Rapporto

2024

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Indice

ASTREA Advanced Security, Training Research, Events Agency

Via Copernico, 38 - 20125 Milano

Prefazione

I dati che leggerete in questo rapporto, riguardanti l'anno 2023, sono, come al solito, peggiori rispetto a quelli registrati ed analizzati un anno fa.
E questo peggioramento vede protagonista negativo, in particolare, il nostro Paese.

I dati che raccoglie il Clusit si riferiscono solo agli incidenti gravi e si limitano alle fonti pubbliche con la conseguenza che la fotografia è pur sempre parziale rispetto al fenomeno nella sua interezza ma, comunque, che l'aumento degli incidenti gravi sia impressionante fra il 2021 e il 2023 è confermato indirettamente dalla quantità di casi di cui si sente parlare costantemente sui media.

Ammesso che la strategia messa in campo sino ad oggi sia utile (sicuramente a evitare una maggiore accelerazione del fenomeno), ancora non si vede all'orizzonte l'arretramento del fenomeno o perlomeno una capacità del sistema Paese di difendersi meglio di altri.

Personalmente credo che siamo davanti a uno scenario estremamente complesso che vede il Paese arretrato da un punto di vista di competenze digitali come ampiamente dimostrato dall'indice DESI della Commissione Europea che nel Report 2023 ci vede quart'ultimi su ventisette per competenze digitali di base e ultimi per laureati in materie ICT.
Inoltre, la quota di donne tra gli specialisti ICT è del 16%, ben al di sotto della media dell'UE del 18,9%.
Se poi andiamo agli investimenti in cybersicurezza possiamo constatare come nel 2023 l'Italia ha speso 2,149 miliardi di euro pari a circa 0,12% del PIL ma sappiamo anche che Paesi europei confrontabili come la Francia e la Germania spendono il doppio per non parlare di nazioni come gli USA che spendono lo 0,3% del PIL.
Si tratta di differenze immense che incidono sulla efficacia complessiva delle misure adottate a protezione dei sistemi.

A mio avviso occorre iniziare a pensare in modo innovativo staccandosi dalle politiche adottate sino ad oggi e quindi imponendo:

1. la valutazione della sostenibilità a tendere degli investimenti in digitale. Benissimo investire, ovviamente. Ma quanti imprenditori e pubbliche amministrazioni sono in grado e calcolano il costo a tendere che avranno le tecnologie adottate in termini di aggiornamento e manutenzione per evitare obsolescenza e in termini di cybersicurezza?

2. limiti nella possibilità di acquistare e liberamente utilizzare qualunque tecnologia in un far west dove quasi senza limitazioni chiunque può vendere e acquistare sostanzialmente quasi qualunque cosa;
3. responsabilizzazione maggiore per chi, in un contesto da far west digitale e senza aver pianificato gli investimenti del caso, arreca danni all'ecosistema e/o a terzi.

Siamo di fronte a un quadro estremamente complesso e le istituzioni e il legislatore stanno facendo la loro parte.

Lo spunto vuole essere quello di provare a ragionare in chiave innovativa valutando evoluzioni nell'approccio che possano portare perlomeno nel medio periodo a un rallentamento del trend e se possibile a una inversione.

Chiudo ribadendo l'auspicio che ormai mi faccio da tempo: che i conflitti armati che interessano due zone del mondo in particolare cessino nel più breve tempo possibile.

*** *** ***

E allora buona lettura del Rapporto che avete fra le mani.
Il risultato dello sforzo di un team di altissimo livello che da anni lavora per sensibilizzare il mondo pubblico e privato sui temi della sicurezza informatica.

Ringrazio, a nome di tutti gli Associati e di tutti coloro che lo leggeranno, i Colleghi che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2024.

Oltre 70.000 copie scaricate e più di 800 articoli pubblicati e servizi su web, cartaceo, Radio e TV nel 2023, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al Rapporto

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2023**.
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 delle Comunicazioni,** che ci ha fornito dati e informazioni estremamente interessanti su attività e operazioni svolte nel corso degli ultimi 12 mesi.
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**.
Segue un approfondimento sulla **Cybersecurity in Sanità: tra aumento degli attacchi e innovazioni normative e tecnologiche**, realizzato dalle Women for Security**.**

E anche quest'anno una survey realizzata da Netwrix, che ha intervistato 1.610 professionisti IT provenienti da 106 paesi, sul**le tendenze della Hybrid Security per il 2024**.

Questi sono infine i temi trattati nella sezione FOCUS ON:
- **Il mondo della sicurezza delle Identità**, a cura di RSA Security Italia
- **Attività della Task Force Cisco Talos in difesa dell'Ucraina**, a cura di Cisco
- **Secure Access Service Edge (SASE)**, a cura di Fortinet
- **Cloud adoption e superficie d'attacco: aumentare la visibilità e la protezione contro gli attacchi nell'infrastruttura e nelle applicazioni cloud**, a cura di Crowdstrike
- **Costruire la cyber resilience per la Space Economy**, a cura di Federica Maria Rita Livelli
- **CSIRT Network: Incident Response per una Crisis Management di successo in un contesto Internazionale**, a cura di NTT Data
- **Intelligenza Artificiale e Automazione: le chiavi per rivoluzionare il SOC**, a cura di PaloAlto Networks
- **La Sicurezza dei sistemi di acquisizione e stampa**, a cura di ASSOIT
- **Attraverso il tunnel del cambiamento: l'evoluzione della connessione sicura da VPN a ZTNA**, a cura di HPE Aruba Networking
- **Strategie di data security nell'era dell'AI Generativa**, a cura di Microsoft
- **Sviluppo sicuro del codice software**, a cura di Roberto Obialero

Analisi dei principali cyber attacchi noti del 2023 a livello globale

Italia sotto assedio

In questa prima sezione del Rapporto CLUSIT 2024, giunto ormai al suo dodicesimo anno di pubblicazione, analizziamo i più gravi cyber attacchi noti avvenuti a livello globale (Italia inclusa) nei 4 anni precedenti e li confrontiamo con l'analisi degli attacchi noti del 2023.

Dal punto di vista quantitativo, negli ultimi 5 anni la situazione è nettamente peggiorata, mostrando una tendenza pressoché costante, tanto che la media mensile di attacchi gravi a livello globale è passata da 139 a 232.

Confrontando i dati del 2019 con quelli del 2023 la crescita in termini numerici degli attacchi rilevati da fonti pubbliche è stata del 60% (da 1.667 a 2.779). Nel 2023 gli attacchi sono aumentati dell'11% a livello globale (ma in Italia sono aumentati ben del 65%).
Oltre ad osservare una crescita costante della frequenza degli incidenti, anche dal punto di vista qualitativo la situazione è peggiorata in modo significativo. La nostra valutazione della Severity media (indice di gravità) degli attacchi rilevati è peggiorata anno dopo anno, il che rappresenta un ulteriore moltiplicatore dei danni. Nel 2023, gli attacchi classificati come "critici" o "gravi" rappresentano ormai oltre l'81% del totale (erano il 47% nel 2019).

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

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

Nel 2022 a queste dinamiche di fondo, principalmente determinate da attività di matrice cybercriminale, si è aggiunto il conflitto tra Russia e Ucraina, che ha accelerato

il dispiegamento di capacità cibernetiche offensive di livello statuale, impiegate da entrambi i contendenti, dai loro alleati e in generale da tutti i principali attori globali, a supporto di attività di cyber-intelligence, di cyber-warfare e di operazioni ibride, realizzate sia "tramite" che "contro" il cyberspazio.

Mosca utilizza da tempo cyber operations per realizzare campagne di disinformazione di massa e plasmare la percezione pubblica. Nell'ambito del conflitto in Ucraina i principali obiettivi di queste attività sono: minare il governo ucraino ed il morale della popolazione, indebolire l'Alleanza Atlantica, influenzare l'esito delle prossime elezioni di vari paesi occidentali e mantenere il sostegno interno in Russia.

Oltre a queste classiche attività di disinformazione realizzate "tramite" il cyberspazio (in particolare tramite i social media), gli aggressori russi hanno intensificato le loro operazioni cibernetiche "contro" il cyberspazio, prendendo di mira il governo ucraino e i suoi membri, e lanciando attacchi distruttivi ad infrastrutture critiche, sia militari che civili.

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

Riassumendo le nostre impressioni sulla situazione attuale, potremmo affermare che, oltre ai danni crescenti causati dal cybercrime e dalle "normali" attività di intelligence che osserviamo da anni, dal 2022 siamo entrati in una nuova fase di "guerra cibernetica diffusa", che si conferma in crescita anche nel 2023.

In questo mutato scenario il nostro Paese risulta inevitabilmente sempre più colpito, come dimostra il significativo incremento di attacchi andati a segno nel 2023. Fin dall'inizio del conflitto nel 2022 abbiamo scritto "l'Italia è nel mirino", ed osservando i dati del 2023 dobbiamo concludere che il nostro Paese rappresenta un bersaglio particolarmente facile, dal momento che ha ricevuto ben '11% degli attacchi rilevati a livello globale (contro un 3,4% del 2021 e un 7,6% del 2022). Per questa ragione abbiamo aggiunto un capitolo specifico e 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 inevitabilmente crescenti.

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

Analisi dei principali cyber attacchi noti a livello globale del 2019-2022 e del 2023

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

+12%

è la crescita degli incidenti dal 2022 al 2023

Lo studio si basa sull'analisi di cyber attacchi noti, andati a buon fine e di particolare gravità, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle Organizzazioni vittima degli stessi.

Nel periodo in esame, tra gennaio 2019 e dicembre 2023 si sono verificati un totale di **10.858** cyber attacchi, suddivisi come mostrato in Fig. 1.

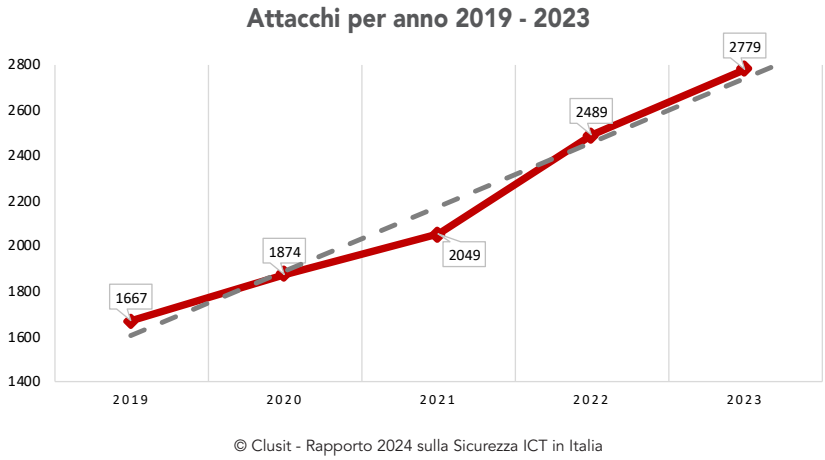


Fig. 1 - Andamento dei cyber attacchi nel periodo 2019-23

Nell'ultimo anno abbiamo registrato 2.779 incidenti, il numero maggiore di sempre, ed è interessante notare come già dal 2019 la realtà abbia iniziato a superare le previsioni indicate in grigio dalla linea di tendenza, e come tale trend si dimostri stabile negli ultimi due anni.

56%

degli incidenti censiti dal 2011 sono avvenuti negli ultimi 5 anni

A conferma di una costante recrudescenza dello scenario degli incidenti, gli eventi degli ultimi cinque anni (2019-2023) sono più della metà (56.3%) degli incidenti da noi classificati in totale dal 2011.

A livello di distribuzione mensile, la prima metà dell'anno vede registrare una attività molto più intensa, con un picco massimo ad aprile 2023 con 270 attacchi, anche in questo caso raggiungendo un record negativo mai raggiunto, come mostrato nella Fig. 2.

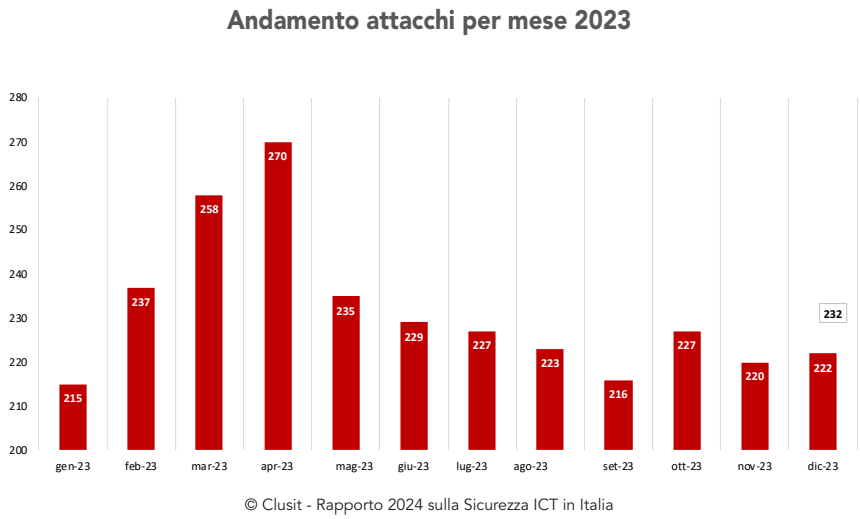


Fig. 2 - Numero di attacchi per mese nel 2023

Conseguentemente, anche la media mensile dei cyber attacchi (**Fig. 3**) è aumentata considerevolmente e arrivata a 232, con una tendenza di crescita costante, considerando che nel 2019 si attestava a poco più della metà.

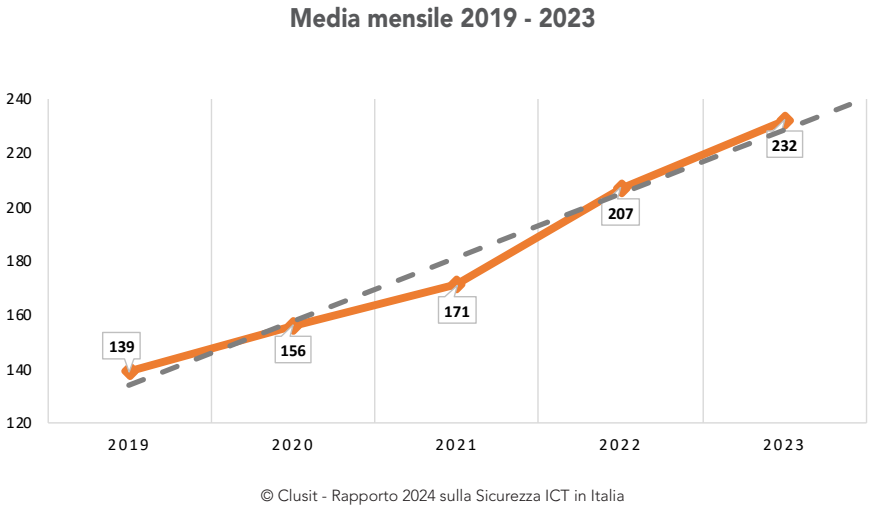


Fig. 3 - Andamento delle medie mensili nel periodo 2019-23

Distribuzione degli attaccanti per tipologia (2019 – 2023)

Il confronto della distribuzione degli attaccanti nel periodo dal 2019 al 2023 (**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 (+13,4% nel 2023 rispetto all'anno precedente). Questo andamento sostanzia le indicazioni degli analisti, che vedono 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 (sia on che off-line). Questo scenario produce maggiori risorse a disposizione di chi attacca, a fronte di proventi sempre maggiori.

+13%
È la crescita degli incidenti causati dal Cybercrime nel 2023

Al contrario, i fenomeni di *Espionage* e *Information Warfare* mostrano una diminuzione significativa (rispettivamente da 259 attacchi del 2022 a 178 del 2023 e da 103 a 46). Aumentano invece sensibilmente gli attacchi dovuti ad attività di Hacktivism, che quasi triplicano, passando dagli 84 del 2022 ai 239 del 2023.

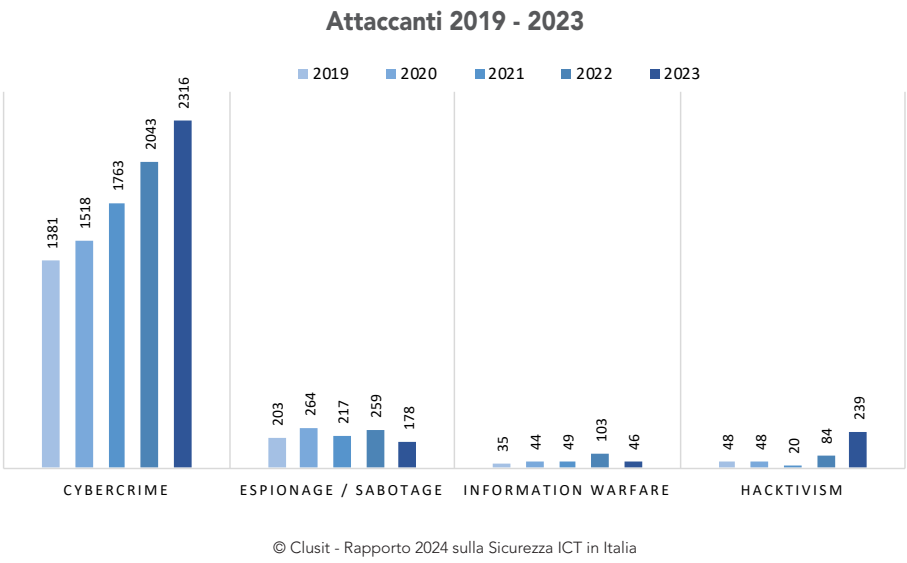


Fig. 4 - Distribuzione degli attaccanti dal 2019 al 2023

Nonostante la crescita in volume degli incidenti, la distribuzione degli stessi dati in termini percentuali (**Fig. 5**) conferma la tenuta del *Cybercrime* (83% del totale,+1 punto percentuale rispetto al 2022) e deve far riflettere su quanto questo ambito attiri le attenzioni della criminalità organizzata: da tempo ormai l'economia criminale sottesa ai reati informatici supera altre economie criminose di natura "tradizionale", forte anche delle dinamiche "as-a-Service" offerte agli affiliati, tanto da risultare "conveniente" anche per i criminali "non addetti ai lavori cyber".

1 su 10

è un incidente con matrice Warfare o Hacktivism

Espionage scende rispetto al 2022 di 4 punti percentuali, quasi dimezzandosi, come pure *Information Warfare* che passa dal 4% al 2%, mentre l'*Hacktivism*, raggiungendo l'8,6% del totale, si conferma in crescita con un aumento di 6 punti percentuali, a dimostrazione che nel 2023 le operazioni a sfondo politico e sociale sembrano essere state a livello globale predominanti rispetto a quelle militari o di intelligence (almeno per quanto riguarda la porzione divenuta di pubblico dominio), ben sapendo, in questo contesto, quanto siano complessi i processi di attribution.

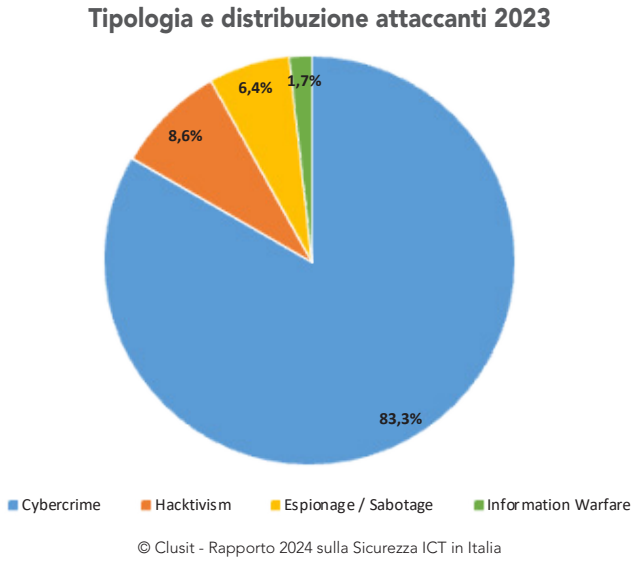


Fig. 5 - La distribuzione percentuale degli attaccanti tra il 2019 e il 2023

Distribuzione delle vittime per categoria

Il dato che emerge dall'analisi della distribuzione delle vittime degli attacchi nel periodo 2019-2023 (**Fig. 6**) è la riduzione dell'incidenza sul totale di *Multiple Target* (3 punti percentuali in meno rispetto al 2022) a dispetto di un aumento della componente *Healthcare* (+2 punti percentuali rispetto all'anno precedente) e *Financial / Insurance* (+3 punti percentuali).

+30%

è la crescita del numero degli incidenti a danno del settore HealthCare

+25%

è la crescita degli incidenti a danno del settore Manufacturing

Una quota percentuale sul totale maggiore rispetto all'anno precedente, in questa triste classifica, la recuperano anche i settori *Education, Manufacturing, Transportation / Storage* e *Wholesale / Retail*. Tra questi, quello della manifattura, in crescita costante fin dal 2019, giunge a questo punto al suo massimo storico (dal 2 al 6% del totale degli attacchi in 5 anni). Questo conferma un quadro abbastanza stabile, influenzato da caratteristiche fisiologiche dei diversi segmenti di mercato, nel quale va ricordato che la corretta lettura della distribuzione è "nessun settore merceologico si può ritenere esente dal gestire il cyber risk, anche perché riguarda tutti i suoi fornitori e tutti i suoi clienti".

Restano costanti nel 2023 le quote degli ambiti *Governativo / Militare / Law Enforcement* e *Professional / Scientific / Technical* (3%) mentre gli attacchi al settore *ICT* incidono sul totale in misura decrescente, un trend iniziato già a partire dal 2020, sebbene stiamo parlando di ancora di una fetta di poco superiore al 10% delle vittime totali.

Professional, Transportation, Wholesale pesano insieme per il 9,1%, ma mentre Professional è stabile, gli altri due settori sono in crescita.

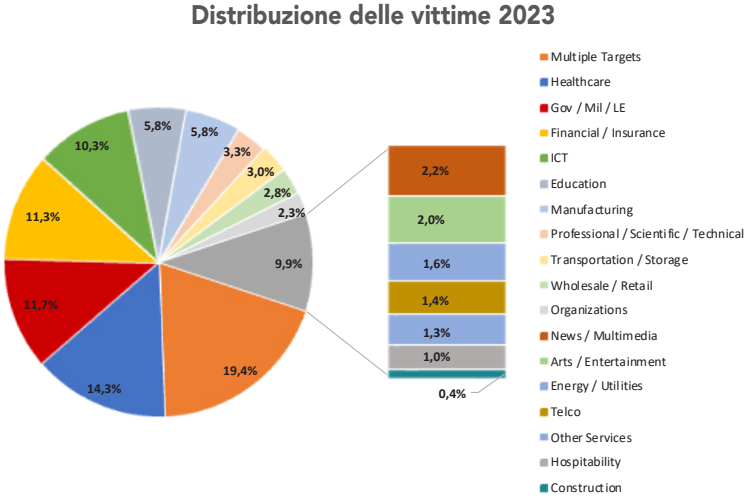


Fig. 6 - Distribuzione della tipologia di vittime nel 2023

L'analisi dei numeri assoluti (**Fig. 7**) in rapporto agli anni precedenti, consente di comprendere meglio come cambia lo scenario delle vittime in relazione al complessivo aumento degli attacchi.

+62%

è la crescita degli incidenti a danno dei settori Financial/Insurance

Se dal grafico precedente l'incidenza di *Multiple targets* risulta minore rispetto al 2022, in valore assoluto il numero di attacchi si distanzia poco da quanto avvenuto nell'anno precedente (539 contro i 541 del 2022) e la categoria si conferma quella più bersagliata per la seconda volta consecutiva, mentre l'ambito governativo viene addirittura colpito più duramente (325 attacchi contro 301).

Crescono in modo consistente i settori *Financial/Insurance* ed *Healthcare*, quest'ultimo il settore specifico più colpito dopo la categoria *Multiple target*.

Restano stabili gli incidenti che colpiscono il settore *ICT* e aumentano in modo consistente quelli verso *Manifacturing*, *Professional / Scientific / Technical*, *Transportation / Storage*, *Wholesale / Retail*.

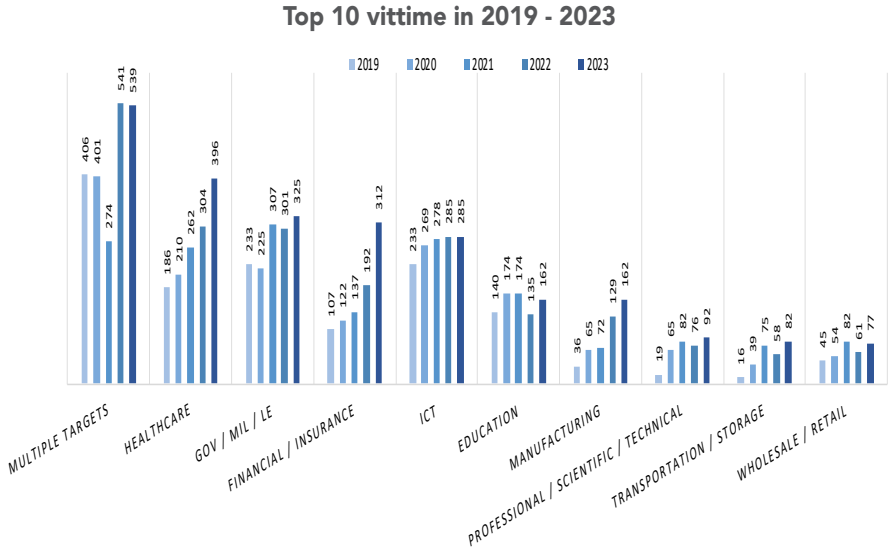


Fig. 7 - Distribuzione delle prime 10 tipologie di vittime dal 2019 al 2023

Distribuzione generale delle vittime per area geografica

La lettura dei dati della distribuzione geografica delle vittime (Fig. 8) rende indirettamente la fotografia di come stia variando la digitalizzazione nel mondo, ma anche di quali siano i Paesi maggiormente presi di mira dalle operazioni cybercriminali.

+7,5%
è la crescita degli incidenti avvenuti nel continente Europeo

Nel 2023 i valori sono sostanzialmente tutti in aumento e per il continente americano questa crescita è particolarmente accentuata, passando da 941 attacchi del 2022 a ben 1.226 nel 2023. L'Oceania è l'unica zona che vede diminuire gli attacchi, in opposizione con la crescita degli anni precedenti. Diminuiscono anche gli incidenti verso località multiple passando da 678 del 2022 a 596 del 2023.

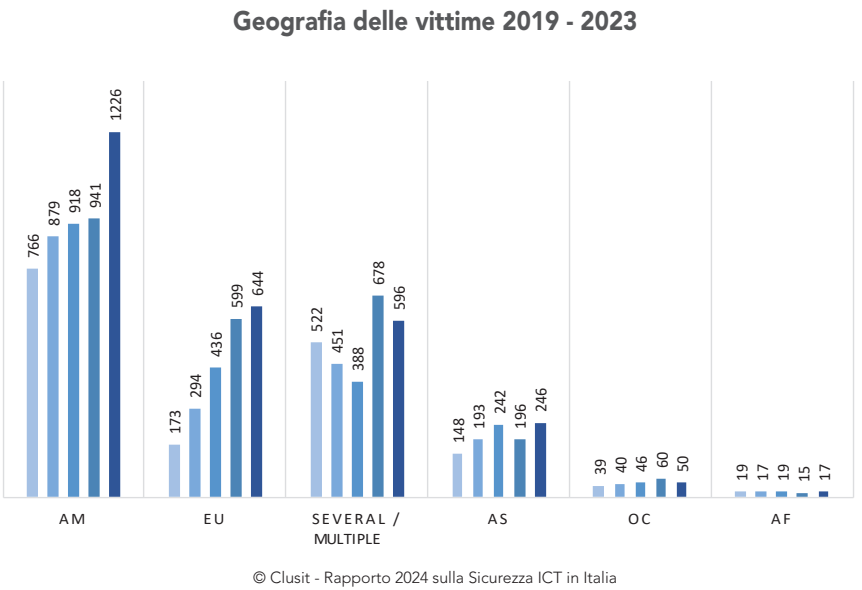


Fig. 8 - Distribuzione geografica della tipologia delle vittime nel periodo 2019-23

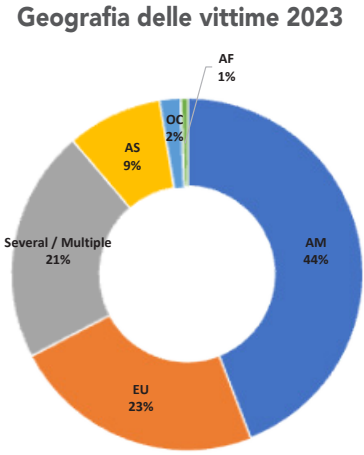


Fig. 9 - Distribuzione geografica delle vittime in percentuale per il 2023

La Fig. 9 presenta gli stessi dati ma in chiave di distribuzione percentuale rispetto al totale, confermando la preponderanza percentuale di vittime in America (44%), contro l'Europa al 23% e l'Asia all'9%. Circa un quinto degli attacchi (21%) è avvenuto parallelamente verso località multiple, mentre rimane marginale la componente, sul totale, degli incidenti riferibili ad Oceania (2%) e Africa (1%).
La consistenza dell'Europa si conferma stabile negli ultimi 3 anni, dopo la grande crescita del 2021.

Analizzando la variazione della distribuzione negli anni (Fig. 10), l'elevata crescita nel continente americano (+6 p.p. rispetto al 2022), causa il fatto che l'Europa, benché subisca un maggior numero di attacchi rispetto all'anno precedente, scenda di un punto percentuale attestandosi al 23%.

È rilevante la riduzione della consistenza, sul totale, del numero di attacchi sulle località multiple, che scendono di 6 punti percentuali, mentre c'è una leggera risalita dell'Asia che passa dall'8% del 2022 al 9% nel 2023. Resta stabile la situazione di Oceania e Africa.

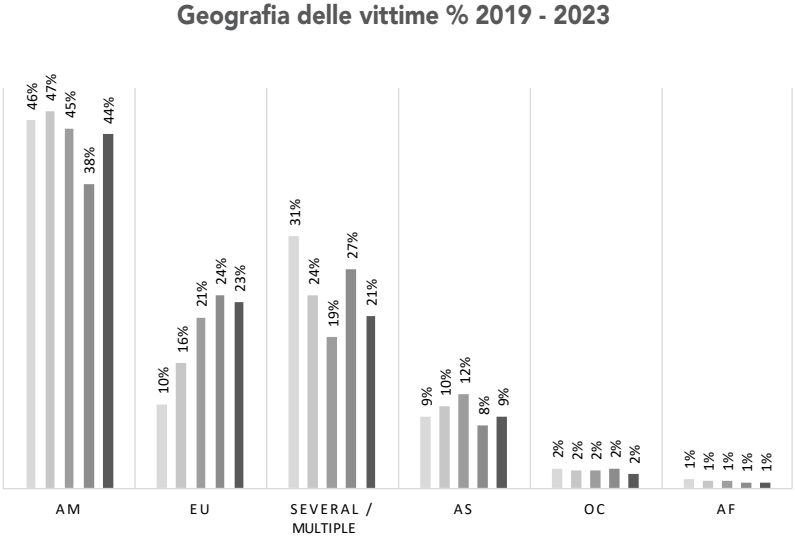


Fig. 10 - Distribuzione geografica percentuale della tipologia delle vittime nel periodo 2019-23

Distribuzione delle tecniche di attacco (2019 – 2023)

Nel 2023 il *Malware* continua ad essere la tecnica preferita dai cyber criminali (**Fig. 11**), sfruttata nel 36% dei casi. Sebbene questa categoria comprenda molte tipologie di codici malevoli, il ransomware è in assoluto quella principale e maggiormente utilizzata grazie anche all'elevata resa economica per gli aggressori, che spesso collaborano fra loro con uno schema di affiliazione.

+75,9%

è la crescita degli attacchi basati su vulnerabilità note e 0-day

Segue lo sfruttamento delle vulnerabilità (18%), note o meno (come nel caso dei pericolosi *zero-day*).

Le tecniche sconosciute, ovvero di cui non sono di pubblico dominio i dettagli circa quali siano state utilizzate nello specifico incidente, rappresentano un quinto del campione.

