha anche pubblicato articoli su argomenti quali gestione del rischio informatico, resilienza informatica e tattiche e operazioni di sicurezza IT.

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.

Maurizio Taglioretti, è Regional Manager SEUR presso Netwrix. Esperto di IT Audit, Security & Compliance Maurizio vanta una ventennale esperienza nel settore della sicurezza IT: prima di assumere questo incarico ha ricoperto diversi ruoli di crescente importanza a livello nazionale e internazionale in note aziende di sicurezza informatica. Maurizio è socio (ISC)2 Italy Chapter e partecipa attivamente come relatore a eventi sulla Sicurezza e la Compliance.

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

Girolamo Tesoriere, si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari. 15+ anni di esperienza nel settore delle TLC con una specializzazione nella consulenza sui servizi di Network Security e Cyber Security. Dopo aver lavorato per diversi anni come Technical Consultant in ambito networking e reporting operativo, nel 2013 partecipa allo start-up del Security Operations Center Enterprise di Fastweb. Al momento è responsabile della struttura di Cybersecurity OnSite Services & Consulting, all'interno del team di Operation che eroga i servizi di sicurezza per il segmento Enterprise di Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

Ivan Tresoldi, attualmente Senior Solutions Engineer in Wiz, è uno specialista nel campo della cybersecurity che unisce una profonda conoscenza tecnica a un approccio consulenziale, con l'obiettivo costante di aiutare le diverse organizzazioni con cui collabora nel proteggere i propri asset più preziosi. Grazie a esperienze professionali che spaziano tra ruoli ingegneristici e commerciali, è in grado di colmare il divario tra requisiti di sicurezza complessi e soluzioni pratiche ed efficaci. Che si tratti di guidare i clienti nell'adozione di metodologie di cybersecurity avanzate, implementare difese cloud-native o formare team specialistici sulle best practice del settore, Ivan è da sempre animato dalla passione di mettere i propri clienti nella condizione di affrontare con fiducia un panorama di minacce in costante evoluzione, con un impegno continuo all'aggiornamento professionale e un comprovato track record nell'accelerare la trasformazione digitale supportata dalla sicurezza by design.

Anna Vaccarelli, è Presidente del Clusit. E'stata Dirigente Tecnologo al Consiglio Nazionale delle Ricerche (CNR) nell'Istituto di Informatica e Telematica di Pisa. Per quasi 15 anni, a partire dal 1998, si è occupata di ricerca nel settore delle cybersecurity e dal 2010 di divulgazione del digitale in generale e della cybersecurity in particolare. Dal 2004 al 2012 è stata docente del corso di sicurezza informatica al Master congiunto Università di Pisa-Cnr in Tecnologie Internet. Nel 2011 ha ideato e poi coordinato fino al 2024, il progetto di formazione Ludoteca del Registro.it, un'azione di diffusione della cultura di internet nelle scuole, focalizzata soprattutto sulla cybersecurity, incontrando oltre 20.000 studenti. Nel dicembre 2021 ha ricevuto dall'Associazione Informatici Professionisti il premio come miglior informatico dell'anno. Negli anni ha coordinato numerosi progetti di ricerca nazionali e internazionali e scritto oltre 100 pubblicazioni scientifiche e tecniche. Dal 2020 è nel comitato direttivo delle Women For Security e dal 2022 nel comitato direttivo di Clusit.

Alessandro Vallega, è Fondatore e Senior partner in Rexilience.eu, società che si occupa di advisory in cybersecurity. In precedenza si è occupato di cybersecurity, governance, risk, compliance e, inoltre, di innovazione, scouting e acquisizioni in una società di consulenza e per un cloud provider internazionale con un ruolo EMEA. Si occupa di IT dal 1984 e di Information Security dal 2007. Alessandro è il fondatore e il chairman della Clusit Community for Security. È coautore, editor e team leader di quattordici pubblicazioni su diversi temi legati alla sicurezza e compliance della trasformazione digitale, tutti liberamente scaricabili dal sito Clusit. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. È nel Consiglio Direttivo / Comitato Scientifico di Clusit dal 2010. Speaker in conferenze, corsi e master universitari, insegna Analisi e Gestione del Rischio al corso Magistrale di Sicurezza Informatica all'Università Statale di Milano e ha una laurea in Scienza Politiche conseguita all'Università degli Studi di Milano.

Andrea Verri, è entrato a far parte di Cisco nel 2000 e ha sempre lavorato su tecnologie emergenti nel settore della sicurezza e dei data center, ricoprendo da allora diversi ruoli in azienda. Ora lavora nel team EMEA Security come Cyber Security Solution Engineer, Cloud and Workload Security con alcuni dei più grandi account aziendali di Cisco per progettare e mettere in atto strategie di protezione dei carichi di lavoro attuali ed emergenti (cloud native) in un ambiente multicloud. La sua area di competenza abbraccia diversi domini tecnologici (sistemi, networking, data center, sicurezza, cloud, containers, programmabilità) per adattarsi perfettamente alle tecnologie di protezione cloud di Cisco come Cisco Secure Workload, Cisco Multicloud Defense, Isovalent Cilium e Cisco Hypershield. Andrea è in grado di comprendere le strategie e le esigenze dei clienti e di mapparle verso soluzioni innovative e per questo motivo è considerato un consulente di fiducia da diversi clienti. Prima di entrare in Cisco, Andrea ha lavorato in altre aziende multinazionali dove ha ricoperto ruoli di consulenza e management sempre legati alle nuove ed emergenti tecnologie sia nel settore delle telecomunicazioni che in quello del software. Andrea è sposato, con un figlio e gli piace andare in mountain bike tutto l'anno.

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, Healthcare, Finance, Manufacturing).
- I Gruppi di Lavoro della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012.
- 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 e 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 attestat**i validi per l'attribuzione di oltre **48.000 crediti formativi** (CPE).

Nel 2024 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, dall'**11 al 13 marzo**, a Milano.

Saremo in seguito: il **25 giugno** a **Roma**, in **settembre** a **Napoli**, il **15 ottobre** a **Verona** e in **novembre** chiuderemo l'anno con un **Security Summit Streaming Edition**. Continueranno inoltre gli **eventi Verticali**, programmati il 28 maggio (**Energy & Utilities**), il 18 giugno (**Healthcare**) e il 5 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

FASTWEB

FORTINET

netwrix

paloalto NETWORKS

SECURITY SUMMIT

www.securitysummit.it