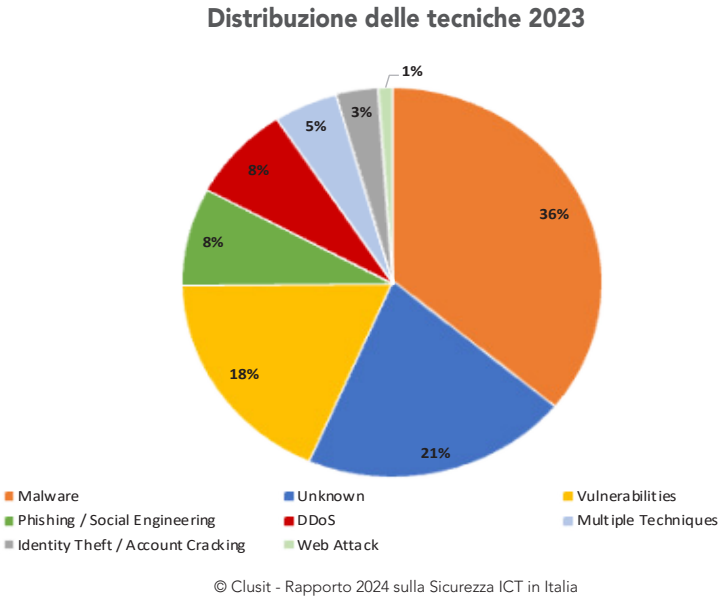


Fig. 11 - Distribuzione delle tecniche di attacco nel 2023

Il confronto con gli anni precedenti (**Fig. 12**) mostra una crescita degli attacchi che fanno ricorso a malware (1.002 contro i 910 del 2022), sfruttamento delle vulnerabilità (510 contro 290) e DDoS (220 contro 111), sostanzialmente raddoppiati rispetto allo scorso anno.

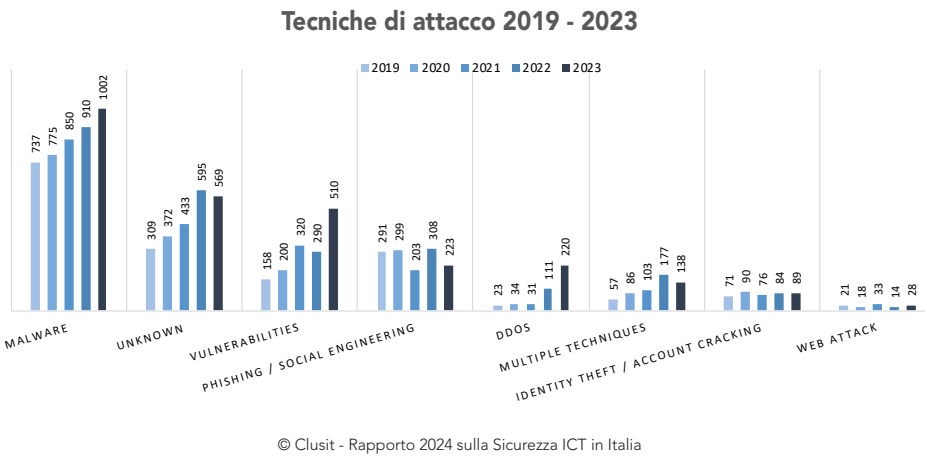


Fig. 12 - Distribuzione delle tecniche di attacco nel periodo 2019-23

Dalla distribuzione percentuale nel tempo, illustrata in **Fig. 13**, è possibile dedurre una serie di considerazioni importanti sui trend. Sebbene il ricorso ai Malware, come abbiamo visto, sia in costante aumento in termini assoluti, in termini percentuali diminuisce l'incidenza sul totale degli attacchi, consolidando una tendenza che osserviamo ormai da alcuni anni.

+98%

è la crescita del numero degli incidenti DDOS

Viceversa, gli incidenti *DDoS* continuano progressivamente a crescere (+4 punti percentuali rispetto all'anno precedente rispetto al totale), così come quelli basati su vulnerabilità (+6 punti percentuali).

In calo anche il ricorso a *Phishing / Social Engineering* (-4 punti percentuali), per quanto la rilevanza di tale tecnica quantitativamente suggerisca che sia un problema sul quale è ancora necessario lavorare molto (awareness degli utilizzatori). Diminuisce anche l'utilizzo di tecniche multiple (-2 punti percentuali).

Resta costante il ricorso a *Identity Theft / Account Cracking* (3% degli attacchi totali) e *Web Attacks* (1%).

Si riducono, in termini di incidenza sul totale, gli incidenti basati su tecniche sconosciute.

Da tenere monitorato l'utilizzo che la comunità dei cyber criminali ha iniziato a fare della AI per selezionare i target, scansionarli per trovare falle (es. vulnerabilità note),

analizzare il codice per trovare nuove vulnerabilità (es. 0 day) e produrre contenuti per phishing o codice per malware. Questo è un trend in rapida ascesa di cui sarà possibile osservare gli effetti solo in un prossimo futuro.

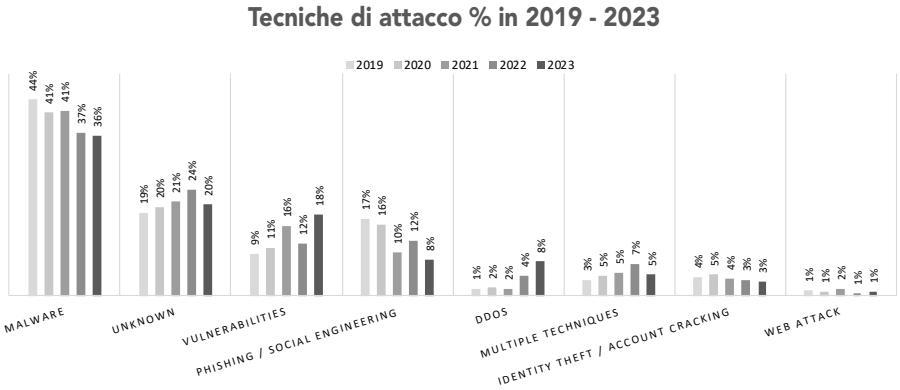


Fig. 13 - Distribuzione percentuale delle tecniche di attacco nel periodo 2019-23

Analisi della "Severity" degli attacchi

L'analisi della gravità degli attacchi si pone come obiettivo la valutazione degli impatti degli incidenti, che non necessariamente corrisponde con l'aumento dei numeri assoluti degli attacchi, né si può banalmente dedurre dalla vittima o dalla tecnica utilizzata.

Negli ultimi tre anni (**Fig. 14**), si è tuttavia instaurata una tendenza preoccupante che ha visto crescere progressivamente ed in modo consistente la gravità degli incidenti.

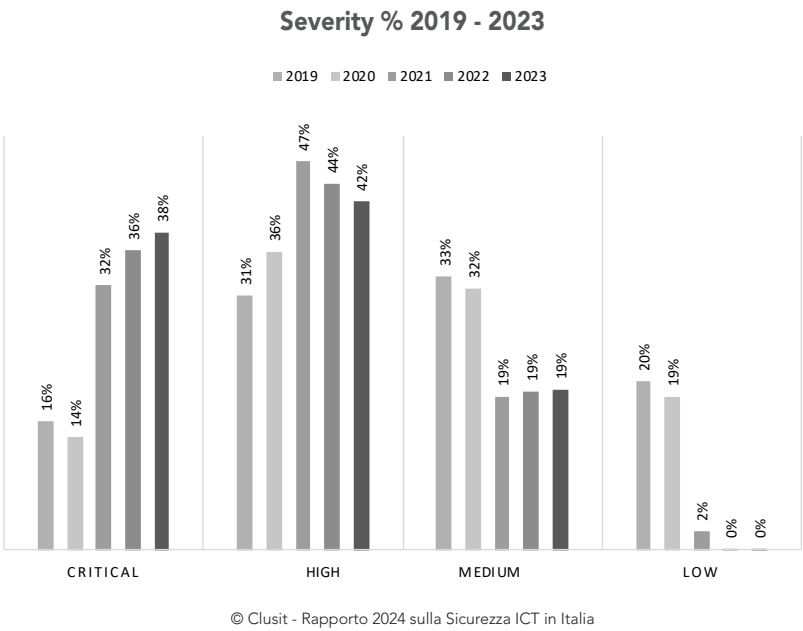


Fig. 14 - Andamento percentuale della Severity degli attacchi nel periodo 2019-23

Rispetto al totale degli incidenti registrati, gli attacchi con impatto critico sono in costante crescita dal 2021 e guadagnano 2 ulteriori punti percentuali nel 2023, sottraendo quote anche agli attacchi *High* che solo in quota percentuale risultano ridotti, dopo il picco massimo nel 2021, pur rappresentando oltre il 40% degli attacchi totali.

Restano sostanzialmente costanti gli impatti medi (19%), dopo il brusco calo del 2021, mentre spariscono di fatto gli impatti bassi, una tendenza già in atto dal 2022.

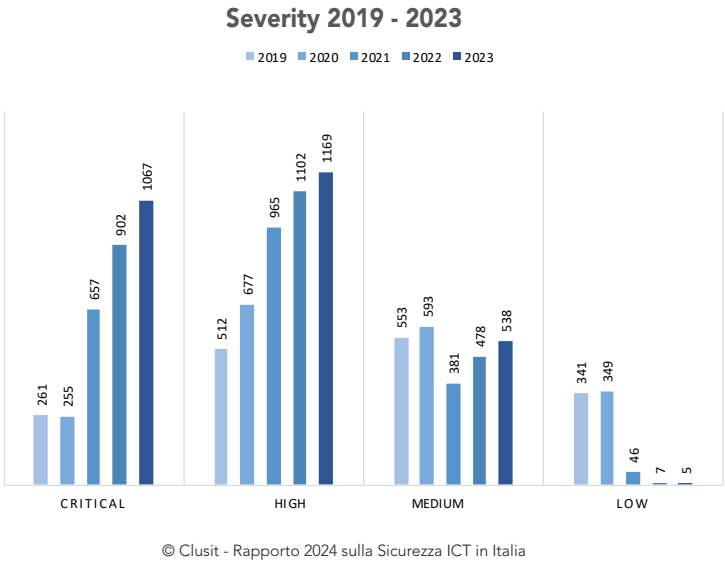


Fig. 15 - Andamento in termini assoluti della Severity degli attacchi nel periodo 2019-23

Come detto precedentemente, e tenuto conto dell'aumento complessivo degli attacchi, gli incidenti con impatti critici (Fig. 15) sono quelli che in valore assoluto crescono di più (da 902 a 1.067 incidenti nel 203), oscurando anche la crescita assieme degli attacchi con impatti *High* (1.169 contro i 1.102 dell'anno precedente). L'aumento del numero di attacchi con impatti *Medium* (da 478 a 538) non è sufficiente, come visto precedentemente, a determinare un aumento percentuale nella distribuzione totale rispetto agli anni precedenti.

4 su 5
sono i casi in cui, quando avvengono, gli incidenti causano la massima Severity (Critical o High)

In termini di distribuzione sul totale, (Fig. 16), l'area di maggior rischio (attacchi *Critical* e *High*) occupa nel 2023 ben l'81% del totale, contro l'80% dell'anno precedente.

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

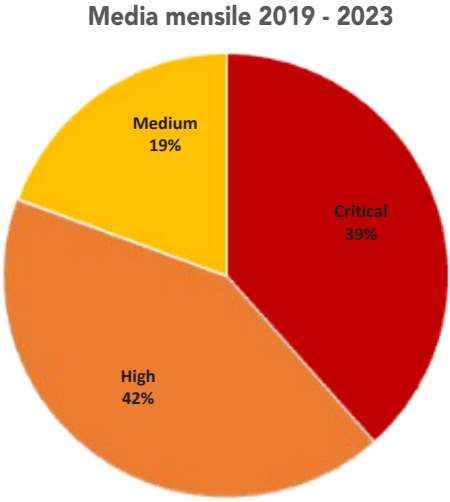


Fig. 16 - Distribuzione della Severity nel 2023

Severity per tipologia di attaccante

Il confronto tra i dati 2023 (**Fig. 17**) e 2022 (**Fig. 18**) evidenzia un'evoluzione nella severity degli incidenti dovuti a *Cybercrime*, andando a sottolineare che, indipendentemente dai numeri, gli attacchi nel 2023 condotti dai criminali informatici hanno determinato mediamente conseguenze maggiormente critiche.

Anche per quanto riguarda *Espionage* e *Information Warfare* gli attacchi con impatto critico sono aumentati considerevolmente, passando da valori prossimi al 50% a valori intorno al 70%. Questo andamento si può con alta probabilità spiegare con riferimento ai conflitti Russo-Ucraino ed Israelo-Palestinese che, almeno sul piano della cyber security, vedono coinvolti molti Paesi.

L'*Hacktivism* mostra invece una significativa riduzione percentuale degli attacchi critici (da circa il 50% del 2022 a poco più del 10% del 2023) rispetto al totale, un andamento costante di quelli ad alto impatto ed un aumento di quelli ad impatto medio. Il fenomeno si spiega in realtà con il consistente aumento degli attacchi afferenti a questa categoria, sempre in conseguenza con l'aggravarsi dello scenario geopolitico, nonché alla natura dimostrativa dei possibili effetti (la cui

-39,6%

è la riduzione degli incidenti di severità Critical per attacchi di Hacktivism

gravità, in confronto agli obiettivi perseguiti dai criminali informatici verso il mondo pubblico o privato, è spesso intrinsecamente più limitata).

Per tutte le categorie scompaiono di fatto gli attacchi a basso impatto.

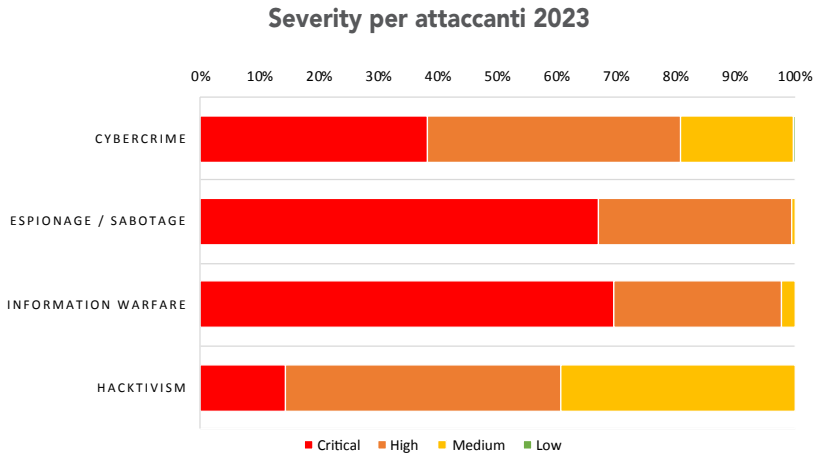


Fig. 17 - Distribuzione della Severity per attaccanti nel 2023

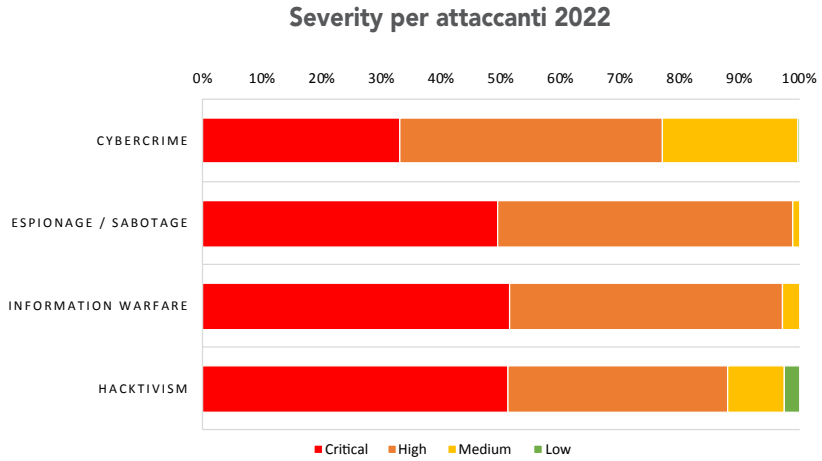


Fig. 18 - Distribuzione della Severity per attaccanti nel 2022

Severity per tipologia di vittima

L'analisi della severity per tipologia di vittima tra 2023 (**Fig. 19**) e 2022 (**Fig. 20**) mostra innanzitutto un aumento della criticità degli impatti verso i settori *Healthcare* (da poco più del 20% nel 2022 al 40% nel 2023), *Financial / Insurance* (da circa il 40% al 50%), *ICT* (dal 30% al 40%) e *Professional / Scientific / Technical* (dal 20% a ben oltre il 40%).

53,2%

degli attacchi ai settori GOV/MIL/LE determinano i massimi impatti

Questo approfondimento consente di evidenziare alcune tendenze interessanti: in termini di quantità di attacchi, infatti, le ultime due categorie (*ICT* e *Professional / Scientific / Technical*) mostrano andamenti in calo o costanti rispetto all'anno precedente, che però causano tipicamente conseguenze particolarmente gravi per le organizzazioni colpite. L'eterogeneità dei soggetti afferenti a questi settori non permette di fornire una spiegazione univoca per questo fatto, ma è opportuno lasciare aperte le due spiegazioni possibili: siamo di fronte ad attacchi particolarmente sofisticati, o a soggetti particolarmente impreparati a contenere le conseguenze di incidenti che, in altri settori, potrebbero essere gestiti con maggiore efficacia?

Restano invece costanti gli impatti critici verso bersagli multipli ed *Education* (entrambi intorno al 30%), mentre la gravità delle conseguenze degli incidenti cala anno su anno nei settori *Gov / Mil / LE* e, sebbene in misura ridotta, *Manufacturing* e *Wholesale / Retail*, pur restando molto elevata.

La categoria *News / Multimedia* nel 2023 non si trova più tra le prime dieci vittime e viene soppiantata da *Transportation / Storage*, che non possiamo quindi confrontare con l'anno precedente, i cui attacchi determinano attacchi critici in quasi un quinto dei casi.

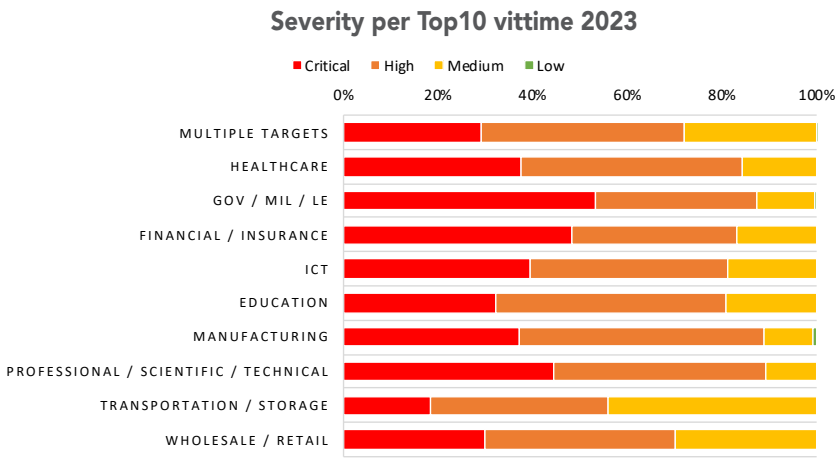


Fig. 19 - Distribuzione della Severity per prime 10 vittime nel 2023

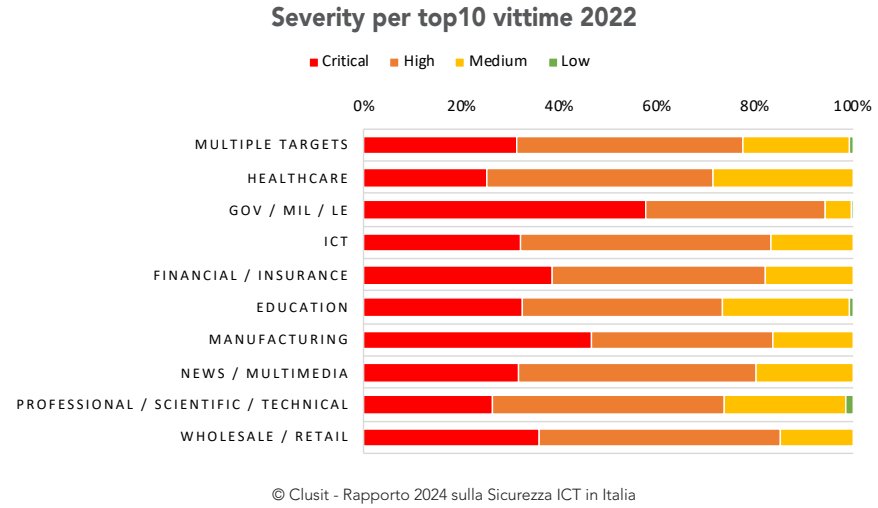


Fig. 20 - Distribuzione della Severity per prime 10 vittime 2022

Severity per tecniche di attacco

A differenza di quanto avvenuto nel 2022, nel 2023 tutte le tecniche utilizzate per generare incidenti hanno determinato una percentuale significativa di impatti critici sulle vittime (**Fig. 21** e **22**).

Se da una parte il Malware mantiene una costante del 40% di severity critica rispetto all'anno precedente, un dato di certo non rassicurante, gli incidenti basati sullo sfruttamento di vulnerabilità determinano nel 2023 conseguenze più rilevanti che in passato (da 40% a 50% di severity critica).

+10%

la crescita di eventi a severity «Critical» di incidenti Malware

Rimane costante la gravità degli attacchi che fanno uso di *Phishing / Social Engineering*, tecniche multiple e *Identity Theft / Account Cracking*.

Sebbene in aumento in termini numerici, i DDoS mostrano di avere una criticità dimezzata rispetto all'anno precedente, per i temi già illustrati nell'analisi della severity per tipologia di vittime, mentre gli attacchi Web acquisiscono per la prima volta negli ultimi due anni una quota consistente di severity critica.

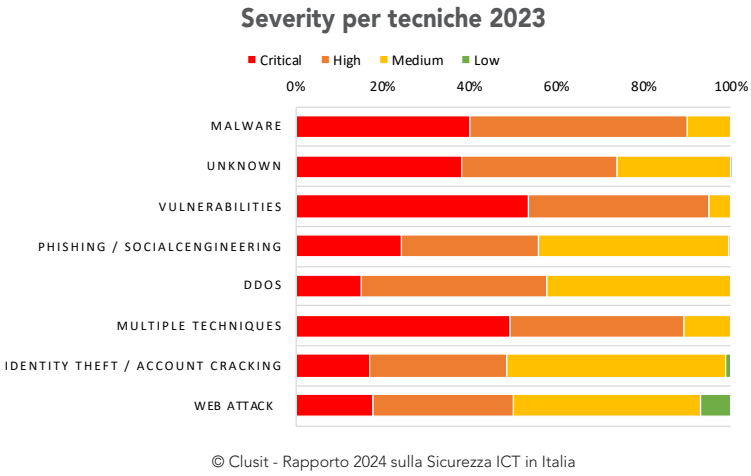


Fig. 21 - Distribuzione della Severity per tecniche di attacco nel 2023

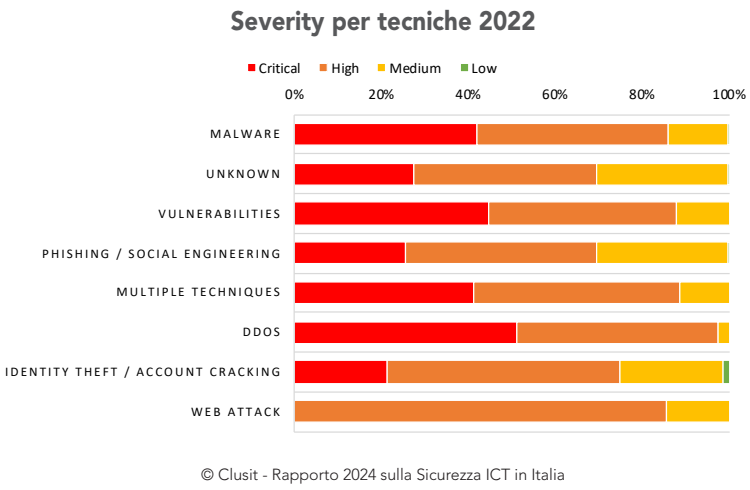


Fig. 22 - Distribuzione della Severity per tecniche di attacco nel 2022

Gli attacchi basati su tecniche sconosciute con *Severity* critica passano dal 30% del 2022 al 40% nel 2023.

Analisi degli attacchi alle organizzazioni governative e alle pubbliche amministrazioni

Il settore pubblico è stato interessato da un importante aumento del numero degli attacchi fra il 2022 e il 2023: 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.

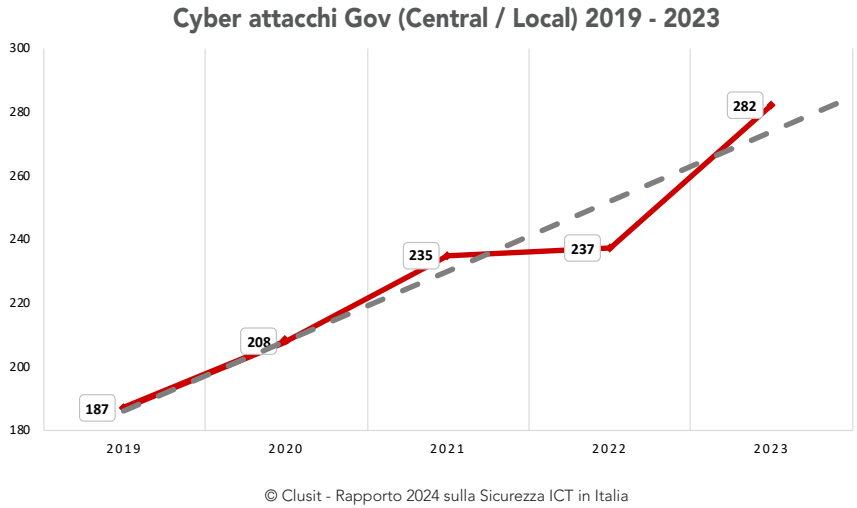


Fig. 23 - Attacchi al settore GOV *(CENTRAL/LOCAL) nel periodo 2019-2023*

Tra il 2019 e il 2023 il campione ha incluso **1.149** attacchi noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Globalmente la crescita è all'incirca lineare, con un forte incremento fra il 2022 e il 2023. Nell'arco dei cinque anni si è comunque passati dai 187 attacchi del 2019 ai 282 del 2023, con un incremento complessivo del 50% (**Fig. 23**).

+50%

*gli incidenti al settore GOV negli ultimi **5 anni***

La distribuzione degli attaccanti (**Fig. 24**) mostra chiaramente l'incremento del fenomeno Hacktivism, il cui numero di attacchi è più che raddoppiato fra il 2022 e il 2023.

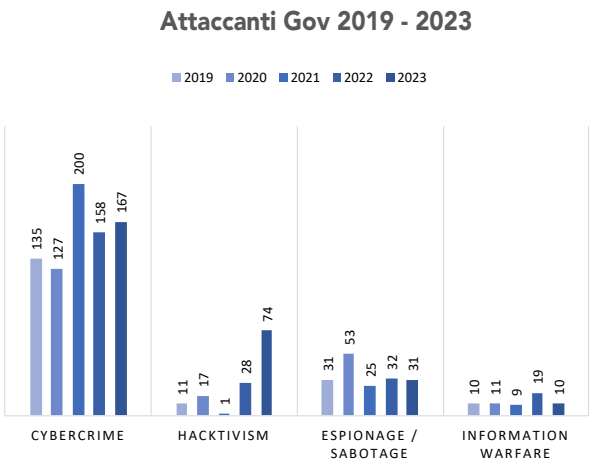


Fig. 24 - Distribuzione degli attaccanti per il settore GOV *(CENTRAL / LOCAL) nel periodo 2019-23*

La distribuzione geografica delle vittime (**Fig. 25**) mostra che gli attacchi sono tornati a crescere prepotentemente nel continente americano, soprattutto in Nord-America, e sono aumentati anche in Asia, mentre sono rimasti pressoché costanti in Europa in linea con gli altri settori.

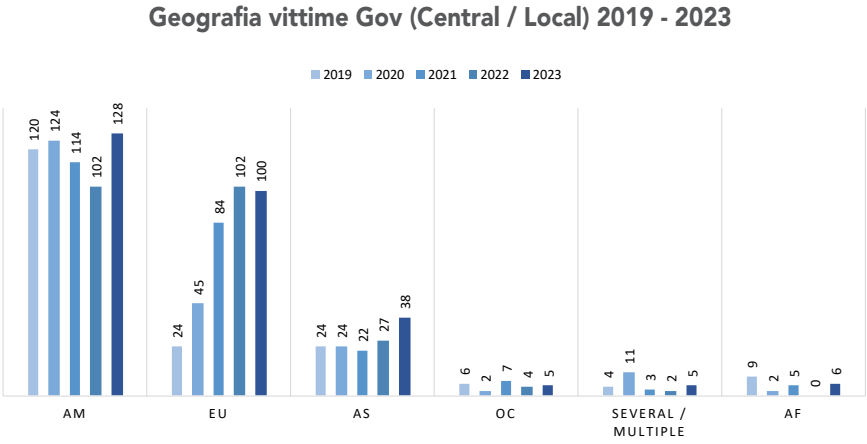


Fig. 25 - Distribuzione geografica delle vittime nel settore GOV *(CENTRAL / LOCAL) nel periodo 2019-23*

Per quanto riguarda le tecniche utilizzate (**Fig. 26**) notiamo che gli attacchi condotti mediante *DDoS*, tipici dei fenomeni di attivismo, sono più che raddoppiati nell''ultimo anno; quelli mediante *Malware* sono rimasti pressoché costanti, mentre quelli basati su *Phishing / Social Engineering* sono diminuiti.

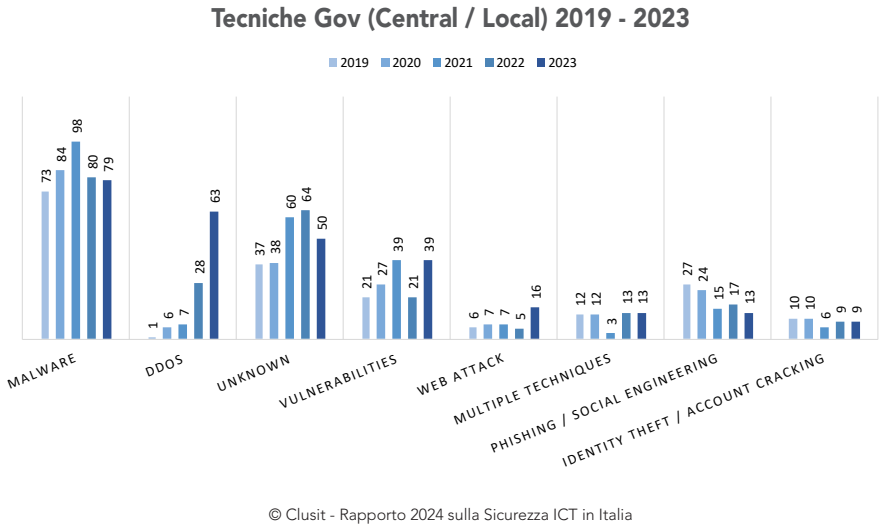


Fig. 26 - Distribuzione delle tecniche di attacco nel settore GOV *(CENTRAL / LOCAL) nel periodo 2019-23*

Analisi degli attacchi in Italia

In questa sezione, in continuità con quanto proposto per la prima volta nel nostro Rapporto relativo al 2022, offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti nei 12 mesi precedenti.

47%

degli incidenti censiti dal 2019 in Italia, è avvenuto nel 2023

Tra il 2019 e il 2023 il campione ha incluso **653** attacchi noti di particolare gravità che hanno coinvolto realtà italiane. Di questi, 310 incidenti sono avvenuti nell'ultimo anno in esame: oltre il 47% del totale degli attacchi censiti a livello italiano dal 2019 in poi si è quindi verificato nell'ultimo anno e la quota cresce addirittura al 76% se si considerano gli incidenti avvenuti a partire dal 2022 (498 eventi su 653), andando (purtroppo) a costituire una base di analisi statistica ormai consistente e affidabile per fornire degli indicatori significativi per questo Rapporto.

Come si evince dal grafico (**Fig. 27**), il dato del 2023 supera nettamente la linea di tendenza degli ultimi anni.

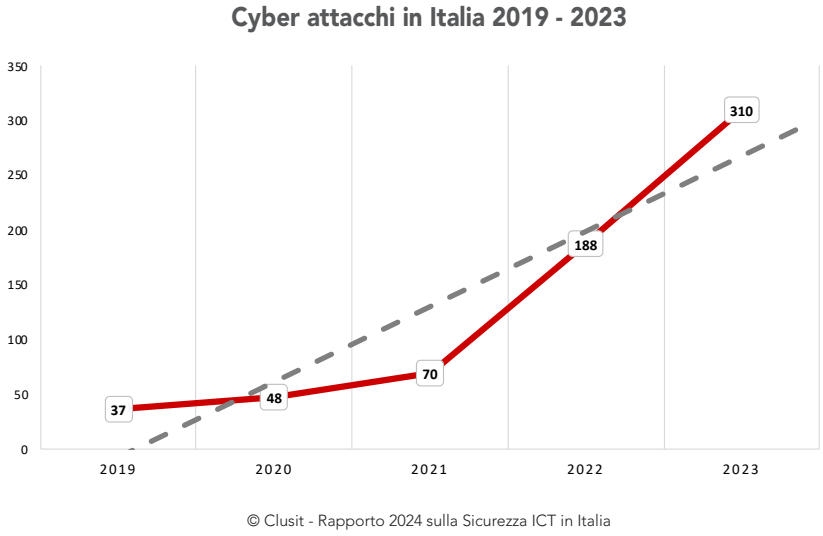


Fig. 27 - Distribuzione dei cyber attacchi in Italia nel periodo 2019-2023

Il numero di incidenti rilevati è cresciuto del 65% rispetto all'anno precedente, ulteriore aumento che fa seguito al preoccupante +169% registrato tra il 2021 e il 2022 (**Fig. 28**).

La situazione nazionale diventa ancora più preoccupante se confrontata, in termini di percentuali di crescita, rispetto al dato globale: all'aumento del 65% segnato dagli attacchi italiani corrisponde infatti un molto più contenuto +12% complessivo. Gli attacchi in Italia stanno quindi crescendo a un ritmo singolarmente elevato che, ancora una volta, può essere indice tanto di una tendenza da parte dei cybercriminali a bersagliare in particolare vittime italiane, quanto più probabilmente di una scarsa capacità delle stesse di proteggersi in maniera adeguata: un dato particolarmente grave, se si considera che gli investimenti in sicurezza in Italia continuano a crescere, come riscontrato dall'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano[1]:

+65%

è la crescita degli incidenti informatici in Italia nel 2023

[1] Fonte: https://www.osservatori.net/it/prodotti/formato/report/report-scenario-cybersecurity-italia-2023

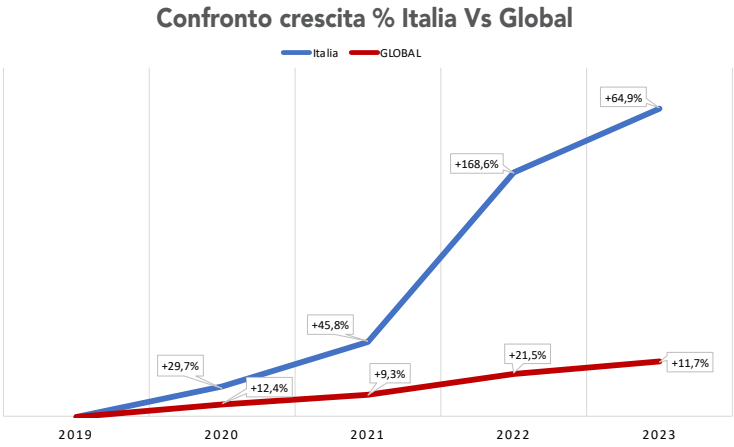


Fig. 28 - Crescita percentuale degli attacchi Italia vs. global - 2019-2023

11,2%

è la quantità di incidenti censiti in Italia rispetto al resto del mondo

Sempre in relazione al dato globale e a conferma di quanto appena affermato, è significativo notare che cresce anche l'incidenza degli attacchi rivolti a organizzazioni italiane rispetto al totale (**Fig. 29**): nel 2022 il dato italiano rappresentava il 7,6% del campione complessivo considerato a livello globale, mentre nel 2023 la quota sale all'11,2%.

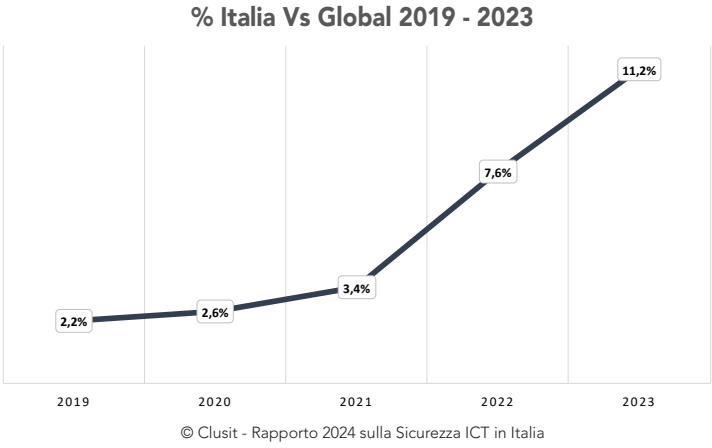


Fig. 29 - Incidenza degli attacchi italiani rispetto al campione globale - 2019-2023

Distribuzione degli attaccanti per tipologia (2019 – 2023)

Per provare a evidenziare alcune tendenze che stanno caratterizzando il panorama degli attacchi, è possibile innanzitutto valutare la tipologia di attaccanti, indicativa delle finalità e propedeutica a capire quali fenomeni prevalenti dobbiamo tenere sotto attenzione (Fig. 30).

Tra quelli avvenuti In Italia, la maggioranza degli attacchi noti si riferisce alla categoria *Cybercrime*, che rappresenta il 64% del totale (19 punti percentuali in meno rispetto al campione globale, che si attesta all'83%, vedere Fig. 5).

Seguono con il 36% gli incidenti classificati come *Hacktivism*, mentre nel nostro Paese non rilevano in modo significativo gli attacchi nelle categorie *Espionage / Sabotage* o *Information Warfare*. Naturalmente, come già detto per lo scenario globale, anche in questo caso il tema dell'*attribution* di tali tipologie di attacco è un aspetto rilevante: gli eventi – perlomeno quelli avvenuti nei primi 9 mesi dell'anno – si riferiscono per la maggior parte al conflitto in Ucraina, nei quali gruppi di attivisti agiscono mediante campagne dimostrative rivolte tanto al nostro Paese che alle altre nazioni del blocco filo-ucraino. Sebbene sia più che possibile un legame con il governo Russo (o più in esteso, con Paesi che stanno mantenendo una posizione ambigua nel conflitto in corso), non vi sono prove certe per classificare queste azioni come *state-sponsored attack*, pertanto come è possibile vedere, non risultano azioni afferenti alla categoria "Information Warfare".

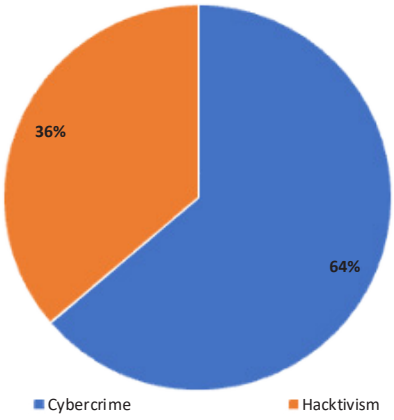


Fig. 30 - Attaccanti in Italia nel 2023

Sebbene continui a diminuire il peso percentuale del *Cybercrime* (che nel 2021 rappresentava il 100% degli attacchi e nel 2022 il 93%), è bene tenere presente che in termini assoluti gli attacchi mantengono invece un tasso di incessante crescita. Gli incidenti di questa tipologia nell'ultimo anno hanno infatti subito un aumento del 13%, passando da 175 a 197 attacchi rilevati (**Fig. 31**), in coerenza con il dato mondiale.

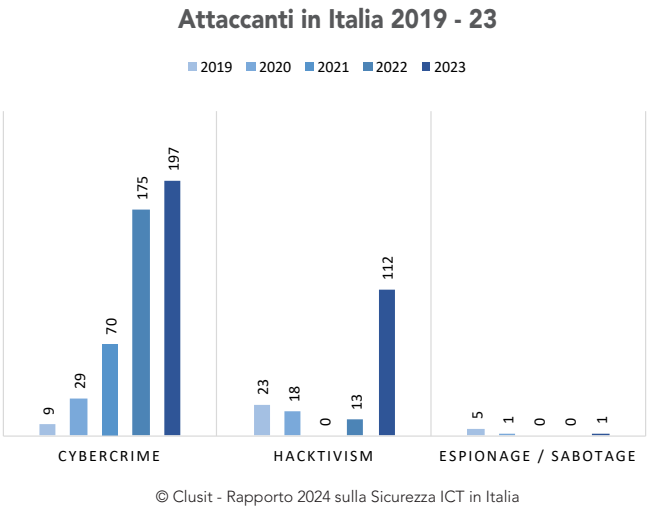


Fig. 31 - Attaccanti in Italia nel periodo 2019-2023

Il trend più significativo, però, è costituito dall'aumento degli attacchi di tipologia *Hacktivism*, che passano dal 7% del campione nel 2022 (13 eventi) al 36% del 2023 (112 eventi), con un aumento del **761%:** un dato che esaspera un andamento globale già preoccupante, che vede gli attacchi *Hacktivism* quasi triplicare, passando da 84 nel 2022 a 239 nel 2023, con un aumento di 6 punti percentuali (vedere Fig. 4). In Italia, gli incidenti afferenti a questa categoria costituiscono una quota molto superiore (36%) rispetto a quella globale (pari al 9%): **circa il 47% del totale degli attacchi con finalità "Hacktivism" a livello mondiale e che rientrano nel nostro campione, è avvenuto ai danni di organizzazioni italiane**.

47%

degli attacchi di Hacktivism a livello Global, è avvenuto a danni dell'Italia

Come discusso per i dati a livello mondiale, anche in questo caso l'analisi dei singoli incidenti permette di evidenziare sia attacchi con finalità politica specificatamente destinati a enti o aziende del nostro Paese, ma anche situazioni nelle quali le medesime azioni, perpetrate come campagne verso più nazioni, nel bel paese causano

conseguenze di maggiore portata (i.e. tale da rientrare nelle statistiche del nostro Rapporto) in relazione alle minori capacità di prevenzione e mitigazione della media delle piccole e medie imprese e pubbliche amministrazioni italiane.

Distribuzione delle vittime per categoria (2019 – 2023)

Guardando alla distribuzione delle vittime, la categoria merceologica per cui si rileva un maggior numero di attacchi è *Government* (19% del totale), grazie all'escalation degli eventi di *Hacktivism*, seguita da *Manufacturing* (13%), più frequentemente vittima di attacchi di matrice criminale.

1° GOV/MIL/LE

il settore più attaccato in Italia nel 2023

La ripartizione è significativamente diversa rispetto a quella del campione a livello mondiale, in cui le due categorie raccolgono rispettivamente il 12% e il 6% degli attacchi (occupando la terza e settima posizione): un quarto del totale degli attacchi rivolti al *Manufacturing* a livello globale riguarda realtà manifatturiere italiane.

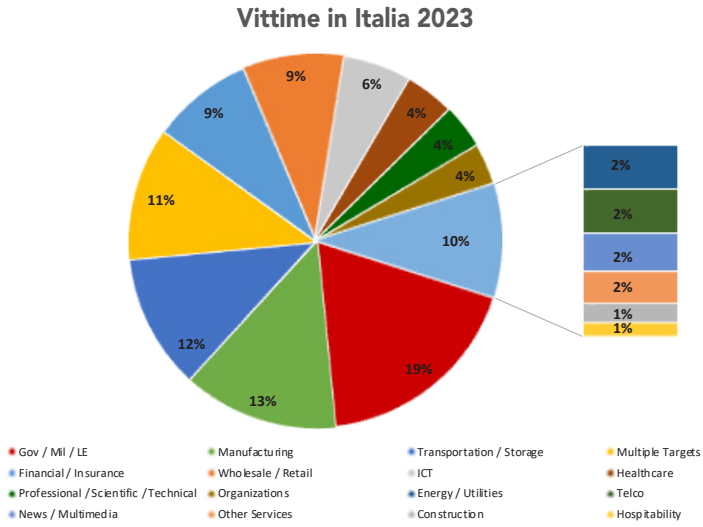


Fig. 32 - Distribuzione delle vittime in Italia nel 2023

Ancora una volta, si rileva rispetto all'anno precedente un aumento del numero degli attacchi per quasi tutte le aree merceologiche prese in esame, come dimostra una sempre più uniforme distribuzione del grafico a torta (Fig. 32).

2° Manufacturing

al secondo posto, in continuità con il passato

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

Se consideriamo i valori assoluti (Fig. 33), spicca *Transportation* che cresce del 620% rispetto al 2022, seguito da *Financial / Insurance* (+286%), *Organizations* (+175%), *Wholesale / Retail* (+170%) e *Telco* (+133%). *Multiple targets* si assesta sul +75%: ricordiamo che si tratta di campagne generalizzate utilizzate per causare attacchi non mirati, che continuano però a generare effetti consistenti e su larga scala. Guardando ai due settori maggiormente attaccati, *Government* ha un incremento del 50%, passando da 38 attacchi (2022) a 57, mentre *Manufacturing* si "limita" a un incremento del 17%.

+286%

è la crescita degli incidenti in Italia subiti da Financial/Insurance

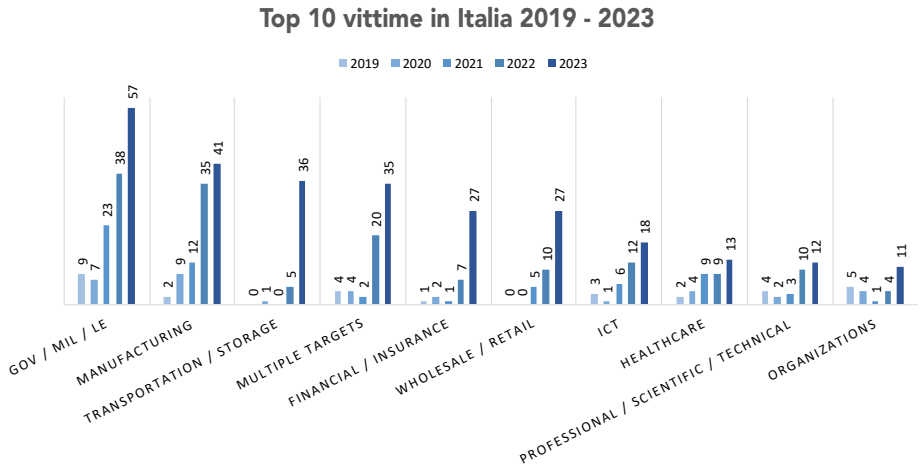


Fig. 33 - Top 10 vittime in Italia nel periodo 2019-2023

Esaminando l'evoluzione negli anni della distribuzione percentuale degli incidenti (Fig. 34) si nota una significativa differenza con gli analoghi dati a livello globale (Fig. 7): l'ambito *Multiple Targets* ha un leggero aumento rispetto al dato globale che appare invece in decisa diminuzione, e ciò dimostra tendenzialmente come il livello di preparazione delle aziende italiane non abbia un effetto trascurabile sulla crescita del numero di incidenti attribuiti da questo Rapporto: le campagne generalizzate di attacco, per altro tipicamente "transnazionali" nella loro diffusione, da noi *fanno più male*.

+50%

gli incidenti al settore GOV/MIL/LEA in Italia nel 2023

In termini di incidenza sul totale degli attacchi, sul settore *Transportation* in Italia si assiste ad un'impennata di ben 9 punti percentuali rispetto a +1 p.p. a livello globale, come pure *Wholesale/Retail,* che vede crescere la propria incidenza di 3,5 punti percentuali (solo +1 p.p. a livello mondiale).

La crescita della componente *Financial* (+5 punti percentuali) è significativa ma coerente con la crescita globale.

In particolare, la crescita consistente dei settori sopra citati (*Multiple Targets, Transportation, Wholesale/Retail, Financial),* ha effetto su come cambia, rispetto al 2022, la distribuzione delle percentuali dei settori colpiti nel 2023.

Ad esempio, sul settore *Government* si assiste ad una diminuzione percentuale, sebbene gli attacchi siano maggiori in termini assoluti, e lo stesso avviene per *Healthcare*, *Manufacturing* e *Professional*.

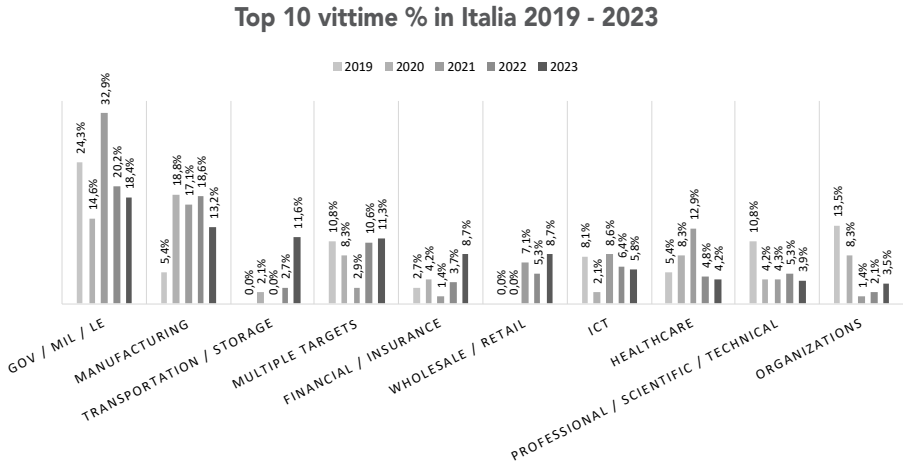


Fig. 34 - Le prime 10 categorie di vittime colpite in Italia in valore percentuale dal 2019 al 2023

Distribuzione delle tecniche di attacco (2018 – 2022)

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

Dalla **Fig. 35** si evince che la tecnica dominante è costituita dagli attacchi DDoS, che passano dal 4% del 2022 a ben il 36% di quest'anno, dato trainato in modo rilevante dall'aumento di incidenti causati da campagne di Hacktivism: molto spesso la tecnica di attacco utilizzata dagli hacktivist è proprio il DDoS, poiché si punta a interrompere l'operatività di servizio dell'organizzazione o istituzione individuata come vittima. Lo scopo degli hacktivist è di innalzare l'attenzione sulla loro causa e la violazione di un sito web, messa in atto tramite attacco DDoS, può essere un mezzo efficace per rendere evidente al pubblico il proprio messaggio di denuncia o protesta.

DDOS

è la principale tecnica di attacco in Italia

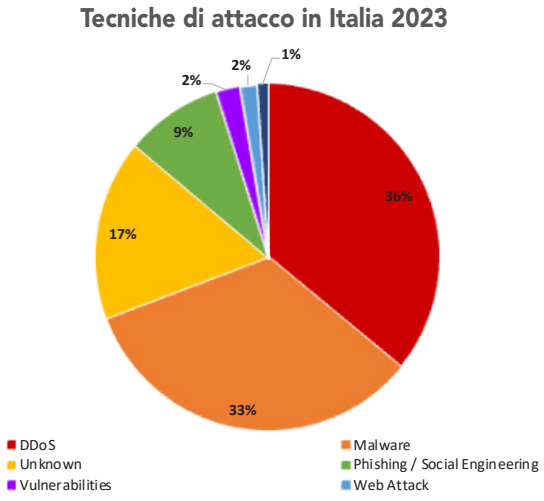


Fig. 35 - Tecniche di attacco in Italia nel 2023

La percentuale sul totale degli attacchi che sfruttano la tecnica del Malware scende in seconda posizione, passando dal 53% del 2022 al 33% del 2023, sebbene gli incidenti aumentino leggermente in valore assoluto.

+4%

è la crescita degli attacchi basati su Malware in Italia

Il Phishing ha invece un lieve aumento dall'8% al 9%, le Vulnerabilities si limitano al 2% ed entrano i web Attack con un 1,6%.

La categoria "Unknown" (ovvero gli attacchi per i quali le tecniche utilizzate non sono di pubblico dominio) registra una decrescita della propria quota, ora al 17% contro il 27% del 2022, aspetto a cui contribuiscono le diverse normative che impongono l'obbligo di segnalazione di alcune tipologie di incidenti.

È interessante studiare lo storico delle tecniche di attacco (**Fig. 36**), analizzandone le dinamiche. Il DDoS, che abbiamo visto coprire una larga fetta percentuale delle tipologie di attacco, segna un colossale incremento del 1.486% rispetto al 2022. Il Malware, benché percentualmente in discesa, registra un incremento del 4% e il Phishing, che rispetto al totale cresce solo di un solo punto percentuale, evidenzia una crescita dell'87% in valore

+87%

è la crescita degli attacchi phishing e social engineering in Italia

assoluto, dimostrando l'efficacia duratura di questa tecnica. Il fattore umano, in Italia ancora più che nel resto del mondo, continua a rappresentare un punto debole facilmente sfruttabile dagli attaccanti, tramite l'utilizzo di tecniche di social engineering. Gli attacchi condotti sfruttando in primo luogo delle vulnerabilità, scendono invece da 11 a 7.

Non può non colpire, rispetto ai dati di altri analisti di mercato, come ad esempio l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano che l'aumento di organizzazioni che si siano dotate di un CISO o abbiano aumentato gli investimenti in sicurezza informatica, possa aver incrementato la capacità di applicare le patch, gli aggiornamenti a correzione delle vulnerabilità note, iniziando quindi a determinare alcuni trend positivi.

I Web Attack diventano 5 nel 2023, mentre gli altri restano sostanzialmente stabili e trascurabili.

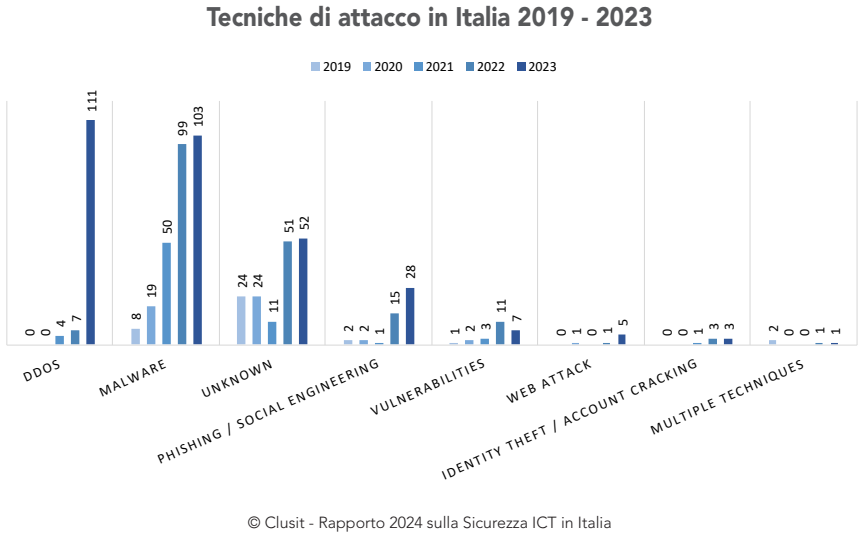


Fig. 36 - Tecniche di attacco in Italia nel periodo 2019-2023

Residuale è il furto di identità (1% vs. 3% del dato globale) che evidentemente non costituisce più un elemento preferenziale di innesco delle azioni di hacking a grande impatto come quelle censite da questo Rapporto. Non possiamo però dire che il fenomeno del furto di identità e di credenziali non sia rilevante nel nostro paese:

come testimoniano altre fonti[2], il numero di denunce di frodi e violazioni contro le persone e le piccole imprese è aumentato tantissimo negli ultimi anni, tuttavia con un impatto che non consente di rientrare nella statistica del nostro Rapporto.

Possiamo dire che nell'ambito delle applicazioni il livello di sicurezza conseguito dalle organizzazioni sia maggiore? In realtà, quello che sappiamo dal dato internazionale è che i criminali compiono questi attacchi con successo anche mediante tecniche non particolarmente sofisticate o innovative. La minore entità di questa categoria di attacchi si spiega piuttosto mediante due principali ragioni:

- come detto sopra, molti degli attacchi al mondo applicativo hanno conseguenze che non permettono di entrare nella statistica di questo Rapporto, come furti di identità, furti di denaro o frodi verso singoli individui o aziende;
- date le peculiarità delle singole implementazioni, violare le applicazioni in molti casi è, per i cyber-criminali, un'attività meno industrializzabile, a minore scalabilità e a maggiore rischio di esposizione degli attaccanti stessi. Il successo garantito ancora oggi da altre forme di attacco, in particolare se rivolte al mondo delle infrastrutture e del middleware, da tempo sembra rallentare l'evoluzione su scala di queste tecniche.

Analisi della "Severity" degli attacchi

Dal punto di vista della severity degli attacchi, il dato italiano (**Fig. 37**) si distacca parzialmente da quello internazionale.

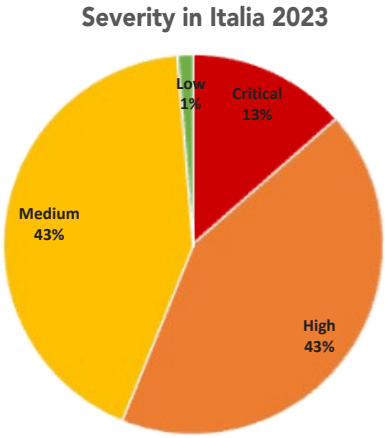


Fig. 37 - Severity degli attacchi in Italia nel 2023

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

Se la severity High è un punto percentuale più alta di quella globale (43% contro 42%), quella Critical è invece molto più bassa (13% contro 38%), mentre quella Medium, al contrario, è molto più alta: 43% contro 19%. Gli attacchi a basso impatto sono anche per l'Italia in percentuali trascurabili (1%). In generale quindi, appare un segnale positivo: gli attacchi danneggiano in maniera critica molto meno che nel resto del mondo e, anche se gli attacchi con impatto medio sono molto più numerosi, è pur vero che i loro danni sono più circoscritti.

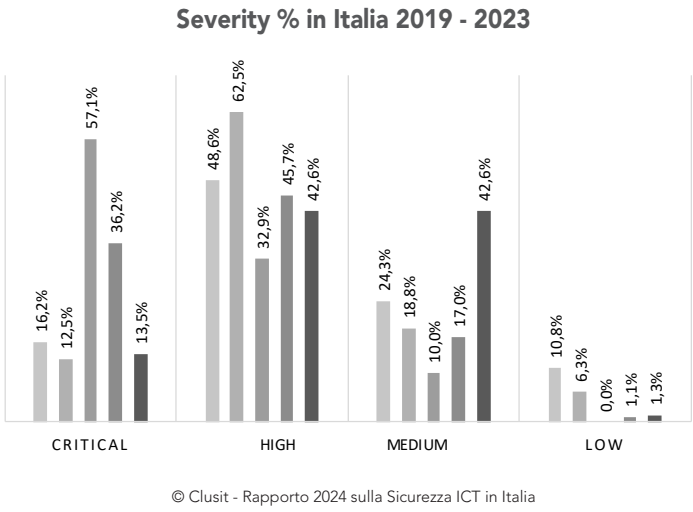


Fig. 38 - Severity degli attacchi in Italia nel periodo 2019-2023

Guardando alla progressione storica (Fig. 38), è possibile notare un significativo aumento dell'incidenza sul totale degli attacchi con severity Medium (+25 punti percentuali corrispondenti a un incremento del 312%) rispetto al 2022. Al contrario quelli con severity High e Critical diminuiscono rispettivamente di 3,1 e 22,7 punti percentuali **ma, in assoluto, gli attacchi con severity High aumentano del 53%**, mentre quelli con severity critical diminuiscono del 38%. Gli attacchi con severity bassa, infine, costituiscono una quota minima del campione. La serie storica italiana è in linea con quella globale per gli attacchi con severity alta, mentre è in controtendenza per quelli con severity Critical (inferiori) e Medium (molto maggiori).

Dobbiamo però analizzare queste tendenze nello scenario di insieme, ricordando che gli incidenti italiani costituiscono più dell'11% del campione mondiale con una crescita del 62% anno su anno. In tale contesto, le variazioni significative di Severity sono determinate anche e soprattutto da quegli incidenti che incidono maggiormente in Italia che nel resto del mondo. Partendo da queste considerazioni, asserire che nel contesto italiano la *Severity* media degli incidenti italiani sia minore non è corretto; piuttosto, i dati suggeriscono che nel nostro paese tutta una serie di attacchi potenzialmente a minore gravità, che negli altri paesi probabilmente tendono mediamente ad essere prevenuti o mitigati in misura maggiore (e quindi non entrano nelle nostre statistiche), in Italia arrivano ad avere gravità *Medium* e, talvolta, *High* innalzando il bel paese in questo triste ranking internazionale.

+53%

di attacchi con severity High in Italia, nel 2023

Allo stesso modo, come visto anche a livello globale (Fig. 20), gli attacchi di categoria Hacktivism che in Italia crescono particolarmente, sono tipicamente associati a una severity alta o media e più raramente a una *Severity* critica. Un ragionamento analogo vale per le tecniche di attacco. I DDoS, ad esempio, possono generare disagi notevoli alle vittime e ripercussioni sugli utenti, compromettendo la disponibilità di servizio e causando danni in termini sia economici sia reputazionali, ma in genere non presentano conseguenze di particolare gravità nel lungo termine.

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

Dall'analisi alla sintesi: dai trend alla strategia

Non possiamo negare che i dati che presentiamo all'interno di questo Rapporto, ormai da anni, siano costantemente e, in modo crescente, peggiorativi.

D'altro canto, l'obiettivo dell'analisi e della raccolta dei dati che, come Clusit, portiamo avanti dal 2011, è quello di supportare la comunità di aziende e pubbliche amministrazioni nella comprensione dei fenomeni legati alla sicurezza delle informazioni e alla cybersecurity, per fornire gli strumenti alle diverse tipologie di organizzazioni per indirizzare le priorità di intervento in relazione al proprio contesto operativo.

Per questo motivo, riteniamo essenziale sintetizzare in questa sezione alcune tra le principali considerazioni che, dalla lettura dei dati, possono costituire spunti di intervento per aziende pubbliche e private, e per le Istituzioni.

In primo luogo, è ormai evidente come sia necessario rafforzare la **governance della sicurezza e la capacità di identificare, analizzare, valutare e gestire i rischi informatici**, sia con misure preventive che di mitigazione, ma anche nella prospettiva di gestire il trasferimento del rischio verso terzi (sia in ottica di coperture assicurative, ma anche trasferendo l'onere dell'implementazione delle misure di mitigazione mediante il ricorso ad un outsourcing di qualità, per esempio nell'ambito di percorsi di *Cloud Journey*). La **capacità di determinare, anticipare e gestire** le evoluzioni legate alle minacce esogene, oltre che al contesto interno dell'organizzazione, è ormai fondamentale nel quadro che il Rapporto ci permette di delineare. Solo nel 2023 abbiamo osservato situazioni di cambiamento nel quadro delle minacce che hanno modificato sensibilmente lo scenario degli ultimi anni: il Malware che per la prima volta in Italia non è la minaccia più frequente, superata dai DDOS, la recrudescenza degli attacchi ai settori *Financial/Insurance, Healthcare, Manifacturing*, sono solo alcuni esempi.

Fondamentale resta, in Italia, mantenere una forte attenzione sul tema della consapevolezza delle persone: la crescita dell'87% degli attacchi di phishing ed ingegneria sociale testimoniano che quanto fatto fino ad oggi non è ancora sufficiente. Ci sono i termini per lanciare un allarme, 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, che ricomprendono anche tutti quegli eventi che interessano i singoli cittadini e le PMI che non possono far parte di questa analisi, per grado di pubblicità ed evidenza mediatica; il fenomeno sta infatti assumendo un grado di estensione che diventa sempre più preoccupante: anche nel 2023, il numero di denunce per truffe e frodi informatiche per numero di abitanti è secondo solo a quelle relative ai furti tradizionali in gran parte delle provincie italiane[3]. È pertanto imprescindibile che la Scuola, l'Università, i soggetti pubblici e privati lavorino in sinergia per **sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni**.
Insieme alla consapevolezza, rimane anche aperto il tema delle competenze più specifiche, il cui gap rispetto alle esigenze del mercato continua ad aumentare. Deve quindi essere ancora al cento dell'attenzione il tema del "*Reskill and upskill*" con riguardo alle **competenze STEM.**

[3] https://lab24.ilsole24ore.com/indice-della-criminalita/index.php

Resta poi imprescindibile rafforzare la **governance dei processi di patch & vulnerability management**. Tanto si è fatto in Italia, come si riscontra dalla riduzione degli incidenti a Severity massima, ma il preoccupante dato globale di crescita del 76% degli attacchi basati su vulnerabilità note e 0-day deve essere di stimolo a mantenere alta l'attenzione.
Come già detto nel 2022, basare la sicurezza e la gestione delle vulnerabilià solo sui penetration test triennali o annuali, non è più sufficiente per sostenere di presidiare la tematica delle vulnerabilità tecniche. È necessario **ragionare in ottica di** processi di reale **presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita (SSDLC** - Secure Software Development LifeCycle**)**, sia in ambienti waterfall che agili (SecDevOps), adottando **soluzioni** che affrontino efficacemente l**'ambito della sicurezza delle applicazioni** su ogni elemento (servizi esposti, front end, middleware, applicazioni mobili, IoT) e non solo in fase di scrittura del codice.

In particolare, le logiche di **security by design** devono diventare parte dei processi di sviluppo di prodotti e servizi a partire da quando i servizi vengono concepiti, dall'on-premise al cloud, con una sempre più stringente **gestione dei processi di sourcing e delle terze parti**, non solo in ottica di compliance, ma anche in ottica di tutela aziendale. Il fenomeno degli impatti derivanti dalla sicurezza della catena di forniture è forse uno di quelli che si dimostra più difficile da intercettare dai dati del nostro Rapporto, ma è certamente un fenomeno importante, sul quale si sta concentrando anche lo sforzo legislativo europeo e nazionale. Tale tema diventa particolarmente rilevante nel mondo manufatturiero, o comunque ovunque siano presenti sistemi **OT/IoT**, spesso bersagli semplici per attacchi come i DDoS o utilizzando le connessioni utilizzate dai manutentori.

Nel 2023 abbiamo ancora visto incidenti che hanno causato una perdita irrimediabile di dati a causa della debolezza delle soluzioni di backup rispetto alle modalità anche comuni di attacco. L'utilizzo di soluzioni di maggiore qualità si sta diffondendo, ma la creazione e protezione delle copie di sicurezza dei dati è un requisito imprescindibile che rimane un punto aperto ancora in troppe organizzazioni. Se l'interruzione dei servizi può essere una conseguenza a volte difficilmente evitabile di un attacco, lo stesso non si può dire per la perdita di dati che deriva da una inadeguata gestione dei backup, strumento che esiste praticamente da quando esistono i computer.

In quest'ottica, le organizzazioni dovrebbero attrezzarsi per **gestire ogni aspetto di una possibile crisi cyber** (*es. tecnologico, di compliance, di comunicazione, etc.*) 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.

Questo diventa particolarmente importante considerando che il vero messaggio che dovrebbe emergere dalla distribuzione è che ogni filiera è colpita ed ogni organizzazione deve riflettere sul fatto che non solo è essa stessa una possibile vittima, ma lo potrebbero essere tutti i suoi fornitori, clienti e stakeholder. Considerando l'importanza che il mercato sta attribuendo ai temi della sostenibilità, dell'ESG come forma per dare garanzia e fiducia al mercato, ecco che la cybersecurity diventa un elemento indispensabile per dimostrare di essere "degni" di quella fiducia.

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

Rimane anche il tema della **frammentazione di infrastrutture e servizi**, con una moltiplicazione di sforzi, ciascuno in sé poco efficace e per niente sinergico con gli altri. Rimangono quindi altrettanto significative iniziative come quella del Polo Strategico Nazionale e della strategia Cyber Nazionale, in particolare a valle di un anno in cui si assiste un forte cambiamento della componente (o motivazione) della schiera degli attaccanti, con un preponderante ritorno in primo piano dell'Hacktivism in relazione ad uno scenario geopolitico incerto. Non bisogna dimenticare che il 2024 è un anno in cui **si apriranno le urne per 2 miliardi di persone in 70 paesi in tutto il mondo**[4], e ciò accade in un momento in cui con l'introduzione della AI nella vita quotidiana pone di nuovo al centro, con alterne fortune ed efficacia, i temi dell'Etica e della Sovranità Digitale, che non possono esistere, tuttavia, senza garanzie sulla sicurezza delle informazioni.

[4] https://www.rainews.it/articoli/2023/12/il-2024-sara-anno-piu-elettorale-di-sempre-oltre-50-elezioni-nel-mondo-alle-urne-76-paesi-92b3804d-2921-43da-8e10-faec53454cae.html

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

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

Gli incidenti analizzati rappresentano certamente un campione significativo di quelli resi pubblici dalle fonti principali. Fra quelli resi pubblici, rimangono quindi esclusi incidenti riportati ad esempio da testate minori, locali o di Paesi del mondo non coperti dall'analisi. Nel corso degli anni, è aumentata l'attenzione alla copertura più ampia delle fonti italiane anche minori. In questo senso, possiamo avere quindi un bias

verso la rappresentatività dei paesi occidentali maggiormente presenti (ad esempio, gli Stati Uniti) e verso l'Italia. Questo aspetto, se correttamente gestito, può essere più di aiuto che di svantaggio per i manager italiani.

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

Ci sono poi incidenti che, pur essendo divenuti noti in contesti circoscritti, non hanno raggiunto le fonti pubbliche. Anche dove vi siano obblighi di notifica, infatti, questo non vuole dire che tutti gli incidenti siano notificati (dipende da caratteristiche dell'incidente e dalla normativa locale e di settore); soprattutto, le autorità in generale non rendono pubblici gli incidenti notificati. Lo stesso per vale per le denunce alle autorità di polizia, alle assicurazioni, e per i dati raccolti dai fornitori di connettività e di servizi di gestione incidenti. Si tratta di dati interessanti, ma in generale disponibili solo a questi soggetti, e quindi molto frammentati. Alcuni li pubblicano a loro volta sotto forma di statistiche. Il Clusit collabora con 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[5]. In questi casi, una delle parti potrebbe avere interesse a dare evidenza dell'attacco per motivi di propaganda, ma può essere difficile validare la veridicità di quanto affermato. Dove non vi siano sufficienti conferme sulle caratteristiche dell'attacco, o addirittura sul fatto stesso che l'attacco sia avvenuto, l'attacco non viene incluso nell'analisi.

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

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

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

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

Analisi Fastweb della situazione italiana in materia di cyber-crime

[A cura di Mario Boemi, Laura Bongiorno, Martina D'Agnolo, Sergio Inglima Modica, Marco Mereghetti, Luca Pupillo, Mirko Santocono, Gabriele Scialò, Girolamo Tesoriere, Fastweb]

Anche quest'anno Fastweb contribuisce a fotografare la situazione del cyber crime in Italia fornendo un'analisi dei fenomeni e dei trend più rilevanti elaborata dal proprio Security Operations Center (SOC) attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici, su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati nel 2023 oltre 56 milioni di eventi di sicurezza in linea per la prima volta con il dato del 2022.

Nel corso del 2023 si è assistito al consolidamento di alcune delle tendenze già osservate nel panorama dei fenomeni del cybercrime. Nonostante l'elevato numero di attacchi DDOS (oltre 15.000 eventi) e la gravità di eventi informatici malevoli ad alto impatto (+32%) continua a crescere la consapevolezza rispetto ai rischi informatici da parte delle aziende e delle pubbliche amministrazioni, testimoniata da una significativa riduzione della durata degli attacchi e da una riduzione del numero dei server che espongono su internet servizi critici (-8%), oltre che dall'utilizzo di strumenti di ricerca e monitoraggio che hanno contribuito a migliorare l'identificazione delle minacce.

L'Intelligenza Artificiale rappresenta un cambiamento significativo nell'ambito della sicurezza informatica, con vantaggi e sfide che ridefiniscono il panorama della difesa cibernetica. Gli algoritmi avanzati e la capacità di apprendimento continuo contribuiscono ad una protezione più sofisticata e reattiva migliorando notevolmente la capacità di rilevare e mitigare le minacce con una riduzione fino al 70% dei falsi positivi rilevati. Tuttavia le tecnologie come la GenAI possono essere sfruttate dagli attaccanti per aumentare l'efficacia e la numerosità degli attacchi, come nel caso del credential phishing che nel 2023 è aumentato dell'87% rispetto all'anno precedente.

In particolare sul fronte degli attacchi DDoS (Distributed Denial of Service) sono stati rilevati circa 2300 eventi significativi e circa 13.000 anomalie riconducibili a possibili attacchi alla rete di Fastweb. Il dato evidenzia un deciso incremento per quanto riguarda gli eventi DDoS ad alto impatto (ad oltre 100 Gbps), in aumento del 32% nel 2023 mentre diminuiscono le anomalie a basso impatto (-40%). Si ribalta, quindi, il trend visto nei due anni precedenti di decremento degli attacchi DDoS, dopo i picchi gestiti nel 2020. I settori più colpiti sono ancora Finance/Insurance e Pubblica Ammi-

nistrazione, che insieme costituiscono oltre il 55% dei casi. L'aumento più significativo è quello del settore del Gambling, cresciuto dal 2% del 2022 a quasi il 12% del 2023.

Il numero di server e device privi di livelli minimi di protezione e quindi esposti a rischi in rete è in costante diminuzione, con un trend in decrescita tra il 2023 e il 2022 pari all'8% e in progressiva riduzione dal 2019. Nel 2023 sono stati rilevati circa 38.000 server e device privi di livelli minimi di protezione.

Infine, si continua ad osservare una lieve flessione negativa nel volume di malware e botnet (-3% rispetto al 2022) e una riduzione nel numero delle famiglie di software malevoli (-29% rispetto all'anno precedente). Tra queste minacce, "ADload" occupa il 27% delle rilevazioni totali: un adware malevolo che, passando tramite applicazioni apparentemente legittime (come riproduttori video o agenti di supporto), viene scaricato tramite link maligni. Si riconferma la diminuzione della quantità di famiglie di malware e botnet sconosciute (-70% rispetto al 2022), un trend in continuità con quanto visto nell'anno precedente e che sottolinea una maggiore efficacia degli strumenti zeroday di difesa sul mercato.

Se gli USA rimangono saldamente al primo posto nella distribuzione geografica dei centri di controllo malware con il 36% del totale, la mappa di quest'anno mostra una distribuzione nuova, con UK e Brasile al secondo e terzo posto per numerosità di botnet C&C (Command and Control). L'Italia esce dalla top ten, pur mantenendo lo stesso ordine di grandezza in termini di dato assoluto.

Per quanto riguarda i tentativi di attacco orientati allo sfruttamento di specifiche vulnerabilità verso grandi aziende e pubblica amministrazione sono state rilevate diverse azioni messe in atto dal gruppo di hacker filorusso NoName057.

In continuità con quanto fatto durante il 2022, Fastweb ha monitorato anche le minacce relative ai servizi Mail che nel 2023, in crescita nel numero e nella tipologia. Il fattore principale utilizzato per veicolare attacchi rimane l'utilizzo di URL malevoli (90% dei casi, dato in linea con il 2022). Tra le più comuni tecniche utilizzate dai cybercriminali, sono in aumento le campagne fraudolente che utilizzano tattiche di social engineering per rendere credibile il raggiro (+13%). Nuovi gruppi di cybercriminali noti per condurre attacchi informatici mirati, come Hive0118 e Narwhal Spider, sono in aumento e mostrano uno scenario in continua evoluzione.

Fenomeno sempre più pervasivo nell'ambito delle tecniche di difesa e di attacco cyber è l'utilizzo dell'intelligenza artificiale. L'introduzione di algoritmi di intelligenza artificiale, in particolare nell'ambito della mail security, ha permesso di migliorare l'efficacia degli strumenti di detection e prevention sul riconoscimento di pattern malevoli contenuti nelle mail e nelle comunicazioni online. L'integrazione dell'AI all'interno

degli strumenti di riconoscimento e difesa delle minacce, inoltre, ha migliorato la capacità di raccogliere informazioni sui "threat actor", ovvero gli attori degli attacchi cyber, come evidenziato dall'aumento significativo di nuove "individual threats" (+17%) nel 2023. Nell'ambito del fenoneno del phishing l'intelligenza artificiale generativa permette ai criminali informatici di costruire attacchi sempre più verosimili e pericolosi attraverso la generazione, ad esempio, di contenuti testuali significativamente più accurati che non contengono errori ortografici o di traduzione che spesso, invece, rappresentano il primo segnale per riconoscere un attacco di phishing.

Per quanto concerne i fenomeni relativi alle frodi, anche nel 2023 le principali tipologie di frodi sono legate alla sottoscrizione con furto di identità e al fenomeno del CLI Spoofing Spoofing o manipolazione del numero chiamante.

Grazie alla collaborazione con 7Layers, società acquisita da Fastweb nel 2020 e specializzata in soluzioni avanzate di cybersecurity, il report include quest'anno per la prima volta anche il monitoraggio relativo alle minacce informatiche rilevate e contrastate tramite il servizio di Managed Detection and Response (MDR).

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 aumento del 260% di eventi e degli alert gestiti rispetto al 2022. Grazie anche all'utilizzo dell'AI da parte degli analisti è possibile così individuare e gestire con maggiore precisione gli eventi malevoli realmente impattanti ("true positive") e scartare i falsi positivi.

In conclusione, le rilevazioni di Fastweb del 2023 hanno mostrato un aumento progressivo della consapevolezza e della resilienza delle aziende e della pubblica amministrazione per quanto riguarda la sicurezza cibernetica: questo si traduce in un trend positivo ed incoraggiante di adozione di soluzioni di protezione, a loro volta capaci di contrastare un panorama di attacchi sempre più variegato e impattante. Nuovi strumenti, come l'intelligenza artificiale, pongono nuove sfide e nuove opportunità in particolare nel mondo dell'attacco e della difesa cyber. Molti dei trend osservati in questi anni si confermano strutturali, e, unitamente a nuove evoluzioni di scenario, contribuiscono a dimostrare la centralità e la necessità di dotarsi di sistemi di cybersecurity completi e pervasivi. Infatti, nonostante l'aumento degli attacchi in termini di volume e impatto, gli strumenti per combatterli diventano sempre più completi e resistenti. Tutto questo deve spingere le aziende a focalizzarsi sulla protezione dei propri asset strategici e delle persone, dotandosi di sistemi di sicurezza capaci di garantire l'operatività aziendale.

Nei paragrafi a seguire è riportato il dettaglio dei singoli fenomeni rilevati.

Malware e Botnet

Il numero di infezioni malware e attacchi veicolati tramite botnet, che interessano i server e i dispositivi appartenenti all'Autonomous System di Fastweb, nel 2023 ha registrato una leggera flessione negativa, pari al -2,5% rispetto al 2022. In continuità con quanto visto negli ultimi due anni, il numero di infezioni rimane pressoché stabile. Rispetto al picco registrato nel 2022 (208 famiglie, +21,6% rispetto al 2021), il numero di famiglie di software malevoli è tornato a valori simili a quelli degli anni precedenti: 148 famiglie (-29%).

Come si evince dal grafico sottostante, nel 2023 il trend di rilevazione del numero di dispositivi infetti è stato crescente durante l'anno (linea arancione), un'inversione di tendenza rispetto a quanto registrato nel 2022 (linea grigia) dove, rispetto ad un picco a gennaio, il numero di infezioni è andato a diminuire durante l'anno.

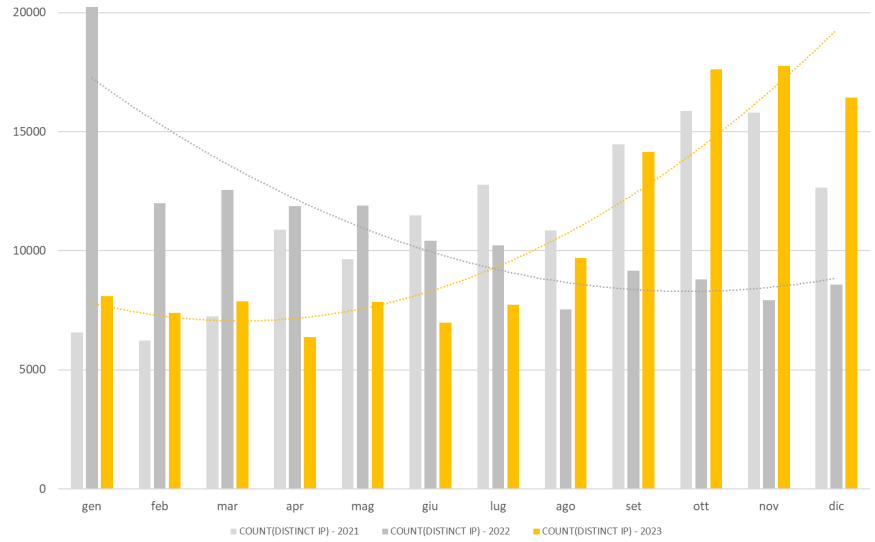


Figura 1 - Distribuzione temporale del numero di infezioni rilevate *(Dati Fastweb relativi agli anni 2021, 2022 e 2023)*

La famiglia di malware più numerosa nel 2023 è risultata "Adload", con il 27% del totale. 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.

La famiglia di malware "downadup" (conosciuta anche come "conficker") come nel 2022 supera in valore assoluto quella di avalanche-andromeda, con rilevazioni pari al 25% del totale delle infezioni. 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 ad una variabile silente distribuita probabilmente attraverso circuiti P2P dal 2021. Al terzo posto troviamo avalanche-andromeda, piattaforma 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 è stata 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.

Come è visibile nel grafico dell'andamento mensile (sotto) dal mese di agosto si registra un importante spike nella numerosità di malware della famiglia ADload, che registra nell'ultimo quadrimestre dell'anno numeriche così elevate da essere la più significativa del 2023. Questo fenomeno può essere dovuto in primis all'aumento del target di attacco del malware, che se prima era presente soprattutto per il sistema operativo dei MAC, ora risulta prevalente anche contro i PC. Un'altra ragione può essere ricondotta alla natura del malware stesso, che sfruttando le pubblicità, può essere stata utilizzata in maniera prevalente sotto forma di advertisement apparentemente legittimo. In ultimo, l'aumento generalizzato dei malware nella parte finale dell'anno può essere stato influenzato dal nuovo conflitto israelo-palestinese.

Il trend positivo di diminuzione delle infezioni causate da malware appartenenti a famiglie sconosciute ("unknown" nel grafico) prosegue registrando risultati migliori rispetto a quanto visto nel 2022: se tra il '21 e il '22 la diminuzione è stata di circa la metà, tra il 2022 e il 2023 registriamo una riduzione pari a quasi il 70% del totale. Ciò sottolinea una maggiore capacità di rilevazione da parte dei vendor di tecnologia di sicurezza e degli esperti del settore.

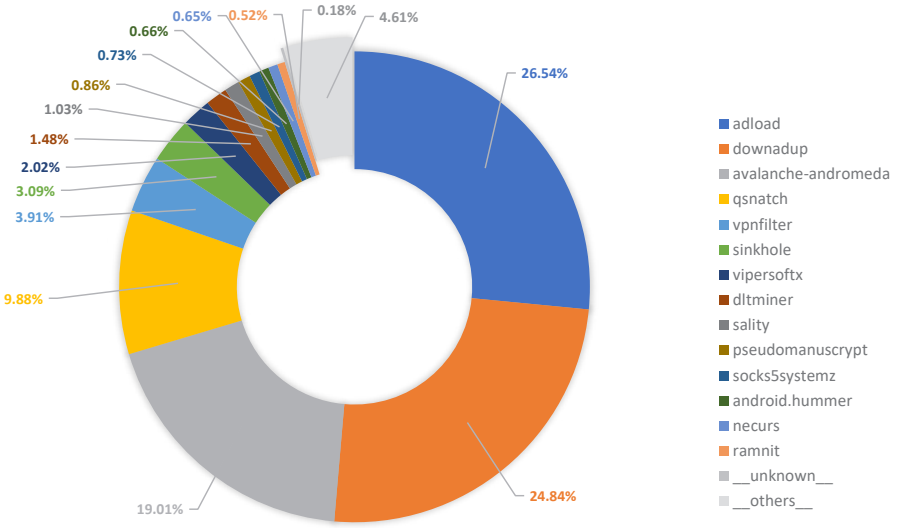


Figura 2 - Analisi delle infezioni rilevate *(Dati Fastweb relativi all'anno 2023)*

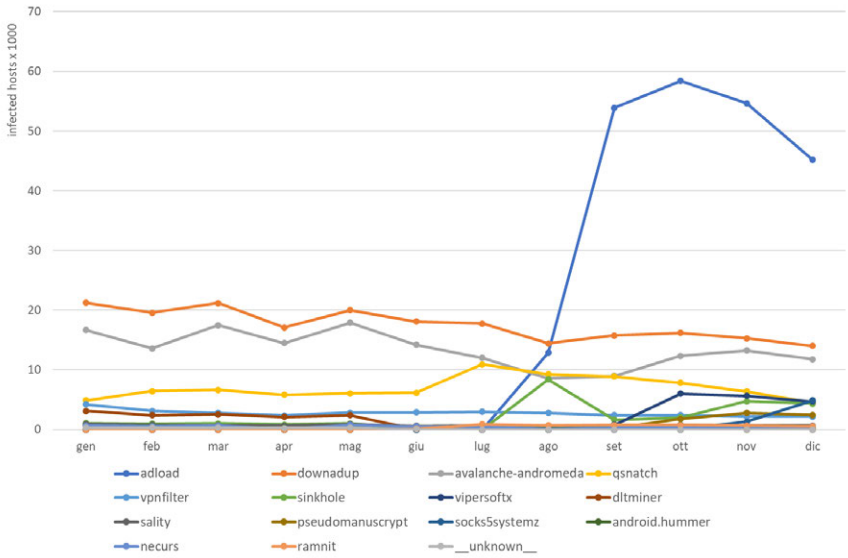


Figura 3 - Rilevazione mensile dei Malware *(Dati Fastweb relativi all'anno 2023)*

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) utilizzate 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 notevole mole di traffico. La logica è quella di rendere inefficaci 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 relativi a server infetti dell'AS di Fastweb si trovavano negli USA, nel 2023 si conferma l'inversione di tendenza che riporta la provenienza di un buon numero di attacchi partiti da server ospitati in Europa. Infatti, rispetto agli anni precedenti, dove gli Stati Uniti erano l'unico paese a registrare una grande concentrazione di data center, gli investimenti in questo ambito si sono moltiplicati anche in Europa. Sono proprio i data center a rappresentare i siti fisici da cui partono gli attacchi centralizzati, con la geografia che è possibile vedere nel grafico seguente.

Da notare come, rispetto al 2022, la distribuzione geografica ha subito una evoluzione rispetto ai dati degli ultimi 3 anni: mentre gli USA mantengono stabilmente il primo posto con il 36% dei C&C totali, al secondo e terzo posto notiamo per la prima volta il Regno Unito (11%) e il Brasile (10%), che nel 2022 non risultavano tra i primi 10 paesi in termine di distribuzione geografica.

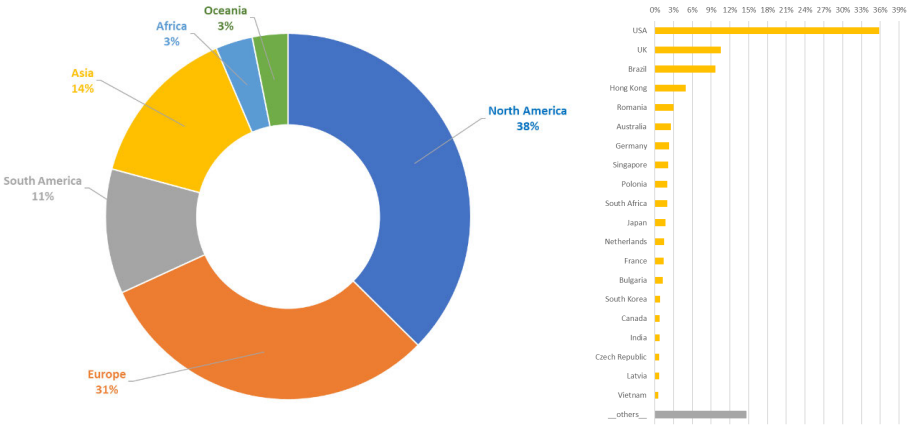


Figura 4 - Dislocazione dei centri di Comando e Controllo *(Dati Fastweb relativi all'anno 2023)*

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 ed il costo del servizio si aggira sui 10-20$ mese per botnet in grado di erogare un attacco di 5-10 minuti ad oltre 100Gbps.

Durante il 2023 sono stati rilevati più di 2.400 eventi di impatto importante e 13.000 anomalie riconducibili a possibili attacchi DDoS diretti verso la rete di Fastweb.

I casi a più alto impatto si registrano in aumento del 32% rispetto al 2022 e si inverte così il trend discendente che è stato osservato negli anni 2021 e 2022, conseguenza dei forti cambiamenti nel mondo del digitale introdotti dalla pandemia. In controtendenza le anomalie a basso impatto che sono diminuite del 40% rispetto al 2022.

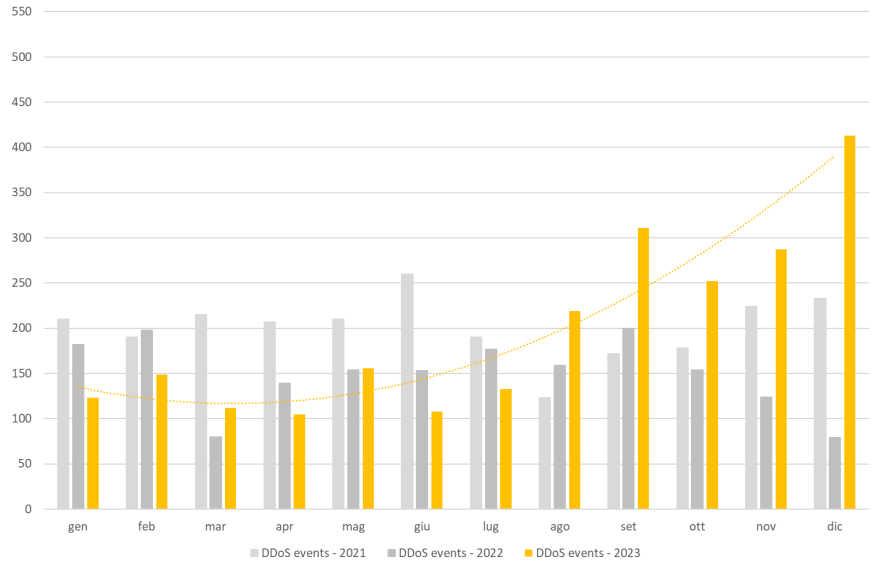


Figura 5 - Distribuzione mensile delle anomalie DDoS *(Dati Fastweb relativi agli anni 2021 - 2023)*

L'incremento del numero di eventi significativi si manifesta nella seconda parte dell'anno ed in particolare l'ultimo trimestre dove l'impatto aggregato mensile di tutti gli attacchi DDoS rilevati e gestiti ha raggiunto livelli mai registrati da Fastweb. Come viene evidenziato nel grafico sotto, a livello di attacchi, misurati attraverso gli aggregati mensili di banda, notiamo un incremento del 72% rispetto al 2022: 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.

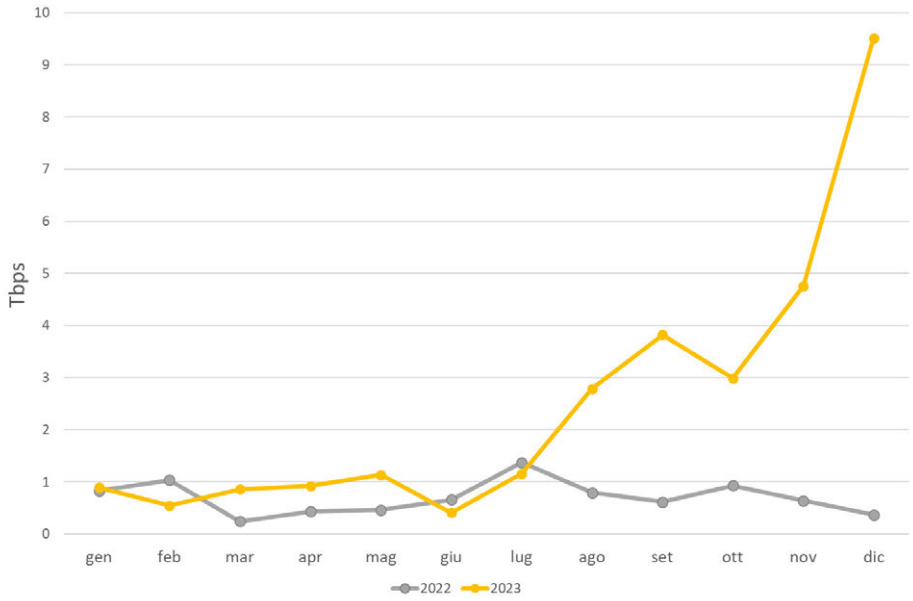


Figura 6 - Distribuzione mensile della banda aggregata degli attacchi DDoS *(Dati Fastweb anni 2022 e 2023)*

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 successivo (**Fig. 7**), il fenomeno riguarda un ampio numero di settori colpiti, tra i quali i più esposti si confermano essere il mondo del Finance/ Insurance e la pubblica amministrazione, che sono obiettivo in oltre il 50% dei casi, valore sostanzialmente stabile rispetto agli ultimi due anni.

Dato interessante riguarda il settore del Gambling, cresciuto dal 1,8% del 2022 a quasi il 12% nel 2023, con un aumento che lo porta al terzo posto. Gli altri settori mantengono la stessa tendenza degli anni precedenti. Si conferma un trend di eventi cyber malevoli che non esclude alcun segmento di mercato

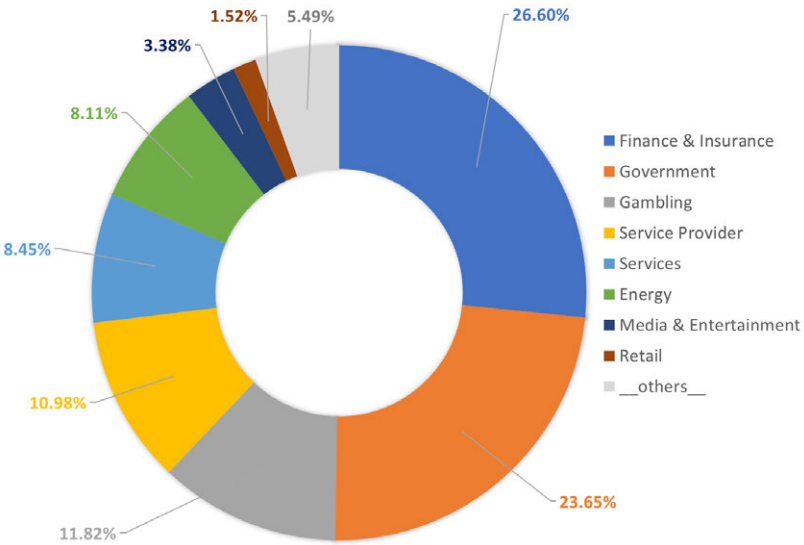


Figura 7 - Segmenti di mercato target di attacchi DDoS volumetrici *(Dati Fastweb relativi all'anno 2023)*

Di seguito viene riportata la distribuzione della banda media in Gbps di un attacco DDoS nel 2023.

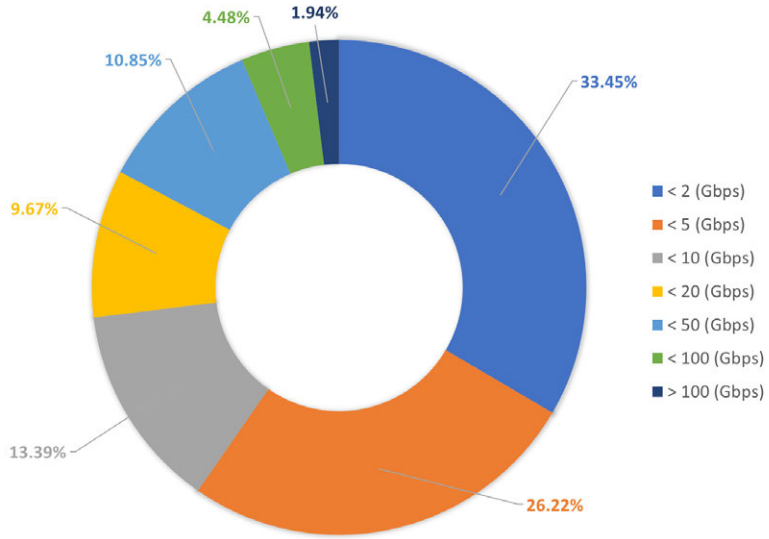


Figura 8 - Distribuzione della dimensione di un attacco DDoS *(Dati Fastweb relativi all'anno 2023)*

Nel corso degli anni, un crescente livello di consapevolezza da parte di aziende e Pubblica Amministrazione in materia di sicurezza informatica, combinato con l'efficacia sempre maggiore delle tecniche difensive, ha determinato una significativa riduzione della durata degli attacchi. Quest'anno, il trend positivo continua, evidenziando come una maggiore consapevolezza da parte delle vittime di attacchi porti a investimenti più consistenti per garantire la protezione dalle minacce di tipo DDos.

Nel 2023 oltre il 93% degli attacchi è durato meno di 1 ora, dato stabile dal 2022. I rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. Nel corso dell'annosono più che raddoppiati gli attacchi che superano le 24h in termini di durata (dal 1,07% al 2,44%) a testimonianza dell'importanza di una protezione adeguata dalle minacce in particolare per le aziende che devono operare in business continuity.

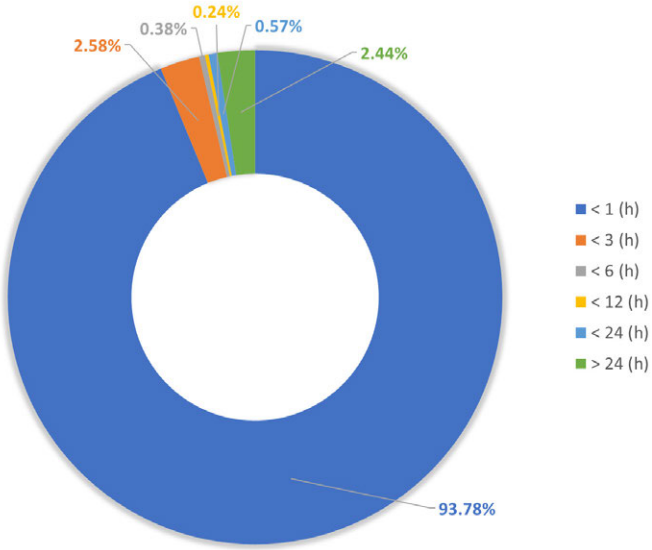


Figura 9 - Durata dei possibili attacchi DDoS *(Dati Fastweb relativi all'anno 2022)*

Nel 2023 le tre principali tipologie di attacco DDoS, si confermano essere "DNS amplification", che ascende considerevolmente dal 29% al 62%, NTP amplification" (dal 29% al 13,8%) e "IP Fragmentation" (dal 3,1% al 2,24%).

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.

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) siano rimasti in prima misura quelli più sfruttati. Gli attacchi diversificati infatti hanno maggiore probabilità di essere efficaci a causa della maggiore complessità e variabilità nel corso dell'attacco per gestire la controparte difensiva.

In tale tipologia di eventi rientrano gli attacchi che variano nel tempo a seconda delle contromisure messe in atto dai nostri 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.

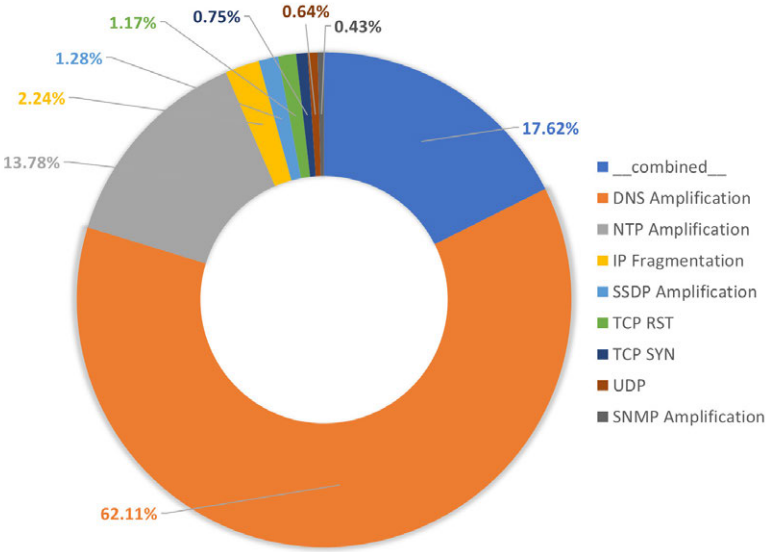


Figura 10 - Tipologie di attacchi DDoS *(Dati Fastweb relativi all'anno 2022)*

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 dunque indicazioni sui volumi delle macchine facilmente attaccabili ed esposte ad elevati rischi di compromissione.

Rispetto al 2022, anno nel quale sono stati rilevati oltre 41.000 server e device che espongono impropriamente protocolli a rischio in rete, nel 2023 registriamo nuovamente una diminuzione pari all'-8% degli apparati esposti (38.000 server e device circa). Il trend discendente continua ormai da diversi anni: -9% nel 2022, -16% nel 2021 e -18% nel 2020. Questa costante diminuzione conferma la consapevolezza e l'attenzione rispetto alle tematiche di sicurezza, che porta le aziende a incrementare progressivamente le linee difensive di base e a porre sempre più attenzione ai servizi esposti, chiudendo quelli critici ed implementando policy adeguate a proteggere gli utenti anche da remoto, garantendo l'accesso sicuro anche in smartworking. L'aumento degli eventi di sicurezza e la relativa diminuzione del numero di infezioni sottolinea un trend positivo per la cybersicurezza, sempre più al centro dell'attenzione delle organizzazioni.

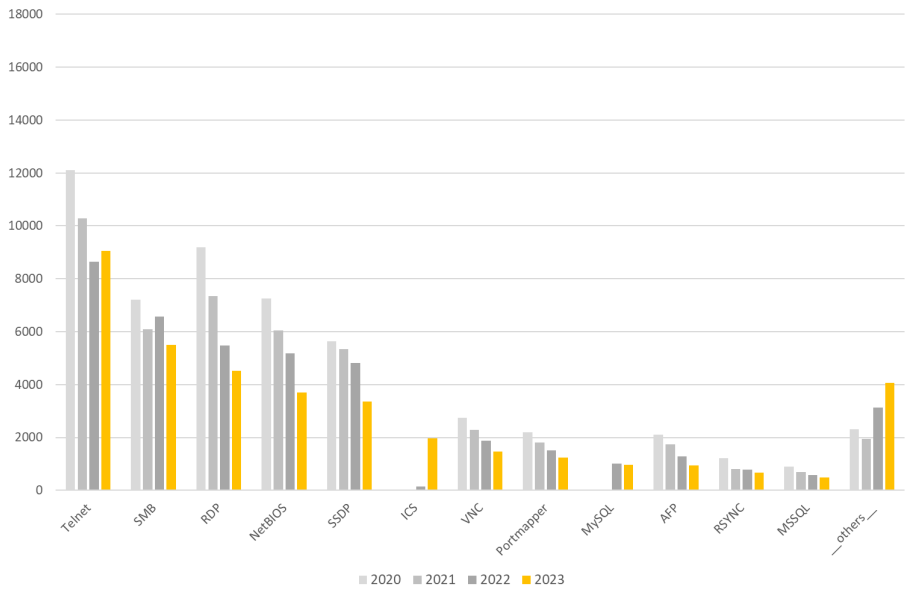


Figura 11 - Servizi critici esposti su Internet *(Dati Fastweb relativi agli anni 2019 - 2023)*

Rispetto al dettaglio dei servizi critici esposti su internet, possiamo notare come lo scenario risulta immutato rispetto al 2022: 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, però, si registra un lieve aumento del 4% rispetto alle rilevazioni del 2022. Se nel '22 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 2023 continua il trend discendente visto negli anni precedenti, con una diminuzione pare al 16%. Rimane al terzo posto l'RDP (-18% rispetto al 2022), utilizzato per la connessione remota ad un PC e che permette di prendere il controllo completo di un apparato se sfruttato dall'esterno.

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 ad 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 2023, le rilevazioni effettuate mostrano che oltre 1.600 IP sono stati inseriti almeno una volta nelle blocklist. Il dato nel 2023 (-51%) è in netto calo rispetto al 2022, dove si erano registrati circa 3.400 azioni di blocklisting. La rilevazione mostra l'inversione di tendenza registrata per la prima volta nel 2022 (con un calo pari al -35%), come evidente dal grafico sotto. Poiché il numero di infezioni generale si mantiene stabile (-2,5% rispetto al 2022) come riportato nel paragrafo "Malware&BotNet", questo fenomeno spiega come i malware siano sempre meno "rumorosi" e compiano azioni più specifiche e mirate.

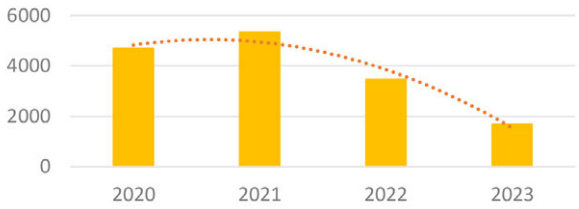


Figura 12 - Quantità di IP in Blocklist dal 2020 al 2023

Un dato rilevante che emerge dal grafico sottostante è relativo alla proporzione lineare che si ha tra il numero di infezioni e il numero di host in blacklist.

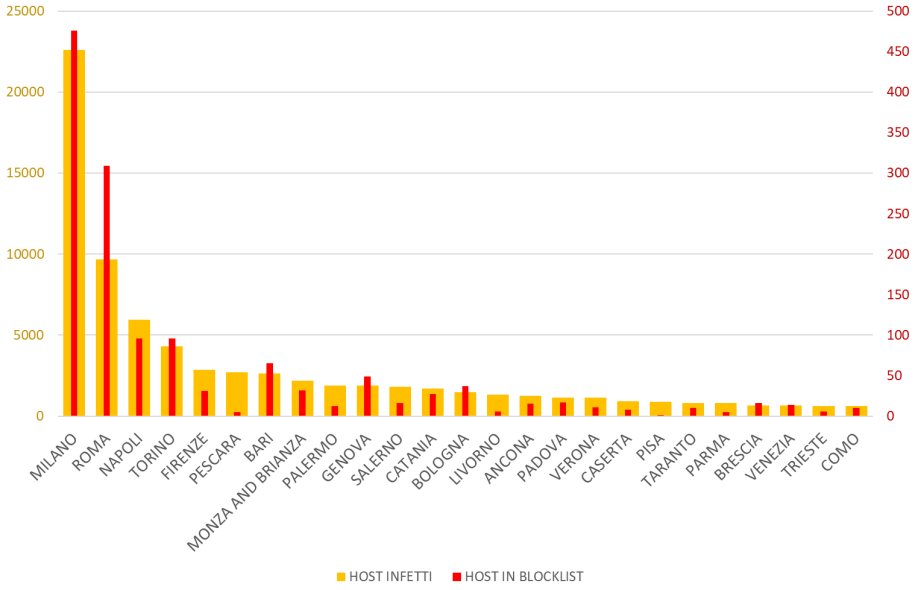


Figura 13 - Relazione tra dispositivi in Blocklist e infezioni rilevate per città *(Dati Fastweb relativi all'anno 2023)*

A livello nazionale le differenze rimangono simili a quanto visto nel 2022, con le regioni del nord Italia in testa con il 55% delle infezioni totali (-8% rispetto al 2022).

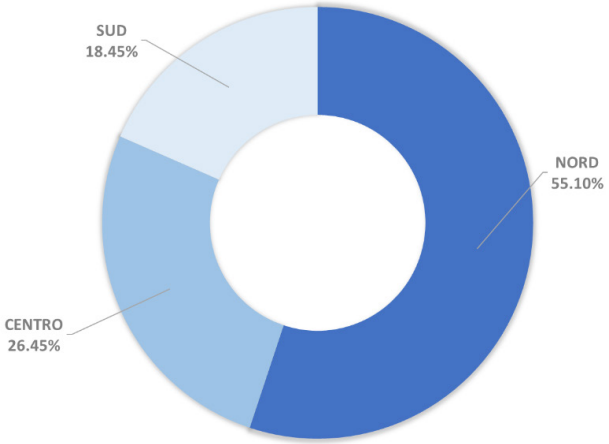


Figura 14 - Distribuzione geografica dei server in blacklist *(Dati Fastweb relativi all'anno 2023)*

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 2023, evidenziano, in continuità con l'anno precedente, la presenza dieventi cyber di tipologia SQL Injection (attacco diretto ad avere accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database) che quest'anno si bilanciano, in termini di quantità, con un incremento di attacchi di tipo Directory Traversal (attacco utile ad avere accesso a file in directory in cui non si è autorizzati ad accedere), OS and Web Server Command Injection Attack e 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). Questi attacchi individuano aree di errata configurazione o codice sviluppato senza un approccio Security by Design.

Nella categoria Denial of Service sono state raccolte quelle tipologie di attacco che hanno il fine di rendere il servizio applicativo indisponibile. Attempts to File Injection rappresenta tutte quelle casistiche in cui l'attaccante prova ad inserire nel sistema file malevoli con l'obiettivo di prenderne il controllo. Infine, in Generic WebApp Attack sono state raggruppate tutte quelle tipologie di attacchi che sfruttano exploit comuni ma non rientrano nelle categorie precedenti.

Nel 2023 le attività legate al cybercrime sono state caratterizzate in maniera importante dalle azioni messe in atto dal gruppo di hacker filorusso NoName057. Questa organizzazione ha condotto una serie di attacchi informatici contro siti istituzionali, governativi e di servizi pubblici europei, rivendicando le sue attività tramite il proprio canale Telegram, esprimendo sostegno alla Russia e criticando la politica estera dei membri della NATO. Le loro azioni hanno coinvolto in modo rilevante anche le aziende ed istituzioni italiane, soprattutto nei mesi di febbraio, marzo, aprile e agosto.

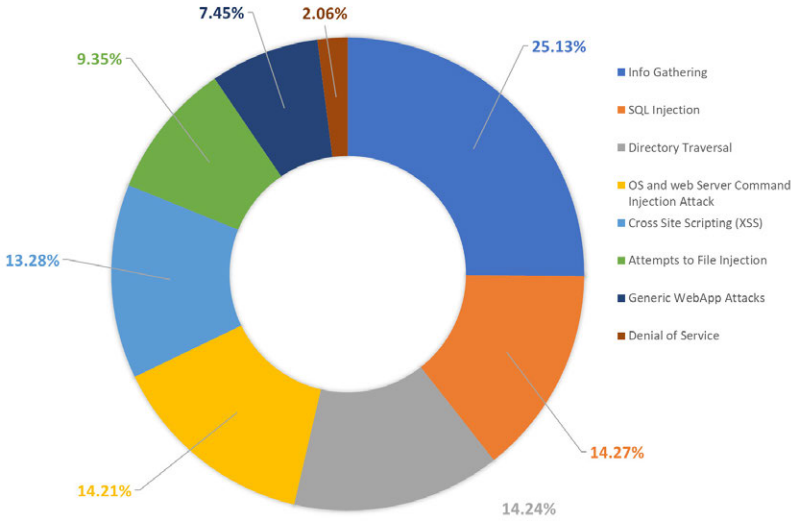


Figura 15 - Tecniche di attacco applicativo rilevate dai WAF del segmento Enterprise *(Dati Fastweb anno 2023)*

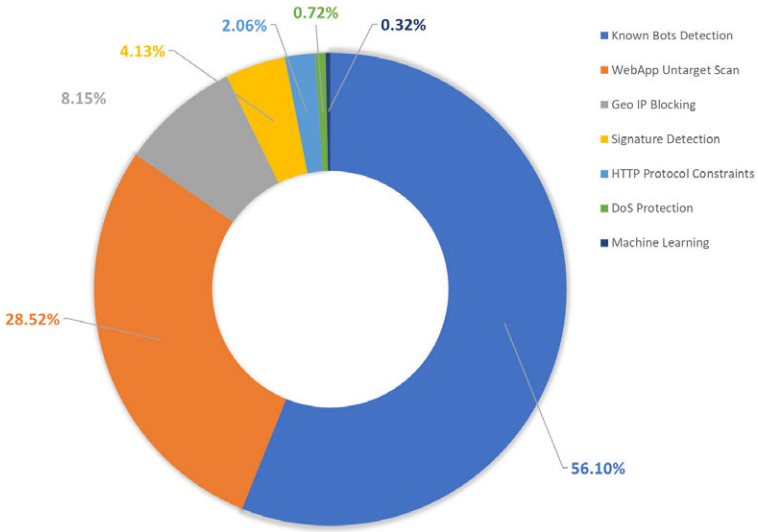


Figura 16 - Tipologie di contromisure maggiormente intervenute a protezione degli attacchi applicativi *(Dati Fastweb relativi all'anno 2023)*

Nel corso del 2023, nonostante il persistere del conflitto tra Russia e Ucraina, si registra una diminuzione degli impatti delle restrizioni geografiche, introdotte per limitare gli accessi dai paesi dell'Est, rispetto all'anno precedente. Tuttavia, si osserva un cambiamento nelle fonti di attacco applicativo identificate dai Web Application Firewall (WAF) e gestite dal Security Operation Center di Fastweb.

Nel 2023 osserviamo un elevato numero di attacchi informatici provenienti dagli Stati Uniti seguiti, come per l'anno precedente, dalla Germania. Al terzo posto la Federazione Russa lascia spazio alla Finlandia che nel corso del 2023 ha incrementato i servizi cloud così anche come riportato dai dati divulgati da Eurostat, a seguire l'Italia, forte dell'apertura di nuove Cloud Regions, e l'Australia che entra per la prima volta in classifica. Rispetto al 2022, pur sparendo alcune aree geografiche, dovute alla restrizione applicate, gli attacchi informatici rimangono sostenuti ed in continua crescita: compaiono i primi blocchi disposti mediante l'uso del IA (Intelligenza Artificiale).

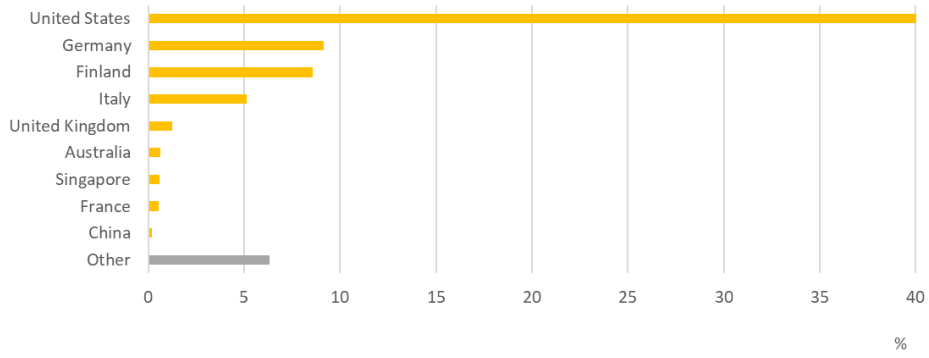


Figura 17 - Dislocazione delle sorgenti di attacco applicativo rilevate dai WAF del segmento Enterprise *(Dati Fastweb relativi all'anno 2023)*

Trend e minacce in ambito Mail

In questa sezione vengono riportati i principali trend del 2023 rilevati da Fastweb nell'ambito Mail Security.

Il vettore principale utilizzato per veicolare attacchi tramite email è rappresentato dall'utilizzo di URL malevoli. Considerando l'andamento annuo, la presenza diretta di allegati malevoli all'interno delle email, appare in crescita (+11% sul 2022). Il dato è apparentemente in controtendenza rispetto al trend delle compromissioni malware

e ransomware (-2,5% infezioni sul 2022). Una spiegazione del fenomeno può essere data dal fatto che la minaccia email, tramite URL, potrebbe condurre l'utente a scaricare file malevoli in una seconda fase dell'attacco.

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

Resta comunque salda, anche se in diminuzione rispetto all'anno precedente, un'importante percentuale relativa alle «Campagne», dove il fattor comune è il tema e/o l'identità dei soggetti da colpire.

Sono in aumento invece le tipologie di minacce, spinte 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 2023

Per quanto riguarda le tipologie di minacce maggiormente veicolate attraverso le email, ad eccezione di Remcos che sfruttando un uso improprio del software di sorveglianza con cui gli attaccanti puntano ad ottenere il controllo da remoto del sistema compromesso, appare predominante la distribuzione delle minacce a quelle forme di codice malevolo che hanno come finalità l'esfiltrazione di informazioni e dati delle vittime (minacce di tipo «info-stealer»).

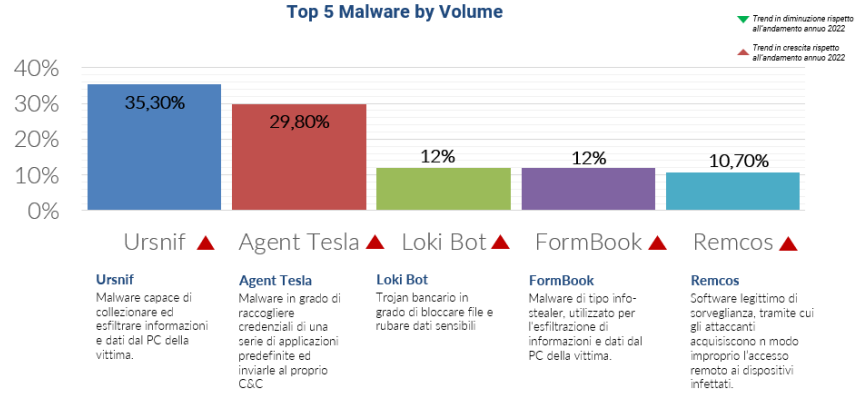


Figura 19 - Top 5 Malware per volume 2023

A livello di tecniche utilizzate dai cybercriminali nel veicolare le minacce via e-mail, sono in deciso aumento le campagne fraudolente che utilizzano le tecniche del social engineering per rendere credibile il raggiro che, solitamente, culmina con perdite economiche anche rilevanti per le aziende prese di mira.

Il social engineering è una tecnica di attacco cyber sempre più sofisticata grazie all'intelligenza artificiale, in grado di colpire direttamente i dipendenti di un'azienda. Questa consiste nel «manipolare» le persone toccando leve psicologiche e comportamentali. Rispetto alle altre modalità di cybercrime, questa pratica si differenzia per una particolarità: il social engineering non sfrutta le falle dei sistemi informatici, bensì il fattore umano.

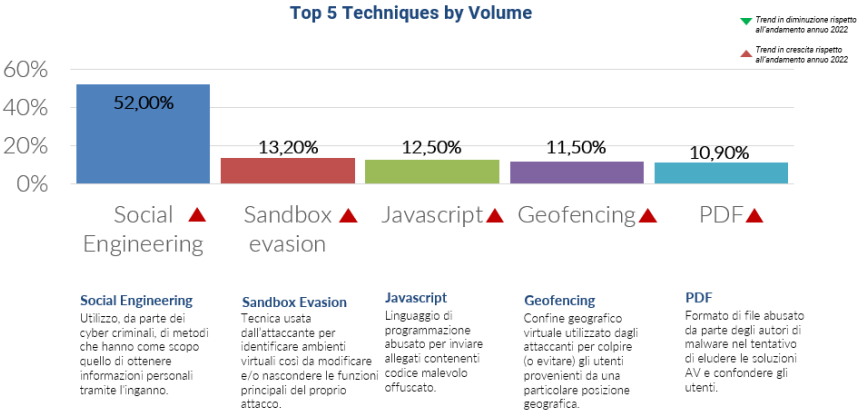


Figura 20 - Top 5 tecniche per volume 2023

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

Il dato sul «Credential Phishing» mostra una crescita importante rispetto all'anno scorso segnando un +87%, una lieve deflessione per i malware generici e quelli orientati all'esfiltrazione di informazioni bancarie, trascurabili invece la crescita per malware di tipo «ransomware» e «RAT».

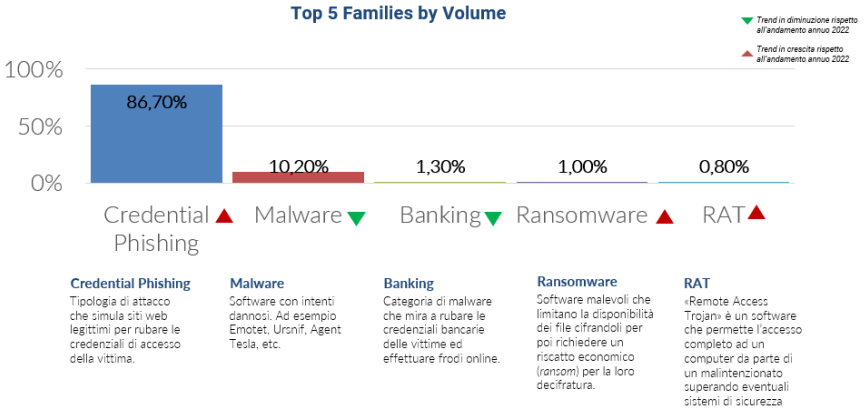


Figura 21 - Top 5 famiglie di minacce per volume 2023

Il team Fastweb CSIRT&SOC, nel corso dell'anno 2023, tramite i sistemi di monitoraggio del presidio e-mail, ha attenzionato un volume di messaggi malevoli afferenti a diversi threat actor. Come è possibileosservare dal grafico sottostante, i principali sono stati:

TA577 (Hive0118)

TA577 è un gruppo di tipo Cyber Crime di possibili origini russe.

Osservato per la prima volta a metà del 2020, questo gruppo ha sviluppato svariati payload di attacco, in particolare si è individuato l'utilizzo di: Qbot, IcedID, SystemBC, SmokeLoader, Ursnif e Cobalt Strike.

In letteratura questo attore è stato associato agli attacchi negli anni passati verso Travelex e Acer tramite il ransomware «Sodinokibi» (aka REvil).

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.

L'avversario ha come target organizzazioni strutturate e si avvale in larga misura di malware bancari già noti. Tra le tecniche sfruttate figurano il phishing e lo spear-phishing incentrato sull'utilizzo di macro ed ingegneria sociale.

Inoltre, il team risulta impegnato in attività di distribuzione di miner per criptovaluta.

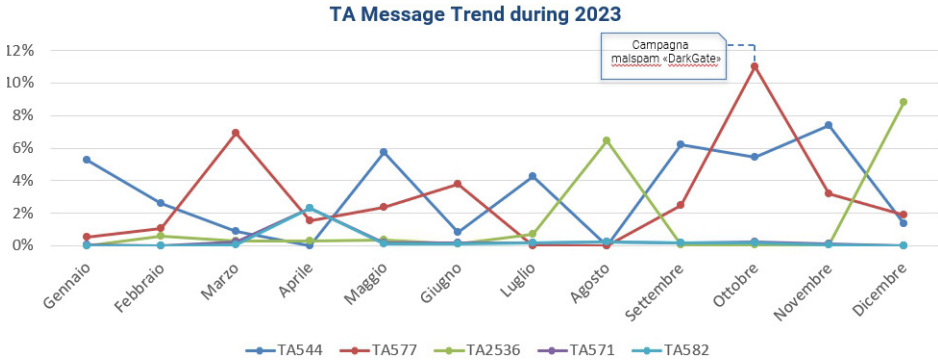


Figura 22 - Threat Actor durante il 2023

Per quanto concerne l'intelligenza artificiale, possiamo notare come l'utilizzo dell'AI abbia impattato sia il lato offensivo che difensivo dell'email 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 ed accorpare dati provenienti da più piattaforme, creando così una profilazione più completa della vittima e permettendo attacchi più mirati. Nel corso del 2023 sono cresciuti gli attacchi di tipo TOAD (Telephone oriented attack delivery). Un attacco TOAD integra tecniche di phishing vocale e via e-mail per indurre gli utenti a divulgare informazioni sensibili. Gli attori, spacciandosi per una persona fidata, effettuano una telefonata ingannevole e successivamente inviano un'e-mail di phishing con un link o un allegato dannoso. L'utilizzo della tecnologia Deepfake aumenta ulteriormente l'autenticità e l'efficacia di questo attacco, consentendo all'aggressore di imitare in modo convincente una figura fidata utilizzando la sua voce in una chiamata o apparendo come lui in una videochiamata.

I numeri in forte crescita legati al social engineering (+13% rispetto al 2022) e, in particolar modo, al credential phishing (+87% rispetto al 2022), ci mostrano come l'utilizzo dell'intelligenza artificiale ha permesso di moltiplicare questa tipologia di attacchi. Il dato più forte, quello rispetto alle tecniche di phishing, è legato non solo agli automatismi permessi dall'AI, ma anche ad una maggiore precisione nell'utilizzo di questi attacchi: grazie alle nuove tecnologie migliora la traduzione delle mail, da sempre principale metodologia per identificare una minaccia di phishing.

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 identificare possibili minacce all'interno degli allegati delle mail e di riconoscere i segni caratteristici degli attacchi di social engineering.

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 2022.

Email Security Offensive	Email Security Defensive
Improved language translation L'utilizzo della Generative AI permette di creare contenuti personalizzati in più lingue, ampliando la superficie d'attacco di Threat Actor internazionali.	**AI backed attachment scanning** L'intelligenza artificiale applicata alla scansione degli allegati potenzia la rilevazione automatica di possibili minacce all'interno dei file inviati via email.
Cross-platform profiling Sfruttando l'AI, gli aggressori riescono a personalizzare ulteriormente i loro attacchi incrociando informazioni da diverse piattaforme, che spaziano dal lavoro alla sfera personale.	**Social Engineering detection** L'AI consente un rilevamento più preciso dei segni caratteristici del social engineering all'interno delle mail.
Deepfake-backed TOAD Gli attacchi TOAD utilizzano una combinazione di phishing telefonico e via email. Questa tipologia di attacco viene resa nettamente più efficace attraverso la tecnologia Deepfake.	**Enhanced actor recognition** Grazie all'intelligenza artificiale gli strumenti hanno la capacità di raccogliere una quantità più ampia di dettagli sui threat actor, distinguendo con maggiore precisione gli individual actors dalle campaigns.

AI Trends in Email Security

Trend e nuovi fenomeni in ambito Frodi

In ambito frodi, il 2023 per Fastweb è stato caratterizzato da due fenomeni principali già osservati:

- frodi da sottoscrizione con furto d'identità
- frodi legate al fenomeno del CLI Spoofing

Le frodi da sottoscrizione con furto d'identità colpiscono cittadini inconsapevoli, che risultano sottoscrittori di contratti, non solo in ambito Telco, a loro insaputa o che scoprono addebiti bancari per servizi mai sottoscritti.

L'identificazione del sottoscrittore con SPID o CIE e con firma digitale con OTP sono misure robuste che riducono le possibilità di azione dei truffatori e tutelano gli utenti e le aziende. Tuttavia, permangono situazioni in cui i truffatori riescono 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.

Un contributo importante al contrasto a questo fenomeno, nel 2023, è arrivato dal sistema Scipafi, che ha integrato e dato accesso a nuovi DataBase delle PA.

Nel 2023 si è osservato un incremento rispetto al 2022, delle frodi da sottoscrizione in cui viene indicato a contratto l'IBAN di un soggetto terzo ignaro. Il metodo di pagamento carta di credito risulta invece più tutelante, grazie all'introduzione della PSD2.

Il fenomeno delle frodi da sottoscrizione è presente sul segmento residenziale e sulle piccole e medie aziende.

Il fenomeno del "CLI spoofing", ossia la manipolazione del numero chiamante per camuffare la reale provenienza della chiamata, continua ad essere ampiamente sfruttato per telemarketing "aggressivo" e per il "robocalling", le chiamate automatiche. La vittima è l'utente che riceve chiamate ingannevoli, che mirano a fargli cambiare operatore fornendo false informazioni, quali l'incremento del canone o disservizi prolungati, nei fatti inesistenti.

Nel corso dell'anno sono stati attuati alcuni interventi, su indicazione dell'Autorità, volti a limitare il fenomeno, che per lo più ha origine fuori dei confini nazionali. Una riduzione del fenomeno è attesa anche dall'applicazione del codice di condotta per i call center, sia nella formulazione del Garante Privacy e sia nella formulazione AGCOM.

Un altro significativo intervento è stato di recente attuato per il contrasto al fenomeno degli SMS ingannevoli, ossia del phishing tramite SMS (smishing). Lo smishing è spesso associato alla falsificazione del mittente, specie se alfanumerico (alias); l'uten-

te che lo riceve viene ingannato perché l'SMS malevolo sembra inviato da un mittente a lui noto, come ad esempio la sua banca. Tali SMS malevoli e ingannevoli spesso sono inviati da soggetti esteri. L'intervento a tutela degli utenti ha quindi previsto il blocco degli SMS con mittente alfanumerico provenienti da estero.

Fastweb registra un calo dei fenomeni legati all'utilizzo fraudolento dei servizi, sia fissi che mobili. In particolare risultano diminuiti i casi di PBX hacking (violazione dei centralini, fisici o virtuali per generare traffico internazionale ad alto costo). Le azioni di prevenzione, il monitoraggio continuo e la rapida reaction in caso di detection di questi casi contrastano questa attività malevola.

Tecniche di attacco e gestione degli Incident

Le rilevazioni derivanti dal servizio di Managed Detection & Response di 7Layers mostrano come le tecniche dei cyber attaccanti sono differenziate tra loro, come si evince dal grafico di **Figura 23**.

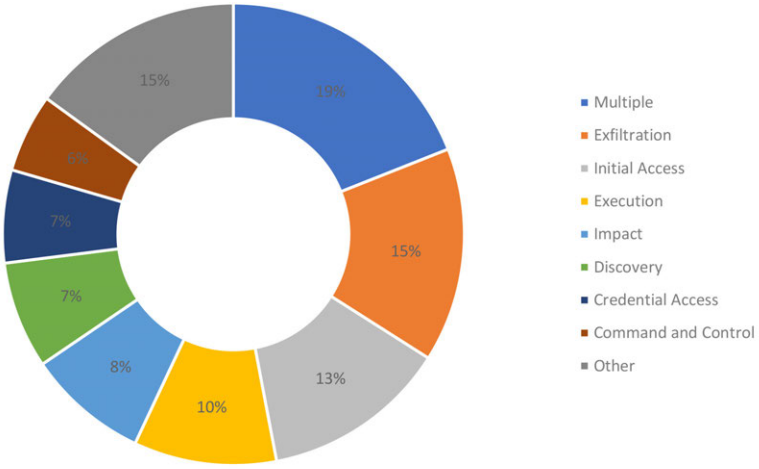


Figura 23 - Tecniche di attacco più comunemente utilizzate sulla base dei dati di agent EDR, Firewall perimetrali, Sonde IDS e Identity Protection

La tipologia più comune è quella degli attacchi "Multiple" (19% del totale), caratterizzati da scenari complessi che coinvolgono una combinazione di diverse tattiche e richiedono un'analisi più approfondita per identificarne i dettagli. Il 15% delle tecniche utilizzate risulta di tipo "Exfiltration", eventi di esfiltrazione di dati sensibili o riservati da un sistema o da una rete al fine di sottrarre informazioni.

Il 13% degli attacchi sfruttano tattiche di tipo "Initial Access", che attraverso una scansione esterna finalizzata a individuare vulnerabilità o punti di ingresso, tentano di penetrare le difese delle aziende; gli eventi di tipo "Discovery" (8% degli attacchi) contribuiscono al processo di scoperta di vulnerabilità e configurazioni deboli durante l'analisi delle fragilità. Eventi ad alto impatto, come ransomware o cryptominer, che possono causare danni molto significativi, contribuiscono al 9% degli attacchi totali.

Queste analisi derivano dalle attività di Incident Response di 7Layers e sono possibili grazie ai dati raccolti da fonti come agent EDR, Firewall perimetrali, sonde IDS e servizi di Identity Protection.

Nel corso del 2023, 7Layers ha registrato un incremento notevole degli eventi monitorati rispetto al 2022. Il servizio MDx, il sistema di gestione dei servizi di security e di risposta agli incident raccolti, ha permesso di registrare un aumento del 260% negli eventi e negli alert gestiti, anche grazie all'ampliamento della superficie di monitoraggio.

L'introduzione dell'intelligenza artificiale nei processi di analisi delle minacce di 7Layers, unitamente ad una più stretta ed efficace collaborazione tra analyst e AI, ha contribuito alla riduzione del 28% degli incidenti analizzati rispetto al 2022. Nonostante questa diminuzione, la quantità di attacchi effettivamente gestiti, testimoniati dai "True Positive", cioè da quegli incident che nascondono attività dannose contro le aziende, è cresciuta del 256% nel 2023. Grazie all'uso dell'AI, quindi, è stato possibile individuare gli eventi realmente impattanti, riducendo sensibilmente il fenomeno dei falsi positivi.

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2023

Il 2023 ha visto la Polizia Postale e delle Comunicazioni porre in campo mirate attività volte a fronteggiare i complessi scenari legati ai crimini informatici.

In particolare l'impegno della Specialità è stato costantemente indirizzato negli ambiti della prevenzione e contrasto alla pedopornografia online, alla protezione delle infrastrutture critiche di rilevanza nazionale, al financial cybercrime e a quelle relative alle minacce eversivo-terroristiche, riconducibili a forme di fondamentalismo religioso e di estremismo politico ideologico, anche in contesti internazionali.

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

I rischi e le opportunità, per i giovanissimi che utilizzano la tecnologia e i nuovi mezzi di comunicazione, sono enormi e noti da tempo.

In questo contesto, il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) si conferma quale fulcro nella lotta alla pedofilia e pornografia minorile online, nonché al contrasto di tutti i fenomeni che coinvolgono i minori, assicurando il ruolo di punto di coordinamento nazionale ed internazionale dei 18 Centri Operativi Sicurezza Cibernetica (COSC) e delle 82 Sezioni Operative Sicurezza Cibernetica (SOSC) della Polizia Postale.

A fronte di un numero complessivo di casi in diminuzione, non sembra ridursi il rischio per bambini e preadolescenti di essere oggetto di attenzioni sessuali da parte di adulti, mentre navigano nel *web*, guardano i loro video preferiti e giocano online. Nell'anno 2023, le denunce relative ai casi di adescamento *online* evidenziano una percentuale di casi riguardanti giovani vittime (9% 0-9 anni), mentre rimane sensibile il dato di quelle tra i 14-16 anni (32%) e significativo quello tra i 10-13 anni (59%).

Si è invece rilevato un incremento dei casi di *sextortion* che negli ultimi anni ha rappresentato una fonte di rischio in particolare per i minori. In passato, infatti, il fenomeno era appannaggio del mondo degli adulti, mentre attualmente coinvolge anche gli adolescenti, in particolare ragazzi tra i 14 e i 17 anni.
Accanto all'azione di contrasto delle diverse fenomenologie significativo è anche l'impegno del C.N.C.P.O. nell'ambito della prevenzione, attraverso la continua e costante attività di monitoraggio della rete, volta a limitare la circolazione di foto e video a sfondo sessuale realizzati con l'utilizzo di minori degli anni 18.

Nel complesso, nel decorso anno sono stati visionati 28.355 siti, di cui 2.739 inseriti in *black list* e inibiti, in quanto presentavano contenuti pedopornografici.
L'attività svolta ha consentito di raggiungere significativi risultati in termini di identificazione di 1.239 soggetti e di effettuare 927 perquisizioni.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	Anno 2023
Persone indagate	1.239
Siti in Black List	2.739

Adescamento online

Nel 2023 si è assistito ad una lieve diminuzione dei casi di adescamento on line e i dati statistici confermano il maggiore coinvolgimento di minori di età compresa tra i 10 e i 13 anni. Infatti, la fascia dei preadolescenti è quella che maggiormente ha avuto interazioni sessuali tecnomediate, 207 rispetto ai 353 casi totali.

Rimangono costanti i casi relativi ai bambini adescati di età inferiore ai 9 anni, *trend* che si sta consolidando in considerazione dell'avvicinamento verso gli strumenti informatici dei bambini più piccoli.

Social network e videogiochi online sono i luoghi ove più spesso avvengono i contatti tra minori e pedofili.

Cyberbullismo

Per quanto concerne il cyberbullismo, si è registrata una diminuzione dei casi dovuta verosimilmente al ritorno ad una vita sociale priva di restrizioni, che ha influenzato positivamente la qualità delle interazioni sociali e delle relazioni tra coetanei. Significativo sul tema è stato l'impegno della Polizia Postale nell'ambito dell'attività di informazione e sensibilizzazione presso le strutture scolastiche, attività che ha contribuito ad innalzare il livello di attenzione degli adulti di riferimento e dei ragazzi sulla necessità di utilizzare la rete in modo corretto e responsabile.
Nel 2023 sono stati trattati 291 casi di cyberbullismo.

CYBERBULLISMO	Totale casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Anno 2023	291	8	72	211

CYBERBULLISMO Minori indagati	Totale
Anno 2023	104

Sextortion

Nell'anno di riferimento, è stato registrato un incremento dei casi di *sextortion* ai danni di minori, che sono passati dai 132 del 2022 ai 137 registrati nel 2023. Il fenomeno, che colpisce anche gli adulti in modo violento e subdolo, fa leva spesso su fragilità tipiche dei ragazzi coinvolti.

Questo fenomeno sta impattando sempre più spesso su vittime minorenni, con effetti lesivi potenziati: la vergogna che i ragazzi provano impedisce loro di chiedere aiuto ai genitori o ai coetanei, di fronte ai quali si sentono colpevoli e imbarazzati per essersi fidati di sconosciuti.

Il senso di intrappolamento che suscita il fenomeno nelle parti offese è amplificato spesso dall'insistente richiesta di denaro da parte dell'estorsore. La maggior parte dei casi riguarda minori di età compresa tra i 14 e i 17 anni, prevalentemente maschi.

SEXTORTION Vittime minori	Totale casi trattati	Casi trattati vittime 0-9 anni	Casi trattati vittime 10-13 anni	Casi trattati vittime 14-17 anni
Anno 2023	137	2	20	115

C.N.C.P.O. – Attività di Polizia Giudiziaria

Si riportano di seguito, le attività investigative di maggior rilievo condotte e/o coordinate dal Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO):

Operazione "Shadow Man" (Maggio 2023). L'unità sotto copertura del Centro Nazionale per il Contrasto alla Pedopornografia Online ha eseguito una custodia cautelare in carcere nei confronti di un cinquantenne, produttore di materiale di pornografia minorile, per anni attivo nella comunità virtuale pedofila *The Love Zone (TLZ)* ove si era distinto per il materiale pedopornografico autoprodotto.
L'operazione trae origine da complesse e lunghe indagini svolte sul Darkweb in collaborazione con Europol e la polizia britannica (*Online CSA Covert Intelligence Team - OCCT*). L'uomo, conosciuto con lo pseudonimo di *Shadow*, per oltre un

decennio era riuscito a eludere le indagini e rimanere anonimo, continuando a realizzare condotte di violenza sessuale aggravata anche ai danni di minori di anni 10. L'utente rappresentava un *high value target* internazionale nell'ambito delle indagini delle polizie di tutto il mondo impegnate in attività sotto copertura online nel contrasto alla pornografia minorile all'interno delle citate comunità pedofile virtuali.

Arresto Bolzano (Maggio/Giugno 2023). Personale della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale e delle Comunicazioni di Bolzano ha eseguito, congiuntamente al personale del CNCPO, che ha avviato l'indagine, la perquisizione nei confronti di un soggetto di nazionalità turca, che aveva inviato a un connazionale immagini pedopornografiche su *Twitter*. L'analisi di tali contenuti ha consentito di rilevare che si trattava di materiale autoprodotto dall'uomo, il quale commetteva abusi sessuali sul figlio infante, documentandoli con video riprese. L'attività si è conclusa con l'esecuzione della misura cautelare in carcere nei confronti dell'indagato.

Operazione "Fast and done" (Agosto 2023). Nel mese di agosto, personale del CNCPO ha dato esecuzione a un decreto di perquisizione per detenzione e diffusione di materiale di pornografia minorile e violenza sessuale su minore emesso dalla Procura della Repubblica presso il tribunale di Roma nei confronti di un 36enne.

L'indagine trae origine da una segnalazione del collaterale australiano relativa a un utente del *Dark Web*, riconducibile al territorio italiano. Dall'incrocio dei dati oggetto di altre segnalazioni ricevute dal CNCPO, nell'ambito della cooperazione internazionale di polizia, sono emersi elementi circa un attuale pericolo concreto di abusi sessuali perpetrati su un minore di anni 10 con autoproduzione e diffusione di materiale di pornografia minorile. Nel corso della perquisizione, richiesta ed eseguita in urgenza, sono stati rinvenuti oltre 20.000 *files* che hanno consentito di procedere all'arresto in flagranza per il reato di produzione, divulgazione e detenzione di ingente quantitativo di materiale pedopornografico e per violenza sessuale aggravata ai danni di un minore.

Operazione "Ciaoamigos" (Settembre 2023). Il CNCPO ha coordinato l'esecuzione di 6 decreti di perquisizione delegati dalla Procura della Repubblica di Salerno nei confronti di soggetti indiziati di detenzione e diffusione di materiale di pornografia minorile. L'indagine, condotta in modalità sotto copertura sul portale *ciaoamigos.it* dal personale della Sezione Operativa per la Sicurezza Cibernetica della Polizia

Postale di Salerno, è scaturita su impulso del C.N.C.P.O., a seguito della segnalazione di un cittadino tramite il *Commissariato di P.S. Online*. L'operazione ha coinvolto, nella fase esecutiva, gli Uffici di Specialità della Campania, Toscana, Calabria e Lombardia.

Operazione "Lucignolo" (Ottobre 2023). Il Centro Operativo per la Sicurezza Cibernetica - Polizia Postale - per il Piemonte e Valle D'Aosta, coordinato dal C.N.C.P.O., ha svolto per diversi mesi un'attività *sotto copertura* su una nota applicazione di messaggistica finalizzata all'individuazione di soggetti dediti alla pubblicazione e divulgazione di materiale realizzato mediante sfruttamento di minori degli anni 18. Oltre 100 investigatori cibernetici della Polizia di Stato sono stati impegnati in tutta Italia nell'esecuzione di 30 perquisizioni delegate dalla Procura della Repubblica di Torino. Gli indagati, con l'utilizzo di accorgimenti tecnici volti al mantenimento dell'anonimato, scambiavano in rete materiale illecito di diversa natura che documentava anche violenze sessuali. I provvedimenti emessi dall'Autorità Giudiziaria procedente hanno consentito di denunciare 30 utenti, indiziati di aver condiviso in rete materiale pedopornografico realizzato utilizzando minori di 18 anni, di cui 3 tratti in arresto in flagranza di reato per detenzione di ingente quantità di materiale.

Operazione "Seven" (Novembre 2023). Gli investigatori del Centro Operativo per la Sicurezza Cibernetica - Polizia Postale - per la Lombardia, dopo oltre un anno di attività investigative condotte in modalità "*sotto copertura*" sulla rete Internet hanno concluso un'indagine grazie alla quale sono stati identificati 29 soggetti che, sfruttando le potenzialità di una nota applicazione di messaggistica, partecipavano a "*canali*" e "*gruppi*" finalizzati alla produzione e alla condivisione di foto e video pedopornografici ritraenti violenze sessuali su minori. Gli abusi, in particolare, riguardavano prevalentemente bambine e bambini in tenera età e, in alcuni casi, neonati. I decreti di perquisizione emessi dalla Procura Distrettuale meneghina e coordinati dal C.N.C.P.O. hanno impegnato più di 150 uomini della Polizia di Stato in oltre 20 province di 9 regioni italiane, consentendo di trarre in arresto 10 soggetti in flagranza di reato per detenzione di ingente quantità di materiale pornografico realizzato mediante l'utilizzo di minori di 18 anni e di denunciarne 16 in stato di libertà, nonché sequestrare numerosi telefonini, tablet, hard disk, pen drive, computer e account di email e profili social. Tra i membri del gruppo è stato possibile distinguere promotori, organizzatori e partecipi, con ruoli e compiti ben definiti, riuscendo a individuare una vera e propria associazione a delinquere finalizzata ad acquisire e diffondere materiale pedopornografico.

Esecuzione di 2 ordinanze di custodia cautelare per Live Distant Child Abuse (Dicembre 2023). Personale del CNCPO, unitamente a quello della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Varese, ha eseguito due misure cautelari nei confronti di un uomo e una donna ritenuti responsabili di aver commesso - dietro corrispettivo in denaro - sessioni *live* di abusi sessuali su minori. Trattasi di un fenomeno denominato *Live Streaming Child Abuse*. L'attività trae origine da un'indagine condotta dal CNCPO e scaturita da una segnalazione di operazioni sospette pervenuta, tramite Guardia di Finanza, dall'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, successivamente confermata da ulteriori informazioni ricevute dalla Polizia Postale dalla *Homeland Security Investigation (HSI)* nell'ambito della cooperazione internazionale di polizia relativa ad un network di soggetti coinvolti nel *Live Streaming Child Abuse*. Gli abusanti, di nazionalità filippina, ricevevano versamenti da account *PayPal* riconducibili a utenti europei per poter assistere a spettacoli video in diretta, aventi ad oggetto abusi sessuali su minori, commissionati sul momento dagli utenti interessati. Tra questi vi era anche un cittadino italiano che, tra il 2019 e il 2020, aveva effettuato pagamenti per acquistare filmati preregistrati e spettacoli in *live streaming* con protagonisti minori. La Polizia Postale di Milano ha effettuato una perquisizione domiciliare e informatica sui dispositivi in uso all'indagato, la cui analisi forense ha consentito di far emergere evidenze probatorie a carico dell'indagato e della moglie di nazionalità filippina, la quale, nel periodo in cui viveva all'estero, faceva parte del citato *network* criminale e offriva a pagamento sessioni di *Live Streaming Child Abuse* in danno dei due figli minori. Ciò ha consentito l'emissione della misura della custodia cautelare in carcere nei confronti dell'uomo, mentre per la moglie, madre di un infante, è stato previsto l'obbligo di presentazione alla polizia giudiziaria e il divieto di espatrio.

Operazione "Viper" (Dicembre 2023). Il CNCPO ha coordinato l'esecuzione, su tutto il territorio nazionale, di 57 decreti di perquisizione delegati dalla Procura della Repubblica di Venezia nei confronti di soggetti indagati nell'ambito del contrasto alla pedopornografia online. L'operazione ha coinvolto gli Uffici di Specialità delle Marche, Puglia, Emilia Romagna, Sardegna, Sicilia orientale e occidentale, Toscana, Liguria, Lombardia, Campania, Umbria, Abruzzo, Calabria, Lazio e Piemonte. L'indagine, condotta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Venezia e coordinata anche sul fronte internazionale dal CNCPO, è scaturita dall'analisi dei dispositivi informatici sequestrati a un precedente indagato, tratto in arresto in flagranza nell'ottobre 2022 per detenzione di ingente quantitativo di materiale pedopornografico. Nel corso della successiva analisi forense, è emerso che il soggetto era molto attivo sulla piattaforma *Viber* ed era iscritto a 42

gruppi e 247 canali dediti allo scambio di materiale realizzato mediante l'utilizzo di minori di 18 anni. I cospicui contenuti multimediali scambiati tra gli utenti, raffiguravano anche torture perpetrate in danno delle piccole vittime. L'attività, condotta in modalità sotto copertura dal personale del COSC Veneto, ha consentito di identificare, oltre a numerosi utenti italiani, anche molteplici stranieri, riconducibili a 44 diversi Stati esteri per i quali il CNCPO ha proceduto ad attivare i canali di cooperazione internazionale di polizia, tramite Europol, Interpol e Ameripol. Le perquisizioni eseguite sul territorio nazionale hanno consentito di arrestare 28 soggetti e di denunciarne 24.

Sezione Operativa

Reati contro la persona

Nel periodo in esame, particolare attenzione è stata rivolta ai fenomeni del *revenge porn*, con 283 casi trattati (di cui 29 in danno di minori), 113 persone denunciate e 2 arrestate, nonché delle truffe romantiche, con 425 casi trattati (di cui 3 in danno di minori), 287 persone denunciate e 8 arrestate. Si ritiene che molti siano i casi che rimangono sommersi e non denunciati in quanto caratterizzati da un coinvolgimento emotivo che provoca nella vittima un forte senso di vergogna nel raccontare quanto accaduto.

Sono stati 31 i casi di *Codice Rosso* che hanno visto la Polizia Postale impegnata attivamente nel contrasto dei reati contro la persona commessi attraverso la rete.

REATI CONTRO LA PERSONA PERPETRATI ONLINE[1]	Anno 2023
Casi trattati	9.538
Persone indagate	1.230
Persone arrestate	19

[1] Stalking / diffamazione online / minacce / revenge porn / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari

Va sottolineato che, con l'entrata in vigore della Legge 24 novembre 2023 nr. 168, sono state introdotte alcune importanti novità nel contrasto alla violenza sulle donne e della violenza domestica e sono stati potenziati alcuni strumenti e procedure per la tutela delle vittime di violenza.

In particolare, detta Legge ha esteso e ampliato la casistica dei reati per i quali poter richiedere l'applicazione dell'*ammonimento del Questore".*

È poi stata introdotta la possibilità, da parte della Polizia giudiziaria, di procedere all'arresto "*in flagranza differita*", strumento previsto per determinate tipologie di reati (*Violazione dei provvedimenti di allontanamento dalla casa familiare, Violazione del divieto di avvicinamento ai luoghi frequentati dalla P.O., Maltrattamenti, Atti persecutori- Stalking*), la cui applicazione ha permesso alla Polizia Postale, nel dicembre 2023, di arrestare l'autore di una serie di azioni delittuose, rubricate come *Stalking,* ai danni di una donna che lo aveva conosciuto in ambito lavorativo. L'impianto normativo ha consentito un significativo impulso alle attività operative e alle attività preventive, volte al contrasto del fenomeno, anche in una fase antecedente alla denuncia di reato. Diverse le giornate dedicate alla formazione dei responsabili di settore degli uffici territoriali per la sensibilizzazione sulle metodologie operative da seguire nella trattazione dei casi.
Infatti, l'uso della violenza, fisica o psicologica, da parte di chi è stato legato alla vittima da una relazione intima, che si manifesta attraverso una serie di atteggiamenti intimidatori e di controllo, volti ad isolarla e indebolirla, rappresenta sempre un campanello d'allarme, che deve essere intercettato il più precocemente possibile.

Significative, inoltre, le campagne di sensibilizzazione in particolare rivolte ai giovani, sulla tematica dei pericoli della condivisione dei contenuti sessualmente espliciti, utilizzando piattaforme *social*, sistemi di messaggistica o *direct message,* tenuto conto che, spesso, molte delle condotte sfociate in gravi episodi sono generate da minacce di divulgazione di foto e video intimi, con una significativa difficoltà di rimozione su internet dovute anche alla scarsa collaborazione di alcuni gestori delle piattaforme o dei siti. Complessa anche la rimozione di contenuti online a causa delle diverse legislazioni di Paesi esteri.
Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti, nonché sono stati svolti servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme di digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).

Da ultimo, si evidenzia l'attività, di assoluta e primaria importanza, rivolta all'individuazione di quelle persone che, attraverso la cassa di risonanza mediatica dei social, hanno manifestato intenti suicidari. Per tali eventi emergenziali vengono attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente.

Sextortion

È un fenomeno pervasivo che di solito colpisce gli adulti facendo leva sulle fragilità personali e sul sentimento di vergogna delle vittime per essere state ingannate da sconosciuti con falsi profili.

Nel corso dell'anno sono stati trattati 1.475 casi di *sextortion* che hanno interessato in particolar modo vittime di maggiore età e prevalentemente di sesso maschile. La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà nel pagare le somme di denaro e nel far richiesta di aiuto a familiari o conoscenti per vergogna.

SEXTORTION	Anno 2023
Casi trattati	1.475
Persone indagate	165
Persone arrestate	3

Attività di rilievo

Identificati e denunciati dalla Polizia Postale gli autori della diffamazione a mezzo internet ai danni della campionessa di nuoto sincronizzato Linda Cerruti (gennaio 2023).

Al rientro da una straordinaria prestazione atletica agli europei di nuoto sincronizzato che l'aveva portata a vincere otto medaglie, la campionessa Linda Cerruti aveva pubblicato sui social una foto in cui compariva in costume da bagno, in una classica posa del nuoto sincronizzato, esibendo le medaglie.

La foto, scattata sul molo di Noli (SV), città natale della campionessa, era stata ripresa da molte testate giornalistiche e aveva attirato numerosissimi commenti, alcuni dei quali palesemente diffamatori e sessisti che l'atleta, amareggiata, aveva deciso di denunciare rivolgendosi alla Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Savona.

Le indagini, condotte anche dagli esperti del Centro Operativo per la Sicurezza Cibernetica di Genova e coordinate dalla Procura della Repubblica di Savona, con il supporto del Servizio Polizia Postale di Roma, hanno permesso di identificare 12 utenti della rete, ritenuti autori dei commenti diffamatori più condivisi.

Con la partecipazione dei Centri Operativi per la Sicurezza Cibernetica della Polizia Postale della Lombardia, Piemonte, Emilia Romagna, Friuli Venezia Giulia, Veneto, Lazio, Umbria e Sardegna, sei soggetti sono stati destinatari di una perquisizione informatica, delegata dalla Procura della Repubblica di Savona, mentre gli altri sei sono stati convocati presso i Centri Operativi della propria città per rispondere del reato di diffamazione aggravata.

La Polizia di Stato arresta 8 persone responsabili di truffe romantiche. Identificate 32 vittime. Oltre 400mila euro sottratti (marzo 2023).
Il Centro Operativo per la Sicurezza Cibernetica Lazio ha arrestato otto persone, in esecuzione di una ordinanza applicativa di misure cautelari emessa dal G.I.P. di Roma per truffa aggravata, riciclaggio e sostituzione di persona.
Le indagini della Polizia Postale coordinate dalla Procura della Repubblica di Roma hanno avuto l'obiettivo di contrastare il sempre più diffuso fenomeno delle cd. "*truffe romantiche*", reati contro il patrimonio commessi in danno di persone fragili che i criminali ricercano e individuano sui social network, portando poi a termine il progetto criminale e la truffa sfruttando le debolezze e le vulnerabilità delle vittime.
I criminali utilizzano profili social *fake* spesso presentandosi come personaggi affascinanti e rassicuranti, con l'obiettivo di instaurare un rapporto con le vittime fino ad indurle a credere ad una relazione sentimentale.
Guadagnata la fiducia e la confidenza, i criminali fanno richieste di denaro, utilizzando le scuse più disparate; la vittima, imprigionata in una relazione a distanza, fatica a rendersi conto e spesso ad accettare di essere vittima di una truffa.
Nello specifico caso, l'indagine è stata avviata a seguito della denuncia di una signora contattata su Facebook da "Larry Brooks", sedicente ufficiale dell'esercito statunitense in missione in Siria, con la foto profilo raffigurante un affascinante uomo di mezza età. Tra i due si veniva ad instaurare una vera e propria relazione sentimentale tanto che la vittima, credendo alla promessa di un futuro insieme, veniva indotta ad effettuare diversi bonifici per consentire all'uomo di far fronte alle difficoltà economiche che gli impedivano di congedarsi e giungere finalmente in Italia.
I primi accertamenti hanno confermato i sospetti della falsità del profilo e, quindi, della truffa perpetrata dal sedicente ufficiale; nel corso delle indagini emergevano ben 32 vittime accertate con un provento illecito di circa 400.000 euro nel periodo dal 2018 al 2021.

La lunga e complessa attività investigativa è stata condotta affiancando tecniche classiche di investigazione ad attività di analisi del traffico delle comunicazioni internet e dei flussi finanziari ed ha consentito di identificare nel Lazio gli odierni indagati.

Sui conti correnti riferibili al gruppo criminale si accertava il transito di somme di denaro provento delle truffe, inviate direttamente dalle vittime, per poi essere incassate, o trasferite su conti nelle disponibilità degli indagati, in molti casi con rimesse di denaro all'estero, per la condivisione dei relativi proventi.
In relazione al quadro indiziario emerso, la Procura della Repubblica di Roma ha contestato il concorso in truffa, aggravata dall'aver approfittato delle condizioni di minorata difesa delle vittime e dalla transnazionalità del reato, nonché il reato di riciclaggio dei proventi del reato.
Agli indagati è stato contestato anche il reato di sostituzione di persona; infatti il nominato "Larry Brooks" risultava persona realmente esistente negli USA e la foto utilizzata nei profili falsi risultava essere di un avvocato statunitense che in relazione alle condotte descritte ed infamanti presentava denuncia alle autorità statunitensi.

"Sei arruolato, vieni a prendere le misure per la divisa" (marzo 2023).
Il Centro Operativo per la Sicurezza Cibernetica di Roma ha denunciato per il reato di sostituzione di persona e detenzione abusiva d'armi un uomo di Frascati, di 54 anni, indiziato per aver raggirato un giovane disoccupato, promettendogli un posto di lavoro e per aver gettato discredito sulla Gendarmeria Vaticana.
L'indiziato, venuto a conoscenza delle aspirazioni del giovane disoccupato, si presentava falsamente come Ufficiale dell'Arma dei Carabinieri e millantando rapporti privilegiati con la Gendarmeria Vaticana, si proponeva quale intermediario per l'assunzione del giovane nel Corpo della Gendarmeria.
Il predetto si convinceva a versare una somma di denaro in cambio del fattivo interessamento; seguiva un fitto scambio di mail fasulle con la Gendarmeria Vaticana per trarre in inganno la vittima del reato, con l'invio anche di finti test selettivi di ingresso. La vittima, convinta del buon esito delle selezioni, si presentava personalmente presso gli uffici della Gendarmeria Vaticana, scoprendo di essere stata vittima di un truffatore.
La Gendarmeria Vaticana, denunciava i fatti al Centro Operativo per la Sicurezza Cibernetica Lazio, che avviava tempestivamente le indagini, coordinate dalla Procura della Repubblica di Roma, che consentivano, attraverso l'esame delle evidenze informatiche, di individuare e denunciare il sospetto autore.
Su delega della Procura si procedeva ad effettuare perquisizione locale e personale del soggetto indagato e si rinveniva e si sequestrava il *device* e il materiale predisposto per simulare l'appartenenza ad un corpo di polizia, in particolare due pistole replica senza il previsto tappo rosso di sicurezza e due portatessere con placche metalliche riconducibili all'agenzia governativa americana FBI.

Associazione a delinquere finalizzata alla truffa e al riciclaggio: il Centro Operativo per la Sicurezza Cibernetica Umbria dà esecuzione a 18 decreti di perquisizione (maggio 2023).

Personale della Specialità, coordinato dalla Procura della Repubblica presso il Tribunale di Spoleto, ha dato esecuzione a 18 decreti di perquisizione nei confronti di persone, operative su tutto il territorio nazionale, indagate per i reati di truffa, ricettazione e riciclaggio.

Le complesse indagini, avviate a seguito della presentazione di numerose querele da parte delle vittime di truffe "romantiche" e di altri reati hanno consentito di delineare una rete criminale articolata su due livelli:

il primo, fortemente gerarchizzato e prevalentemente radicalizzato nei paesi dell'Africa centro occidentale, si occupava di creare falsi profili al fine di adescare ignare vittime; il secondo, invece, costituito da decine di persone deputate al riciclaggio del denaro fraudolentemente ottenuto, aveva l'incarico di mettere a disposizione i propri conti ovvero di reclutare persone disposte a fornire, talvolta inconsapevolmente, il proprio conto corrente per far confluire le transazioni illecite in cambio di una percentuale già stabilita dal gruppo criminale.

Gli indagati, situati capillarmente sull'intero territorio nazionale, sono stati in grado di raggiungere vittime in svariati paesi europei ed extraeuropei. In particolare, una volta ottenuto il contatto con le potenziali vittime su uno dei numerosi social network, le stesse venivano coinvolte in un legame affettivo virtuale tale da convincerle a versare spontaneamente somme di denaro. In caso di rifiuto, gli indagati minacciavano le vittime della pubblicazione di foto e video "intimi" o conseguenze legali per dei supposti comportamenti illeciti della vittima.

Successivamente, i proventi così ottenuti venivano smistati su diversi conti correnti ed utilizzati per l'acquisto di beni di varia natura: automobili, materiale edile, condizionatori ecc., che venivano poi spediti verso la Nigeria all'interno di alcuni *container*.

Le indagini informatiche eseguite su alcuni apparati mobili a disposizione degli indagati hanno consentito di accertare dell'esistenza di veri e propri gruppi su social network, creati con utenze straniere, per mantenersi in contatto e con lo scopo di gestire le vittime e di riciclare il denaro.

L'incisivo impulso della magistratura nell'attività di indagine effettuata nei confronti dei compartecipi ubicati in diversi Paesi UE – extra UE e il decisivo intervento del Servizio Polizia Postale e delle Comunicazioni, anche tramite l'attivazione dei canali di cooperazione internazionale (Europol/Interpol), hanno permesso di scoprire un giro d'affari di oltre un milione di euro in due anni.

Altrettanto preziosa è stata la collaborazione di Poste Italiane S.p.A. e di altri istituti di credito, che hanno, in tempi brevi, fornito i riscontri necessari per individuare la catena di trasferimenti di denaro originata dalle attività illecite compiute dalla struttura malavitosa.
Le indagini svolte dal Centro Operativo per la Sicurezza Cibernetica Umbria hanno portato all'individuazione e consequenziale esecuzione di 18 perquisizioni, coordinate dal Servizio Centrale di Polizia Postale e delle Comunicazioni e la collaborazione dei Centri Operativi della Campania, Emilia Romagna, Lazio, Liguria, Marche, Sicilia e Veneto, nelle province di Modena, Padova, Genova, Pesaro, Latina, Caserta, Campobasso, Palermo ed il concorso del Reparto Prevenzione Crimine Veneto coinvolto dalla Direzione Centrale Anticrimine.

Estorsioni in Rete: utenti di siti di incontri minacciati e costretti a pagare da sedicenti sfruttatori. La Procura della Repubblica di Perugia emette sei decreti di perquisizione (giugno 2023).
Personale della specialità ha eseguito 6 decreti di perquisizione personale, locale ed informatica, emessi dalla procura di Perugia nei confronti di altrettanti cittadini di nazionalità straniera, ma residenti in Italia, indagati per i reati di estorsione e minacce in danno di alcuni utenti di siti di incontro.
L'attività di indagine, effettuata dal Centro Operativo per la Sicurezza Cibernetica – Polizia Postale – Umbria, unitamente alla Squadra Mobile della Questura di Perugia, è stata avviata a seguito della denuncia di un uomo che, dopo aver contattato delle ragazze su un sito di incontri, è stato minacciato da ignoti soggetti ed indotto al pagamento di diverse somme per un importo complessivo superiore a 3000 euro.
Dagli approfondimenti investigativi è emerso che il "*modus operandi*" usato dagli autori delle minacce - operanti sull'intero territorio nazionale, è sempre stato lo stesso: dopo essersi presentati come "gestori" di alcune ragazze presenti sui siti d'incontri, hanno inviato ai fruitori, tramite applicazioni di messaggistica istantanea, una serie di minacce consistenti nella richiesta di pagamenti come mancato introito per i servizi resi online. Gli investigatori della Squadra Mobile e della Polizia Postale perugina, dall'incrocio dei dati dei tabulati telefonici e file di log, hanno individuato i profili di 6 soggetti destinatari di provvedimenti di perquisizione locale, personale ed informatica congiuntamente eseguiti con il sequestro di numerosi supporti informatici.

Ordinanza di custodia cautelare nei confronti di un giovane 19enne in relazione al reato di atti persecutori (ottobre 2023).
La Sezione Operativa per la Sicurezza Cibernetica di Foggia ha dato esecuzione ad un'ordinanza di custodia cautelare degli arresti domiciliari con braccialetto elettro-

nico, emessa dal Gip presso il Tribunale di Foggia, su proposta della locale Procura della Repubblica, nei confronti di un giovane 19enne, sottoposto alle indagini preliminari in relazione al reato di atti persecutori.
L'attività d'indagine aveva inizio dalla querela presentata da una giovane donna, che lamentava un grave stato di ansia e timore per la propria incolumità, con conseguente destabilizzante turbamento psicologico, dovuto alle reiterate minacce e molestie, poste in essere dal soggetto, che sentendosi rifiutato sentimentalmente, ha posto in essere le condotte illecite.

Esecuzione della misura cautelare del divieto di avvicinamento nei confronti del marito (novembre 2023).
La Procura Distrettuale di Catania ha delegato il Centro Operativo per la Sicurezza Cibernetica di Catania all'esecuzione di una misura cautelare di divieto di avvicinamento ed installazione del cosiddetto "braccialetto elettronico", emessa dal GIP del Tribunale nei confronti di un uomo di anni 39, residente a Catania, ritenuto responsabile dei delitti di atti persecutori aggravati. La vicenda trae origine da una segnalazione via *e-mail* al citato Centro Operativo, in cui un utente riferiva che, mentre era in attesa in una sala di un nosocomio catanese, aveva dato in uso il suo telefono ad un uomo che, essendone momentaneamente privo, aveva urgente necessità di chiamare la moglie.
Nel corso di quella telefonata, il segnalante aveva udito delle frasi minacciose rivolte dall'uomo all'interlocutore. Le indagini, da subito avviate, hanno permesso di identificare una donna come titolare dell'utenza telefonica formulata. Gli operatori accertavano che la donna, madre di minori, era vittima di minacce e molestie reiterate dopo la separazione ad opera del marito con innumerevoli telefonate e messaggi. Le risultanze investigative acquisite dalla Polizia Postale consentivano al Pubblico ministero di richiedere ed ottenere una misura cautelare nei confronti dell'indagato.

Atti persecutori e revenge porn nei confronti di una donna italiana residente in Germania. La Polizia di Stato denuncia un cittadino fiorentino (dicembre 2023).
Gli investigatori del Centro Operativo per la Sicurezza Cibernetica di Firenze, coordinati dalla locale Procura della Repubblica, hanno denunciato in stato di libertà un fiorentino, che si è reso responsabile di atti persecutori e *revenge porn* nei confronti di una donna italiana residente all'estero.
Le indagini sono state avviate a seguito di una segnalazione telefonica al citato COSC, con cui la donna, in evidente stato di agitazione ed in lacrime, ha raccontato di essere vittima di atti persecutori da parte di un conoscente, residente a Firenze, con il quale, l'anno precedente, aveva intrattenuto una relazione sentimentale.
Nel giro di pochi giorni, dopo una costante e minacciosa insistenza, l'uomo - che non

ha mai accettato la fine della relazione - aveva addirittura inviato, via mail, al marito della donna, varie foto ed un video sessualmente esplicito, prodotti durante i loro incontri, prospettando l'intenzione di mandare tutto anche ai suoi figli.
Inoltre, lo *stalker* aveva minacciato di raggiungere la donna all'estero, conoscendone l'indirizzo di residenza, se quest'ultima non avesse lasciato il marito e non l'avesse raggiunto a Firenze per una futura convivenza.
La persona offesa, grazie ad un tempestivo intervento degli operatori della Polizia Postale, veniva invitata a presentare denuncia per l'attivazione della procedura di urgenza prevista dal cd. "*Codice Rosso*".
La rapidità di intervento assicurata alla vittima e la tempestiva collaborazione del Consolato operante, che ha subito trasmesso la querela sporta dalla donna, hanno permesso di avviare immediati accertamenti di polizia giudiziaria da parte della Polizia postale, grazie ai quali il responsabile è stato tempestivamente identificato e reso destinatario di un decreto di perquisizione eseguito dal Centro operativo per la Sicurezza Cibernetica della Polizia Postale per la Toscana. L'attività di perquisizione consentiva di rinvenire nella disponibilità dell'indagato le immagini e il video sessualmente espliciti inviati al marito della vittima, nonché le *chat* e le *email* indicate nella querela, con conseguente sequestro di tutti i dispositivi informatici, delle utenze telefoniche e degli *account* in uso all'indagato.

Arresto in flagranza differita per stalking di un romano di 31 anni. Determinante la recente modifica normativa al "codice rosso" (dicembre 2023).
Il Centro Operativo per la Sicurezza Cibernetica di Roma ha arrestato in flagranza differita un cittadino romano di 31 anni, gravemente indiziato per il compimento di numerosi atti persecutori commessi negli ultimi due mesi nei confronti di una ex collega di lavoro.
L'attività è stata avviata a seguito della denuncia sporta dalla giovane vittima, dipendente di una importante società multinazionale di consulenza, per una serie di episodi allarmanti.
Ad un primo recapito presso la propria abitazione di un mazzo di fiori da parte di un ammiratore sconosciuto, erano seguite infatti condotte che avevano ingenerato in lei uno stato di profonda agitazione, tanto da indurla a cambiare le proprie abitudini di vita e pensare di rivolgersi ai servizi sociosanitari per un'assistenza psicologica.
Riceveva infatti sulla mail aziendale una e-mail anonima con allegata una sua foto tratta dal profilo Instagram della donna. In seguito, scopriva che a suo nome, senza il suo consenso, erano stati effettuati alcuni tentativi di acquisti *e-commerce* ed erano stati attivati una serie di servizi on line, fra i quali registrazioni su siti web pornografici o di incontri a sfondo sessuale.

L'allarme generato da tali episodi si dimostrava fondato con la ricezione di due mail con gravi minacce.
Tutti gli accertamenti investigativi condotti dal personale del C.O.S.C. Lazio non consentivano inizialmente di identificare il reale autore di tali comportamenti, che dimostrava una notevole abilità nel cancellare le proprie tracce informatiche. I collegamenti internet infatti erano stati effettuati con l'utilizzo di tecniche informatiche di anonimizzazione e gli acquisti online erano stati realizzati con pagamenti esteri. La svolta delle indagini avveniva alla Vigilia di Capodanno, quando la donna denunciava un episodio analogo a quello iniziale, ovvero l'acquisto su di un noto portale online di un anello in oro e brillanti di notevole valore fattole recapitare alla propria abitazione la sera del 28 dicembre.
Gli accertamenti effettuati tempestivamente consentivano di identificare un giovane romano di 31 anni, ex collega della vittima con precedenti penali per violenza e già condannato per detenzione abusiva di armi.
Sulla scorta di quanto emerso, in considerazione del profilo criminale dell'autore, veniva richiesto di urgenza un decreto di perquisizione anche informatica che, tempestivamente emesso dall'Autorità procedente della locale Procura di Roma, veniva eseguito con esito positivo. Il predetto pertanto veniva tratto in arresto in flagranza differita, grazie alle prove raccolte sull'ultimo atto persecutorio denunciato, consumato nelle precedenti 48 ore dall'intervento degli investigatori e cristallizzato con l'acquisizione delle tracce informatiche rimaste sul telefono cellulare del ragazzo, relative all'acquisto dell'anello, nonché delle pregresse minacce.

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

Nell'esercizio delle proprie competenze istituzionali, il Servizio Polizia Postale e delle Comunicazioni, quale Organo del Ministero dell'Interno per la sicurezza delle telecomunicazioni si avvale del Centro Nazionale Anticrimine Informatico per la Protezione Infrastrutture Critiche (CNAIPIC), quale Centro d'eccellenza, per garantire ed assicurare la protezione continuativa delle infrastrutture critiche.

L'azione preventiva e cautelativa svolta quotidianamente dal CNAIPIC, in regime continuativo, si dispiega attraverso la condivisione - con tutti gli attori istituzionali che animano l'ecosistema della cybersicurezza nazionale - delle evidenze informative e delle criticità, raccolte nell'ambito della sua attività di monitoraggio.

Anche nel corso dell'anno appena trascorso, l'attività di polizia svolta dal CNAIPIC si è articolata attraverso la diffusione di dedicati *alert*, correlati dagli indicatori di com-

promissione e dagli avvisi tecnici di informazione di sicurezza, che permettono alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali, nonché ai potenziali target di azioni ostili l'adeguamento e la salvaguardia della propria rete informatica, in modo da renderla resistente agli attacchi.

Quest'attività è perseguita mediante il dispiegamento dell'intera rete di sicurezza, che in maniera capillare abbraccia la struttura centrale e le diramazioni territoriali più vicine e prossime agli obiettivi da proteggere.

In tal senso, il CNAIPIC ha stimolato ulteriormente l'opera di sensibilizzazione dei propri Centri Operativi per la Sicurezza Cibernetica (COSC) al fine di mantenere un'attenzione particolareggiata ai fenomeni criminali cibernetici, mediante il continuativo coinvolgimento dei Nuclei Operativi di Sicurezza Cibernetica (NOSC), nell'azione di assicurazione e mantenimento di dedicati servizi di monitoraggio e analisi.

Il dato statistico - corroborato dalle analisi di settore svolte - ha confermato un aumento esponenziale del numero di attacchi informatici, diretti a paralizzare, bloccare o in genere creare nocumento ai sistemi informatici e alle reti telematiche delle infrastrutture critiche. Si tratta delle realtà strategiche del Paese, di carattere pubblico o privato, deputate all'erogazione dei servizi essenziali e allo svolgimento dei compiti più importanti a favore della collettività.

Tali azioni malevole costituiscono sempre più spesso eventi terminali di attività ostili ancor più complesse e strutturate, pervasive e silenti, finalizzate all'intrusione nei domini strategici di questi Enti, per permettere ai soggetti attaccanti l'acquisizione e l'esfiltrazione di informazioni sensibili.

La finalità che anima gli attaccanti nell'esecuzione di queste operazioni va rintracciata principalmente in un'attività criminosa, c.d. cybercrime, analoga a quella tradizionale, ma caratterizzata dall'abuso di componenti tecnologiche informatiche da parte di vere e proprie associazioni a delinquere, che vanno sempre più strutturandosi al loro interno in vari sottogruppi, che hanno la funzione di coordinarne le attività, nonché di determinare gli obiettivi strategici e tattici verso cui indirizzare l'azione ostile.

In questo contesto, l'enorme mole di informazioni captate (contenute all'interno dei sistemi attaccati di queste realtà) è suscettibile di proficuo ed immediato reimpiego, sia quale oggetto di scambio nei mercati neri del *darkweb* ovvero quale mezzo per la realizzazione di massive campagne estorsive a livello globale.

È proprio la presa di coscienza della transnazionalità intrinseca del crimine informatico che richiede la necessaria attivazione di canali di cooperazione internazionale. Il

risultato diretto, tangibile di questo sforzo si compendia in un rilevato aumento delle richieste di cooperazione in ambito internazionale, ricollegate anche al ruolo sempre più proattivo e strutturato del CNAIPIC quale punto di Contatto nazionale della rete HTC 24/7, ai sensi della Convenzione di Budapest sul cybercrime. L'acquisita consapevolezza della necessità impellente di internazionalizzazione della prevenzione e repressione dei reati comporta una maggiore specializzazione degli operatori, affinché possano garantire l'intervento in emergenza, connotato da uno scambio celere di informazioni, prove digitali e richieste di preservazione all'estero di dati informatici.

Centro Nazionale Anticrimine Informatico per la Protezione Delle Infrastrutture Critiche (C.N.A.I.P.I.C. e N.O.S.C.)

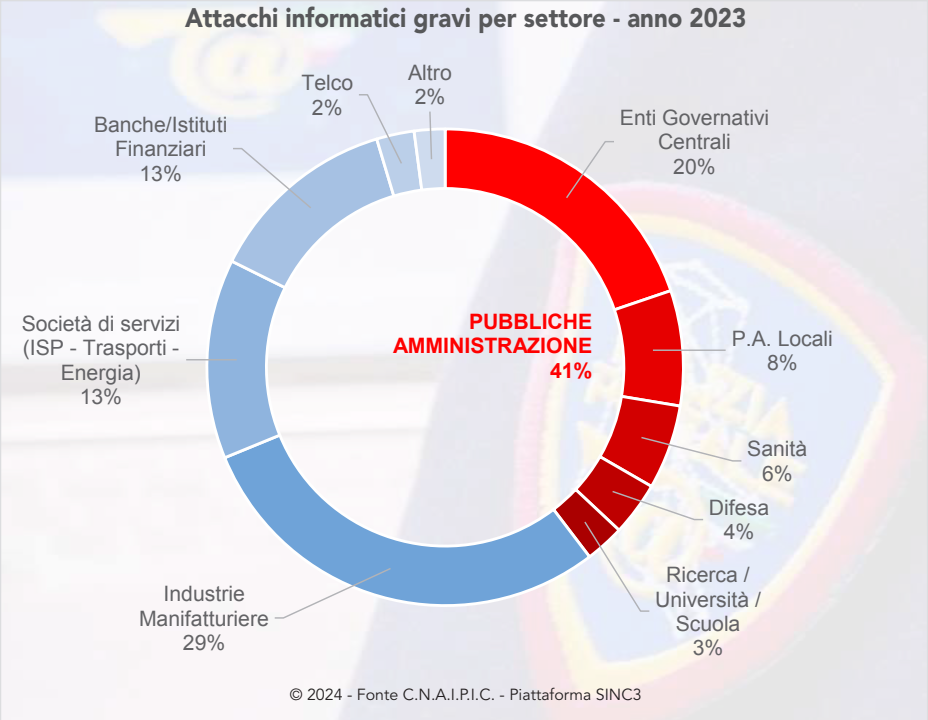
ANNO 2023	
Attacchi rilevati	12.101
Alert diramati	77.012
Indagini avviate dal C.N.A.I.P.I.C.	96
Persone indagate	224
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	79
Attacchi Ransomware	269

All'esito dell'analisi statistica, ancora una volta, la categoria merceologica per cui è stato rilevato un maggior numero di attacchi - connotati prevalentemente per la riferita finalità di cybercrime - è costituita dal comparto delle pubbliche amministrazioni, seguito dal settore manifatturiero. All'interno dell'intera macro-area degli enti pubblici, l'attività operativa del CNAIPIC ha consentito di registrare un incremento di attacchi che, ancorché indirizzati verso target multipli, hanno manifestato la propria azione dirompente con particolare riferimento ad alcuni settori vitali della vita civile, quali le strutture del comparto sanitario.

Si fa riferimento - nello specifico - alle primarie strutture ospedaliere, nonché alle aziende sanitarie regionali o locali.

Le reti informatiche di questo settore sono spesso comunicanti tra loro e afferiscono alla gestione di alcuni applicativi necessari per l'erogazione dei servizi sanitari agli utenti. Il motivo principale di quest'attenzione va rinvenuto nel fatto che le aziende sanitarie italiane dispongono ancor oggi, per lo più, di ridotte capacità di reazione,

mentre i dati che detengono e il loro trattamento rappresentano una concreta ricchezza per le organizzazioni criminali. Inoltre strutture, come ospedali e cliniche, di rado possono permettersi lunghi periodi di disservizio causati da un cyber-attacco, per ovvi motivi, e questa circostanza diventa una fondamentale leva, di cui approfittano i criminali per richiedere il pagamento in tempi brevi di un cospicuo riscatto.



Analizzando la sola attività di contrasto del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, riferiti agli attacchi contro le IC, OSE, PAL e aziende, nel 2023, la Polizia Postale ha rilevato e investigato 632 casi di attacchi cyber gravi. Di questi, sono stati 192 gli eventi particolarmente gravi per il loro impatto negativo a livello nazionale, in termini di sospensione di erogazione di servizi essenziali o comunque di pubblico interesse. Il 41% degli attacchi cyber gravi ha interessato le Pubbliche Amministrazioni.

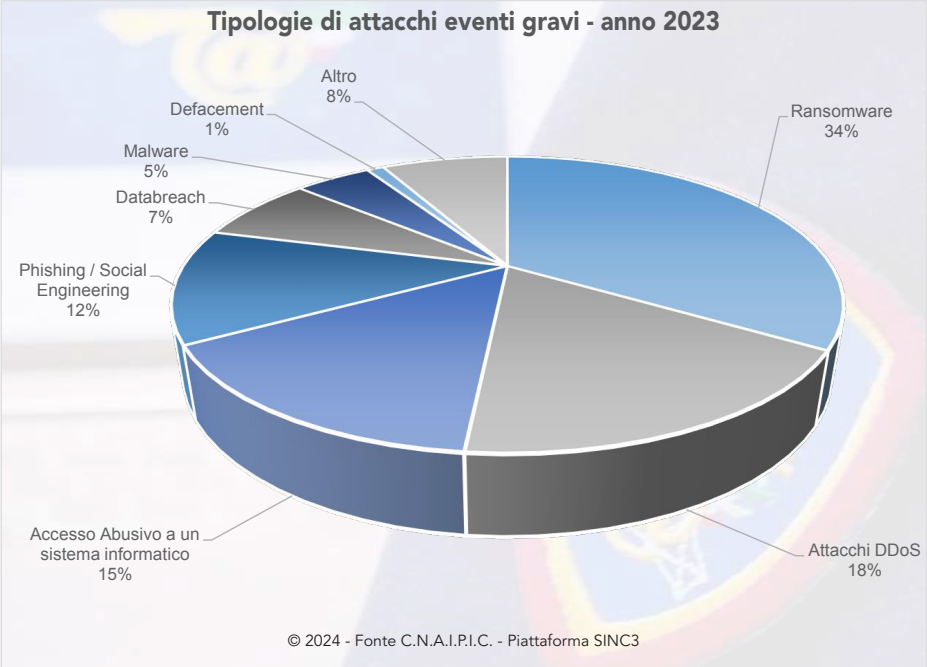
Accanto alla matrice criminale, si è è rilevata, in maniera certamente non meno preoccupante, la proliferazione di attività ostili motivate da ragioni di *cyber-warfare*, specie nel corso di fasi storiche, come quella attuale, caratterizzate da tensione e conflitti internazionali che vedono nel dominio cibernetico uno dei principali terreni di elezione.

Prima l'aggressione della Federazione Russa all'Ucraina e, successivamente, l'esplosione del conflitto israelo - palestinese sono stati accompagnati, sin dalle prime fasi, da un significativo aumento di attività ostili, massive e mirate, aventi come bersaglio le infrastrutture critiche della nazione attaccata, come pure dei Paesi che ne sostengono le ragioni nel conflitto. È questa la dimostrazione di come il dominio del cyberspazio sia divenuto elemento imprescindibile delle nuove guerre.

Le offensive cibernetiche dei principali gruppi criminali - che in questo settore assumono sempre più spesso una connotazione statuale - si caratterizzano ancora principalmente come campagne di phishing ovvero per la diffusione di malware distruttivi (specialmente Ransomware).

Al contempo, si registra un costante aumento di attacchi DDoS (Distributed Denial-of-Service), mentre più sporadicamente si assiste ad un'esfiltrazione di dati sensibili dai domini colpiti.

Quest'ultima tipologia di attacco si caratterizza per la messa in campo di tattiche e tecniche finalizzate ad interrompere i servizi informatici di un'organizzazione, spesso governativa/statuale, provocandone l'inservibilità di server o delle connessioni di rete, per renderli inutilizzabili. Generalmente, l'effetto della saturazione dei sistemi colpiti viene causata dalla generazione di enormi volumi di traffico - proveniente dall'estero - per sovraccaricare server o interconnessioni di rete.



Gli eventi di cyber crime gravi nel 2023 sono stati caratterizzati per il 34% da attacchi di tipo Ransmware, per il 18% da attacchi DDoS e per il 15% da accessi abusivi a sistemi informatici.

Paradigmatiche e più attuali appaiono le proiezioni nel dominio cibernetico del conflitto Israele-Hamas. Sin dall'inizio del conflitto, infatti, gruppi hacker State-Sponsored hanno iniziato a dirigere attacchi mirati ad arrecare disservizi alle infrastrutture critiche israeliane estendendo poi, specie a scopo dimostrativo, le azioni ostili ai danni di infrastrutture dei paesi occidentali, tra cui l'Italia, ritenuti vicini alla causa israeliana. In via generale, il numero degli avversari schierati sui due opposti fronti appare elevato e comprende realtà hacktiviste sia note che emergenti, oltreché consorzi criminali APT - Advanced Persistent Threat, che utilizzano tecniche di hacking continue e sofisticate per ottenere l'accesso a un sistema e garantirsi una persistenza silente all'interno dello stesso, rimanendovi per un periodo prolungato, e sono generalmente rivolti a bersagli di alto valore. In particolare, sono state analizzate rivendicazioni di molteplici attacchi verso obiettivi israeliani realizzati con tecniche quali attacchi

DDoS, hijacking di API per l'invio di messaggi push ai telefoni mobile, leak di credenziali e documenti. Gli eventi cinetici del conflitto sono stati subito accompagnati dalla diffusione di disinformazione e dalla condivisione di video falsi o fuori contesto, con l'obiettivo di alimentare un caos informativo che contribuisse a creare disordini.

Operazione Cookie Monster

Nell'aprile del 2023, nell'ambito di una più vasta indagine a livello internazionale, denominata Operazione COOKIE MONSTER, svoltasi simultaneamente in 17 Paesi, condotta da FBI e dalla polizia olandese, coordinata da Europol ed Eurojust e diretta dalla Procura di Roma, gli investigatori del CNAIPIC hanno messo a segno un'operazione senza precedenti. Genesis Market, piattaforma specializzata nella vendita di credenziali di accesso e dati rubati, con un giro di affari di oltre 2 milioni di identità virtuali sottratte, è stata disattivata, con sequestri, eseguiti in tutta Europa, dei server sui quali poggiava l'infrastruttura informatica. In Italia risultavano coinvolte migliaia di credenziali afferenti, sia a spazi informatici della vita privata di comuni cittadini, sia a password per l'accesso a spazi istituzionali della p.a., nonché di banche e grandi imprese nazionali, erogatrici di servizi pubblici essenziali. All'esito delle indagini, sono stati emessi 37 decreti di perquisizione personale, locale e informatica nei confronti di altrettanti clienti della piattaforma, che nel corso del tempo avevano acquistato migliaia di credenziali di accesso.

Operazione internazionale TALPA, gruppo Ragnar Locker

Ragnar Locker è una delle maggiori gang specializzate in attacchi informatici di tipo ransomware, in grado di cifrare e quindi paralizzare i sistemi colpiti, pregiudicando così l'erogazione di servizi pubblici essenziali in vari settori, quali sanità, energia, trasporti e comunicazioni. Negli ultimi tre anni, la *crew* ha colpito almeno 168 aziende in Europa e negli Stati Uniti; in Italia risultano attinte importanti aziende del settore alimentare e chimico. La *crew* era solita richiedere riscatti da 5 a 70 milioni per ottenere la restituzione dei dati, ma a fronte del pagamento la restituzione non aveva luogo; seguiva piuttosto l'ulteriore ricatto della pubblicazione sul darkweb dei dati esfiltrati (tecnica della doppia estorsione), dissuadendo le vittime dal rivolgersi alla Polizia con la minaccia di pubblicare i dati sulla propria pagina, chiamata Wall of Shame (muro della vergogna). Operazione condotta per l'Italia tra il 16 ed il 20 ottobre, sotto la Direzione della Procura di Milano, dal Cosc Lombardia, con coordinamento del CNAIPIC, ha consentito l'individuazione ed il fermo in Francia, all'aeroporto di Parigi, di un informatico 35 enne, figura di spicco della gang, con ruolo di sviluppatore dei software malevoli. Perquisizione estesa alla sua abitazione, sita a Praga.

Financial Cybercrime

L'analisi delle evidenze riferibili al decorso anno 2023 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 *modus operandi,* tipici del crimine finanziario di interesse della Polizia Postale e delle Comunicazioni. In primo luogo il c.d. *"phishing"*[1] che consente il furto dei dati sensibili per l'accesso ai sistemi di *home banking*, funzionale ad 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.

Al riguardo giova rammentare come l'innalzamento delle procedure di sicurezza attivate dalle banche (anche con la doppia verifica sul telefono del titolare, ostacolo per la realizzazione dell'operazione in frode) abbia indotto i criminali ad attuare la tecnica del c.d. "*sim swap*", largamente diffusa: sussistendo la necessità di acquisire i codici autorizzativi, i criminali si attivano per ottenere un duplicato della SIM card della vittima (grazie a *dealer* compiacenti o attraverso l'utilizzo di documenti falsi) ove ricevono gli OTP necessari al perfezionamento delle operazioni fraudolente.

Analogamente, si registra una consistente operatività delle tecniche criminali del "*man in the middle*", del BEC (*business e-mail compromised*) e del *Chef executive Officer Fraud* (CEO *Fraud*): dinamiche delinquenziali che rappresentano a tutt'oggi le principali tipologie di frode maggiormente diffuse in danno di piccole e grandi aziende.

- Il BEC (*Business e-mail compromised*) può essere realizzato attraverso diverse modalità:
  - intercettando le comunicazioni fra aziende o tra privati (attraverso un accesso abusivo ad una delle caselle di posta elettronica delle potenziali vittime), al fine

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

di individuare eventuali messaggi che contengono richieste di pagamento, sostituirsi con l'inganno al creditore e dirottare i bonifici comunicando nuove coordinate bancarie;
- alterando in modo impercettibile l'indirizzo email del creditore, per trarre in inganno la controparte, dirottando come di consueto i bonifici su altri conti (è tipica anche la modalità che utilizza la tecnica denominata "*spoofing*", che consente un mascheramento dei dati reali di chi sta operando il crimine, facendo artatamente apparire alla controparte, che deve effettuare il pagamento, l'indirizzo email del creditore).

- CEO *(Chef Executive Officer)*
  - In questo caso i criminali, dopo un attento studio sulle fonti aperte (legate soprattutto agli spostamenti ufficiali dei CEO di grandi aziende per la partecipazione degli stessi ad eventi finanziari di grande rilievo), avendo cura di creare un indirizzo mail quasi identico a quello del capo dell'azienda (talvolta perfettamente identico attraverso la tecnica dello *spoofing*) o utilizzandone uno reale (previa illecita disponibilità delle credenziali di accesso), contattano un dirigente aziendale con potere dispositivo inducendolo, con l'inganno, a fare uno o più bonifici per un'operazione finanziaria riservata ed urgente. Spesso tali dinamiche criminali prevedono l'intervento di una figura con il ruolo di avvocato specializzato in contratti internazionali, nonché la formazione di documenti completamente falsi che supportano la strategia dell'inganno posta in essere.

L'attività di questa Specialità nel settore del *financial cybercrime* è svolta a 360°, sia con azioni di contrasto attuate in ambito repressivo, sia con strategie di contenimento realizzate sotto il profilo preventivo (con campagne mirate di informazione rivolte alle *law enforcement* non specializzate in materia di *cybercrime* e al pubblico, anche attraverso i *social* ufficiali).

FINANCIAL CYBERCRIME E MONETICA

ANNO 2023

CASI TRATTATI	10.755
PERSONE INDAGATE	927
SOMME SOTTRATTE	40.503.616 €

In tale complessiva azione, funzionale alla prevenzione ed al contrasto al *financial* cybercrime, la cooperazione internazionale assume un ruolo assolutamente strategico, atteso che la transnazionalità delle condotte illecite connota costantemente l'indagine giudiziaria di specifico settore.

Ordinariamente, infatti, è all'estero che si consuma, almeno parzialmente, la condotta criminosa e tanto le tracce informatiche (sovente abilmente manipolate attraverso i più vari strumenti di anonimizzazione), quanto le tracce finanziarie (conti correnti e strumenti finanziari, sistemi di pagamento elettronico, corrieri di denaro, cryptovalute, ecc.), frequentemente, riconducono fuori dal territorio nazionale; per tale motivo, nei casi di prontezza di reazione delle vittime e, quindi, nell'immediatezza dei fatti, grazie alla richiamata cooperazione è possibile conseguire buoni risultati in termini di recupero delle somme distratte e di identificazione degli autori.

Nel particolare contesto operativo, fondamentale è l'apporto della piattaforma OF2CEN *(On Line Fraud Cyber Centre and Expert Network)*, realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica, con la quale viene svolta un'accurata analisi delle frodi di interesse della Specialità: una struttura informatica frutto di specifiche convenzioni con le principali banche, con ABI e con gran parte del mondo bancario che consente di intervenire in tempi ristretti sulle segnalazioni oggetto di investigazione. A tal proposito si evidenzia che è allo studio una progettualità che consentirà di elevare i livelli di efficienza della citata piattaforma.

Nell'ottica di una proficua azione di contrasto, che come sopra rilevato non può prescindere da strategie di intervento operativo realizzate in sinergia con altri paesi, è da segnalare la costante, consueta, partecipazione, a vari tavoli di lavoro internazionali, tra cui merita espressa menzione quello denominato EMMA (European Money Mule Action), giunto ormai alla sua nona edizione e le cui ultime risultanze sono state condivise da tutti i paesi aderenti (partecipano, infatti, forze di polizia di altri 27 stati europei e l'agenzia Europol): in un periodo di tempo concertato vengono avviate operazioni in sinergia, anche con indagini congiunte, dando esecuzione a mirati provvedimenti delle Autorità Giudiziarie, identificando i titolari dei conti correnti con risultati investigativi di notevole rilievo.

Il 2023, inoltre, è stato caratterizzato dal sempre più crescente interesse, da parte delle organizzazioni criminali, per le c.d. cryptovalute. Le evidenze offerte dalle più recenti investigazioni offrono, infatti, il riscontro ad un innalzamento dei livelli di impiego di tali valute digitali, con conseguente sempre maggiore capacità di gestione dei sistemi di *blockchain* su cui registrare le transazioni perfezionate con "criptovalute". Tali transazioni si caratterizzano per una maggiore difficoltà di tracciamento, (costituendo per tale motivo utile strumento attraverso cui perfezionare l'efficace riciclaggio dei proventi illeciti) rendendo più complesse le investigazioni per la conseguente necessità di impegnare professionalità con elevati livelli di competenze in grado di utilizzare sofisticati *software* di analisi, che agevolano l'esplorazione dei citati sistemi di *blockchain*. A ciò si aggiunga che sebbene le transazioni in argomento, al netto delle richiamate difficoltà, siano tracciabili,[2] l'utilizzo di alcune particolari monete digitali - create per essere, nel loro funzionamento, totalmente anonime (su tutte le cripto valute "monero" e "dash") - rende impossibile acquisire informazioni utili alle investigazioni.

Per tutte le richiamate ragioni, appare più che verosimile che l'abilità tecnica richiesta per movimentare capitali ingenti attraverso il ricorso a criptovalute sarà sempre più rapidamente acquisita anche dalle organizzazioni criminali di stampo mafioso, le quali, nella recente storia, si sono caratterizzate per aver assicurato alle giovani generazioni di affiliati accresciuti livelli di professionalità e specializzazioni funzionali al successo dell'impresa criminosa.[3]

---

[2] Ogni utente e ciascun portafoglio virtuale (*wallet*) è, infatti identificato nella *blockchain* da un codice univoco alfanumerico. Seppure tale caratteristica ne determina la natura pseudo-anonima rimane tuttavia astrattamente possibile riuscire a collegare un indirizzo *wallet* all'IP con cui è stato gestito. Diventa quindi possibile, ad esempio, associare un *wallet* ad una area geografica, elemento utile all'identificazione del possessore.

[3] La circostanza che le criptovalute si caratterizzino per una elevata volatilità (in un mercato che, peraltro, è attivo senza soluzione di continuità 365 giorni all'anno H24), potenziale ostacolo al loro utilizzo nell'azione di riciclaggio può essere agevolmente superata

Sul tema, deve segnalarsi inoltre la circostanza di un sempre maggior utilizzo delle criptovalute anche da parte dei cittadini i quali, anche con bassa scolarizzazione informatica, sono sempre più attratti dagli investimenti in moneta digitale con la speranza di realizzare veloci e importanti guadagni esponendosi anche a furti e frodi attraverso attacchi di phishing o attraverso finte piattaforme di trading online.

Proprio per tale motivo, nell'ambito del panorama delittuoso di interesse è da segnalare la forte espansione delle truffe attuate tramite proposte di investimenti di capitali *online* (il c.d. *trading online*). Le evidenze più recenti riportano, infatti, una decisa crescita delle denunce e, conseguentemente dei capitali investiti sottratti alle vittime, con un coinvolgimento di soggetti passivi del reato non più circoscritto a persone vulnerabili come gli anziani, ma esteso a diverse tipologie di "investitori", segno della sempre maggiore capacità organizzativa della sottesa struttura criminale, ramificata per lo più all'estero.

TRUFFE ONLINE
ANNO 2023

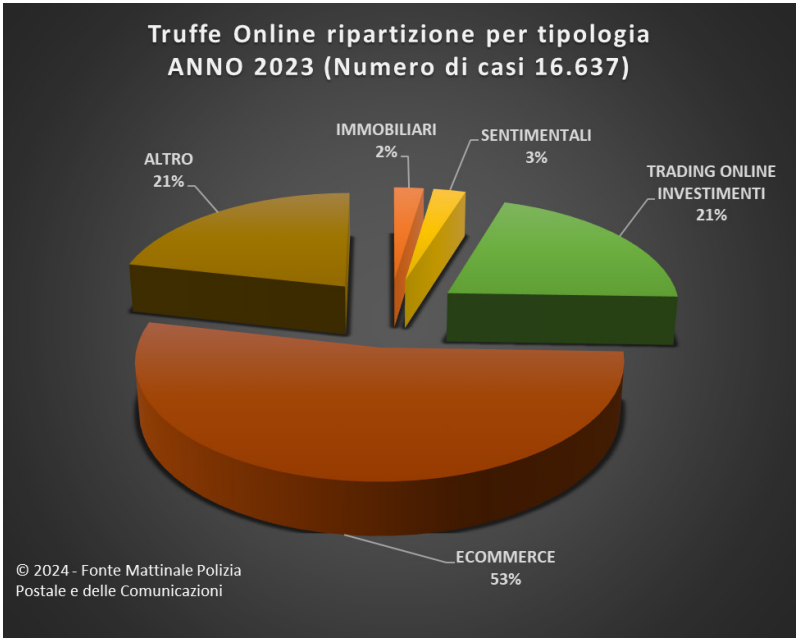
CASI TRATTATI	16.637
PERSONE INDAGATE	3.610
SOMME SOTTRATTE	139.536.457 €

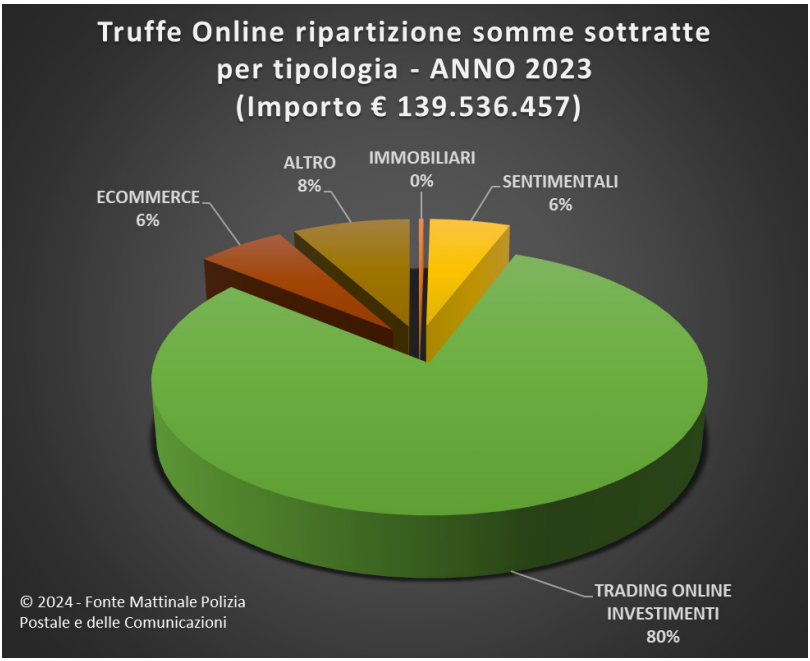
© 2024 - Fonte Mattinale Polizia Postale e delle Comunicazioni

attraverso la conversione delle più utilizzate criptovalute in stablecoin: crypto asset con valore stabile ancorato o ad una valuta fiat (generalmente il dollaro USA, esempio THETER, BUSD o USDC) o al prezzo dell'oro (suscettibile di ben minori fluttuazioni: come ad esempio la criptovaluta DIGIX GOLD).

ANNO 2023
TRUFFE ONLINE
rilevazione nazionale

		IMPORTI SOTTRATTI	
IMMOBILIARI	**CASI TOTALI 16.637**	440.585 €	**PERSONE INDAGATE 3.610**
SENTIMENTALI ROMANCE SCAM		7.699.707 €	
TRADING ONLINE		111.628.439 €	
E COMMERCE		8.492.999 €	
ALTRO		11.274.727 €	
		TOTALE 139.536.457 €	





Tra le nuove minacce che potrebbero modificare lo scenario della contraffazione e della violazione dei diritti di proprietà intellettuale - e più in generale delle condotte delittuose che attualmente si perfezionano in rete - si inserisce l'ideazione del c.d. "metaverso".

Spesso definito superficialmente come il naturale sviluppo dei social media, si caratterizza per esserne un potenziamento con funzionalità e destinatari virtualmente infiniti. Seppur ancora oggi si trovi nella sua fase iniziale di sviluppo, l'evoluzione della tecnologia computeristica sta rapidamente trasformando le primordiali "realtà virtuali" che, da ambienti virtuali immersivi, mutano sempre più in una rivisitazione della tecnologia della rete internet, capace di sostituire tutti gli apparati mobili esistenti, generando nuove tecnologie e mutando il comportamento dell'uomo: non "semplicemente" una rete di computer, server e altri dispositivi elettronici attraverso cui gli utenti, una volta online, comunicano tra di loro, interagiscono, visitano siti, fanno acquisti, ma una vera e propria "realtà alternativa" dove gli utenti, attraverso i loro avatar, interagiscono tra di loro, fanno attività, acquisti e partecipano ad eventi in un mondo che imita quello fisico e nel quale accedono usando tecnologie come la realtà virtuale (VR), la realtà aumentata (AR), l'IA, i social media e la valuta digitale.

In tale nuovo scenario internet è incorporato nell'esperienza umana quotidiana: si realizza una trasposizione della realtà fisica in una dimensione virtuale e la navigazione si trasforma in vita (apparente).

Naturalmente una tale svolta tecnologica non è esente da problemi, il metaverso, infatti, potrebbe acuire criticità già esistenti nell'era digitale. Fra le diverse distonie potenzialmente ipotizzabili, si potranno manifestare significativi problemi riguardo alla tutela dei dati e delle informazioni sia private che aziendali: gli utenti, infatti, potrebbero esporsi con sconosciuti sentendosi "al sicuro", mettendo a rischio i loro asset nella vita reale e permettendo ai malintenzionati di appropriarsi di tantissime informazioni sensibili quali, ad esempio, documenti personali, dettagli bancari, informazioni sul nucleo familiare e altri dettagli riservati. A questi temi andranno ad aggiungersi molte delle questioni attinenti alla tutela della proprietà intellettuale: il metaverso, infatti, favorirà il c.d. *immersive commerce,* uno shopping immersivo che può ben rappresentare il futuro dell'e-commerce in una realtà potenziata da una "esperienza sensoriale", con veri e propri negozi virtuali dove i clienti-avatar potranno fare acquisti digitali. Tutto ciò rappresenterà opportunità e rischi per titolari di diritti di proprietà intellettuale ed industriale, così come per fornitori di contenuti. Opportunità per i titolari di poter immaginare una presenza strategica nel nuovo ecosistema, ma rischi relativi a pirateria o contraffazione (in caso di marchi) e difficoltà in tema di prova di illecito sfruttamento.

Proprio in virtù di un tale possibile scenario, è parso necessario avviare uno studio approfondito - che sarà realizzato attraverso un Gruppo di Lavoro appositamente costituito in seno al Servizio Polizia Postale - delle potenziali evoluzioni del metaverso e dell'impatto che potrà avere in termini di diffusione delle condotte delittuose che ben potrebbero trovare in tale "ambiente" nuove e proficue opportunità.

Di seguito, un dettaglio delle **operazioni più significative** portate a termine dalla Specialità nell'azione di contrasto ai richiamati fenomeni delittuosi nell'anno 2023.

Operazione "Ghost Money"

In data 18 maggio 2023, i Centri Operativi per la Sicurezza Cibernetica (COSC) di Roma e di Torino, hanno dato esecuzione a provvedimenti di custodia cautelare, emessi dal G.I.P. di Roma nei confronti di 6 indagati per truffa aggravata, frodi informatiche, riciclaggio e auto riciclaggio.
Le indagini condotte da personale del COSC di Roma, sono state avviate a seguito di frodi realizzate con la tecnica del *sim swap* attraverso la quale il sodalizio criminale riusciva a carpire le credenziali dell'*home banking* inviate al numero telefonico delle

vittime, che venivano così private dei propri fondi. Le perquisizioni e l'analisi dei dispositivi sequestrati ha consentito di far emergere un complesso sistema di frodi informatiche (di oltre 2 milioni).
L'evoluzione investigativa ha consentito di smascherare il contesto criminale che ha colpito diversi istituti di credito mediante falsi mandati di pagamento SEPA, sfruttando le vulnerabilità dell'architettura dei sistemi informatici, e riciclando i proventi attraverso l'utilizzo di società intestate fittiziamente a c.d. "*teste di legno*".

Operazione "Grandi Firme"

In data 29 giugno 2023, personale dei Centri Operativi per la Sicurezza Cibernetica (COSC) di Catania e Napoli, coordinati dal Servizio Polizia Postale e delle Comunicazioni, hanno dato esecuzione a decreti di perquisizione locale e personale, emessi dalla Procura Distrettuale di Catania, nei confronti di 11 soggetti, di cui 7 residenti a Catania e 4 a Napoli, indagati per associazione a delinquere finalizzata all'introduzione nello Stato e commercio di prodotti con segni falsi.
L'operazione di polizia giudiziaria nasce dagli sviluppi delle evidenze acquisite all'esito di altre perquisizioni effettuate in data 10 novembre 2022, nel contesto dell'operazione "Gotha IPTV" tesa a contrastare la diffusione di palinsesti televisivi ad accesso condizionato.
L'analisi del materiale sequestrato nel corso della richiamata operazione di PG consentiva, infatti, di acquisire chiari riscontri indiziari circa il coinvolgimento di ulteriori soggetti coinvolti nell'illecito commercio, realizzato attraverso social media e servizi di messaggistica crittografata, di capi di abbigliamento, scarpe ed accessori vari contraffatti, riportanti i marchi di famose aziende di moda.
All'esito delle perquisizioni il personale operante ha rinvenuto un ingente quantitativo di merce contraffatta e diversi apparati cellulari utilizzati per le illecite condotte.

Operazione "Dream Earnings"

La Sezione Operativa per la Sicurezza Cibernetica di Pordenone, il Centro Operativo per la Sicurezza Cibernetica (COSC) di Trieste e la Squadra Mobile di Pordenone, con il coordinamento del Servizio Centrale Operativo e del Servizio Polizia Postale, hanno svolto un'indagine transnazionale nei confronti di un'organizzazione criminale dedita alle frodi finanziarie c.d. del "*Trading online*" radicata in Albania.
Nel corso delle indagini sono emerse decisive evidenze a seguito dell'analisi svolta sul materiale informatico e in particolare sugli oltre sessanta computer rinvenuti nel sequestro di due *call center* siti in Tirana, da cui si è potuto ricostruire il ruolo di ciascun componente all'interno del sodalizio criminoso.

L'attività investigativa ha sin da subito evidenziato la particolare complessità del sistema criminale, soprattutto dal punto di vista tecnico, caratterizzato dall'adozione di sofisticate tecniche di *spoofing* e *social engineering*, che hanno permesso di celare alle potenziali vittime la vera identità degli interlocutori inducendole a credere di essere in contatto con reali *broker* e quindi a concludere l'investimento.
La collaborazione tra le forze di polizia e le rispettive autorità giudiziarie è stata formalizzata con la costituzione di una squadra investigativa comune il cui lavoro in sinergia ha portato all'esecuzione di 13 ordinanze di custodia cautelare ed al deferimento in stato di libertà di 61 cittadini albanesi risultati essere tutti membri, con specifici compiti e ruoli, dell'organizzazione criminale transnazionale dedita alle truffe finanziaria del falso *trading online*.

Operazione "Cremonese Calcio"

Gli specialisti del Servizio Polizia Postale e delle Comunicazioni si sono attivati il 9 ottobre u.s. in seguito alla denuncia presentata dall'U.S. Cremonese Calcio per una patita frode informatica di tipo B.E.C. Fraud (Business Email Compromise).
In particolare, gli ignoti autori del reato, mediante la violazione dei sistemi di posta elettronica aziendali, si inserivano nella corrispondenza intrattenuta tra la U.S. Cremonese Calcio e l'omologa belga del Genk, riuscendo a modificare le coordinate bancarie per il pagamento della seconda rata dell'acquisto del calciatore belga Cyriel Dessers.
Indotta in errore, la U.S. Cremonese Calcio disponeva in data 28 settembre 2023, un bonifico di euro 1.719.500,00 su un conto corrente attestato presso la banca belga ING di Avenue Marnix 24 – Bruxelles.
L'immediata attivazione dei canali di cooperazione internazionale di polizia, ha consentito il blocco cautelativo del conto corrente contenente l'intera somma frodata.

Operazione "Piazza Italia"

Nel contesto di un'indagine avviata dal C.O.S.C. di Napoli su una truffa di $ 375.929,83, compiuta mediante la tecnica del B.E.C. (Busines Email Compromise), in danno della Società italiana "Piazza Italia S.p.a." con sede legale a Milano, il Servizio Polizia Postale ha attivato i canali diretti esistenti con l'Homeland Security Investigations, operante presso l'ambasciata americana in Italia, al fine di richiedere l'immediato blocco delle somme sottratte. Sulla base delle informazioni fornite dagli investigatori italiani, la predetta agenzia statunitense ha realizzato i necessari, richiesti, approfondimenti che hanno permesso, per un verso di avviare una propria indagine su frodi consumate in danno di società operanti negli USA e, per altro verso, di recuperare $ 220.000,00, restituiti alla predetta azienda italiana.

Operazione "Emma"

Si è conclusa a fine novembre 2023, l'Operazione di polizia ad alto impatto denominata EMMA, giunta alla sua nona edizione, messa in campo anche quest'anno dalla Polizia Postale e delle Comunicazioni e dalle Forze di polizia cyber di altre 27 Nazioni e coordinata da Europol ed Interpol.

I numeri complessivi dell'Operazione nei diversi Paesi europei, frutto del lavoro di tutte le Forze di polizia estere impegnate insieme alla Polizia italiana, sono ragguardevoli: anche grazie al supporto di oltre 2.822 istituti bancari e altre istituzioni finanziarie, sono state individuate 10.736 transazioni bancarie fraudolente e sono state avviate oltre 4.659 autonome indagini, riuscendo a prevenire frodi per un danno stimato in 32 milioni di euro.

Più di 10.759 i money-mule individuati (titolare di un conto bancario, che trasferisce denaro dal proprio conto corrente in cambio di contanti) e 474 gli organizzatori e coordinatori di muli identificati.

L'iniziativa è stata resa possibile anche grazie alla fattiva collaborazione delle banche e degli istituti di credito italiani, che, attraverso CERTFin e ABI, hanno assicurato un supporto in tempo reale agli investigatori, grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente dall'Italia al fine di prevenire e contrastare le aggressioni criminali ai servizi di *home banking* e monetica.

Operazione "Spinoff"

Nel mese di dicembre il Servizio Polizia Postale ha coordinato una vasta operazione della Polizia di Stato contro la pirateria audiovisiva.

Nell'ambito di un primo filone investigativo, avviato con la Procura Distrettuale di Catania, sono state eseguite 21 perquisizioni nei confronti di altrettanti soggetti indagati (attivi nelle città di Catania, Messina, Siracusa, Cosenza, Alessandria, Napoli, Salerno, Reggio Emilia, Pisa, Lucca, Livorno e Bari) a cui la procura etnea ha contestato a vario titolo reati quali associazione per delinquere a carattere transnazionale finalizzata alla diffusione di palinsesti televisivi ad accesso condizionato, danneggiamento di informazioni, dati e programmi informatici, accesso abusivo a sistema informatico e frode informatica.

Le indagini, avviate dal Centro Operativo Sicurezza Cibernetica di Catania con il diretto coordinamento del Servizio Centrale Polizia Postale, hanno permesso di delineare l'esistenza di un'associazione criminale organizzata in modo gerarchico secondo ruoli ben precisi e con promotori attivi sul territorio nazionale, avente come finalità la costante distribuzione, ad un elevatissimo numero di utenti, in ambito nazionale ed internazionale, di palinsesti live e contenuti on demand protetti da diritti televisivi,

di proprietà delle più note piattaforme (quali Sky, Dazn, Mediaset, Amazon Prime, Netflix) attraverso il sistema delle IPTV illegali, con profitti mensili per svariati milioni di euro.
Le perquisizioni sono state eseguite anche nei confronti di altri 10 soggetti (attivi nelle città di Napoli, Bari, Catanzaro, Palermo, Teramo e Bergamo) identificati in un secondo filone di indagine coordinato dalla Procura della Repubblica presso il Tribunale di Catanzaro. Nella circostanza, le investigazioni sono state avviate dalla Polizia di Stato del Centro Operativo per la Sicurezza Cibernetica Calabria e dalla dipendente Sezione Operativa per la Sicurezza Cibernetica di Catanzaro, con il consueto coordinamento del Servizio Polizia Postale.
Partendo dall'analisi di vari canali Telegram, è stato possibile riscostruire le condotte delittuose consumate in diverse province del territorio nazionale, al solito finalizzate alla diffusione illecita, dietro pagamento di corrispettivo, del segnale audiovisivo dei canali delle più note piattaforme che offrono servizi di PayTv (Sky, Dazn, Now, Disney Plus, Discovery Plus). Gli indagati, ritenuti responsabili allo stato delle indagini, di violazione del diritto di autore e di accesso abusivo a sistema informatico e telematico, costituiscono l'articolazione operativa di un'organizzazione che vede quale soggetto di spicco un cittadino italiano con precedenti di polizia specifici, emerso anche nelle indagini coordinate dalla Procura della Repubblica di Catania.
L'illecito flusso economico generato è di diverse centinaia di migliaia di euro.
La complessiva operazione di polizia giudiziaria ha portato al sequestro di n. 21 pannelli di gestione utenti e n. 2 pannelli di gestione flussi, consentendo l'inibizione dell'illecita diffusione dei segnali audiovisivi diretti a circa 50.000 utenti. Nel medesimo contesto sono stati sequestrati anche numerosi dispositivi cellulari ed informatici contenenti evidenze utili a riscontrare le ipotesi investigative.

Opeazione "Dark Money"

Gli investigatori della Polizia di Stato in servizio presso il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale della Liguria, coordinati dalla Procura della Repubblica presso il Tribunale di Genova, hanno eseguito la misura cautelare della custodia in carcere nei confronti di una 42enne straniera ritenuta il terminale italiano di un'articolata organizzazione dedita alle frodi informatiche, alla ricettazione ed al riciclaggio, e il deferimento all'Autorità Giudiziaria di altri soggetti, ritenuti suoi complici.
La lunga attività di analisi forense dei dispositivi informatici sequestrati ha permesso di sbloccare numerosi telefoni e dispositivi in uso alla 42enne, permettendo così di avere un quadro ancora più ampio della portata delle sue condotte illecite. In particolare, sono state trovate numerose evidenze di conti aperti fraudolentemente e di carte di credito emesse oltre che in Italia in diversi stati europei e negli Usa oltre

a quelle reperite nel *darkweb*. Il provento delle attività criminose, stimato in diversi milioni di euro, è stato in parte investito in cryptovalute.

Operazione "Falso Trading Online"

Nell'azione di contrasto alle condotte truffaldine realizzate attraverso false piattaforme di trading online, approfondite indagini degli investigatori specializzati del Centro Operativo Sicurezza Cibernetica – Polizia Postale e delle Comunicazioni di Torino hanno consentito di sottoporre a sequestro un sito web tramite il quale erano stati raccolti centinaia di migliaia di contatti di soggetti poi caduti vittima dell'inganno del falso *trading*.
La tecnica impiegata dai cyber-criminali consisteva nel costruire ad arte dei banner che richiamavano in modo illecito i nomi di società prestigiose al fine di persuadere con facilità le vittime a cliccare ed inserire i propri dati. Una volta compilati i form, i dati personali degli ignari utenti venivano trasmessi a società che servendosi di centralini telefonici effettuavano le chiamate ingannevoli; i broker "d'assalto" avevano quindi il compito di rappresentare alle vittime dei piani di investimento "sicuri", spesso nel settore tecnologico o delle criptovalute, in grado di far conseguire all'investitore profitti esorbitanti in tempi rapidissimi.
L'operazione, svolta sotto la direzione della Procura della Repubblica di Torino, è il risultato di uno studio tecnico mirato delle pagine web sospette e della concatenazione tra queste e le società coinvolte nel riciclaggio del denaro provento delle truffe; centinaia le transazioni economiche analizzate ed enorme il flusso di dati telematici esaminato per comprendere che i dati venivano aggregati in pacchetti "*ready to use*" a disposizione delle società truffaldine. Agli indagati sono stati contestati i reati di abusivismo finanziario e truffa aggravata.

Cyberterrorismo

Nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua costantemente il monitoraggio del web e svolge attività investigative, sia d'iniziativa che su specifica segnalazione (anche grazie a quelle che giungono dai cittadini tramite il portale del Commissariato di P.S. Online), al fine di individuare i contenuti illeciti presenti all'interno degli spazi e dei servizi di comunicazione online di ogni genere.

In particolare, il personale del settore Cyberterrorismo svolge attività informativa ed investigativa nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web.

Il target operativo di tale settore, dunque, si concretizza nella prevenzione e repressione dei reati che utilizzano la dimensione virtuale per fini terroristici, minando l'ordine e la sicurezza pubblica per ragioni riconducibili sia a forme di fondamentalismo religioso, sia a forme di estremismo politico ideologico, anche in contesti internazionali.
In ambito di cooperazione internazionale per la prevenzione ed il contrasto del *cyber* terrorismo, la I Sezione della III Divisione del Servizio Polizia Postale e delle Comunicazioni costituisce il punto di contatto nazionale della rete *Europol IRU - Internet Referral Unit*, coordinata dal Centro E.C.T.C. di *Europol (European Counter Terrorism Center*) – per il monitoraggio dei contenuti terroristi *online*, e partecipa insieme agli operatori di polizia di altri paesi anche ai cd. "*action day*" che vengono promossi in tale ambito, con notevoli risultati operativi.
E invero, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione *online*, *social network* e applicazioni di messaggistica istantanea, ha determinato parallelamente un considerevole aumento, ad una platea pressoché illimitata, di qualsiasi tipo di contenuti propagandistici riconducibili al terrorismo sia di matrice religiosa, che ideologica.

In tale ambito, si rende necessario garantire l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione *online* dei contenuti illeciti, assicurando un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione e con le Agenzie di *Intelligence*, competenti in materia di contrasto al terrorismo.
Nell'ambito del contrasto al fenomeno del c.d. *cyberterrorismo* gli operatori della Polizia Postale hanno concorso alla prevenzione ed al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica.
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 182.000 spazi web oggetto di approfondimento investigativi; tra questi 2.700 risorse digitali sono state oscurate poiché caratterizzate da un contenuto illecito.

Tra le numerose attività investigative svolte nel corso del 2023 dalla Polizia Postale, degna di nota è quella che ha permesso di identificare e denunciare due promotori del gruppo no-vax denominato "guerrieri ViVi", e di oscurare alcuni canali di comunicazione in rete.
In particolare, all'esito di un primo filone investigativo (che già nel 2022 aveva consentito di denunciare ventiquattro appartenenti al gruppo no vax - no green pass de-

nominato "guerrieri Vivi"), il Centro Operativo per la Sicurezza Cibernetica di Genova ha eseguito nel mese di gennaio 2023 perquisizioni nelle città di Brescia, Verona e Matera, delegate dalla D.D.A. della Procura della Repubblica di Genova, a carico di tre soggetti, indiziati di essere promotori del sodalizio nell'ambito di un procedimento per violazione degli artt. 1 e 2 c. 1 e 2 della l. n. 17/1982 (associazione segreta) e degli artt. 110 - 414 c. 1 n.1 e c.3, in relazione all'art. 340 c.p. (istigazione all'interruzione di un servizio di pubblica necessità).
E invero, il Centro Operativo di Genova, ha identificato i capi dell'organizzazione dopo mesi di serrate indagini informatiche che hanno consentito di setacciare centinaia di chat su numerosi social e documenti postati in rete, scardinando l'anonimato che gli autori ritenevano di avere conseguito grazie all'utilizzo di reti VPN e del sistema di messaggistica Telegram.

L'attività di proselitismo e istigazione a delinquere del gruppo no-vax ha quotidianamente preso di mira rappresentanti istituzionali e appartenenti all'ordine dei medici attraverso commenti "violenti", postandoli in maniera coordinata e ripetitiva sui profili social delle vittime, soprattutto di chi esprimeva opinioni a favore dei vaccini, imbrattando con scritte in vernice rossa le sedi di alcune Asl, di hub vaccinali, ospedali, ordini dei medici, scuole, sedi di alcuni sindacati e testate giornalistiche.
Con la conclusione delle restrizioni legate alla pandemia, il gruppo no vax, dichiaratamente ossessionato da ogni presunta forma di controllo, non ha interrotto la propria attività di proselitismo e si è orientato verso gli argomenti dei sistemi di pagamento e di identità digitale, dei cambiamenti climatici, del 5G, "attaccando" in rete, con lo stesso modus operandi, talvolta anche con minacce, chi esprimeva opinioni a favore dello sviluppo di tali tecnologie o tematiche.
Gli attacchi venivano coordinati su gruppi *Telegram* creati *ad hoc* e, all'interno degli stessi gruppi, venivano poi pubblicizzate le incursioni, con immagini o *screenshot* di quanto vandalizzato.
Sono state create anche alcune *challenge* con cui i promotori invitavano gli adepti a compiere azioni illecite, come posizionare striscioni o adesivi ritraenti il logo del gruppo su sedi Istituzionali, in una sorta di gara che prevedeva un premio in *bitcoin* da assegnare all'autore dell'azione più eclatante.
Le perquisizioni eseguite dagli investigatori del Centro Operativo per la Sicurezza Cibernetica di Genova, con l'ausilio degli Uffici di Milano, Venezia, Campania, Basilicata e Molise, e il coordinamento del Servizio Polizia Postale e delle Comunicazioni di Roma, presso le residenze degli indagati, hanno consentito di acquisire evidenze informatiche a conferma dell'operatività dei "*ViVi*" e di procedere al sequestro preventivo dei loro mezzi di comunicazione e propaganda in rete, emesso dal GIP del Tribunale di Genova.

Nel contesto delle attività investigative che sono state avviate grazie alla cooperazione internazionale, appare opportuno evidenziare quella che, il 26 gennaio 2023, a seguito di attivazione da parte del Servizio Centrale Operativo e del Servizio per la Cooperazione Internazionale di Polizia-Gruppo ENFAST-Divisione SIReNE, ha permesso al personale del Servizio di Polizia Postale e delle Comunicazioni Roma, unitamente alla Squadra Mobile di Rimini, di eseguire un Mandato di Arresto Europeo emesso dalla Germania per omicidio volontario, nei confronti di un trentenne di nazionalità turca, incensurato in Italia, ricercato su tutto il territorio Schengen.

In particolare, in seguito all'attività investigativa svolta dal Servizio Polizia Postale e delle Comunicazioni su un dato telematico condiviso in sede di cooperazione internazionale, veniva individuata la posizione del ricercato internazionale in Rimini, nella zona di Marina Centro.
Il turco, sottoposto a perquisizione presso l'hotel dove aveva preso alloggio con false generalità, veniva trovato in possesso di una pistola calibro 9x19 marca "Glock", con doppio caricatore e nr. 14 cartucce 9x19 "da guerra". All'esito degli immediati accertamenti svolti, l'arma era da ritenersi clandestina in quanto non censita sul catalogo Nazionale delle Armi, risultando altresì oggetto di segnalazione della Polizia Tedesca, per fatti accaduti su quel territorio. Venivano trovati anche documenti d'identità falsi, alcuni *smartphone* e altro materiale di interesse investigativo.
Il soggetto, quindi, è stato tratto in arresto, oltre che per il MAE, anche per la flagranza di reato riguardo alla detenzione e porto dell'arma clandestina, nonché del munizionamento da guerra e per il possesso dei documenti falsi.

Ed ancora, appare opportuno evidenziare un'ulteriore attività investigativa, parimenti avviata dalla Polizia Postale nell'ambito dello scambio informativo all'interno della rete di uffici *dell'European Network Fugitive Active Search Teams* (*E.N.F.A.S.T.*), a seguito della segnalazione pervenuta dalla Direzione Centrale della Polizia Criminale - Servizio Cooperazione Internazionale di Polizia -Divisione S.I.Re.N.E., inoltrata dal collaterale ufficio tedesco.

Nel dettaglio, in data 11 febbraio 2023, personale della Squadra Mobile della Questura e del Centro Operativo per la Sicurezza Cibernetica di Palermo ha tratto in arresto un cittadino straniero di 26 anni, ricercato in Italia e in ambito *Schengen* poiché destinatario di un mandato d'arresto europeo emesso dalla Germania, per i reati di tentato omicidio in concorso ed istigazione a delinquere.
Lo stesso soggetto era ricercato anche in Italia, poiché destinatario di un ordine di carcerazione emesso dalla Procura della Repubblica presso il Tribunale di Ferrara, dovendo espiare la pena definitiva di anni 9 e giorni 1 di reclusione (per reati di

spaccio di stupefacenti, detenzione di armi clandestine, furto aggravato, resistenza e minacce a P.U.).
In particolare, gli approfondimenti informatici condotti nell'immediato dal Servizio Polizia Postale e delle Comunicazioni, eseguiti sulle connessioni effettuate dal latitante per accedere al proprio *account social*, hanno permesso di localizzarlo nella zona del centro storico palermitano.
La prosecuzione degli accertamenti investigativi condotti da personale del C.O.S.C. e della sezione omicidi della Squadra Mobile di Palermo, anche attraverso una complessa attività di O.C.P., ha consentito la compiuta localizzazione del ricercato che, nonostante utilizzasse documenti falsi e numerazioni telefoniche intestate ad altri connazionali, veniva tratto in arresto e condotto, dopo le formalità di rito, presso la Casa Circondariale "A. Lorusso" Pagliarelli di Palermo.

Tra le numerose attività investigative effettuate nell'ambito del cd. cyberterrorismo appare opportuno evidenziare anche l'operazione "Alchimia" che ha permesso l'identificazione di diversi minori che sperimentavano miscele esplosive con sostanze chimiche acquistate *online*, i cui effetti venivano documentati con la pubblicazione di foto e video sui social.
In particolare, grazie ad una complessa attività di polizia giudiziaria, condotta tra ottobre 2022 e febbraio 2023, gli investigatori del Centro Operativo per la Sicurezza Cibernetica di Milano hanno individuato alcuni spazi *Telegram* utilizzati da adolescenti per condividere le loro esperienze su armi ed esplosivi.
Come emerso nel corso delle attività investigative, gli internauti, tutti minorenni e residenti in diverse aree geografiche del territorio nazionale, erano accumunati dalla passione per le armi e all'interno delle chat affermavano di andare in giro con coltelli e a volte persino con pistole (a salve o da *softair*), ovvero chiedevano informazioni e consigli su come confezionare molotov, esplosivi e detonatori, pubblicando anche foto degli ordigni realizzati, incuranti di possibili controlli da parte delle forze dell'ordine.
Al termine dell'indagine, coordinata dal Tribunale per i Minorenni di Milano, nella mattinata del 28 giugno 2023 scorso la Polizia Postale, in collaborazione con le D.I.G.O.S. e con l'ausilio di unità cinofile specializzate della Polizia di Stato, ha eseguito 8 perquisizioni nelle città di Avellino, Lecce, Milano, Pisa, Sassari, Nuoro e Treviso, con esito positivo, riscontrando ulteriori elementi investigativi a conferma del quadro probatorio già acquisito.

Tra le numerose attività investigative portate avanti nel corso del 2023, si segnala altresì quella che ha consentito alla Polizia di Stato, lo scorso 17 ottobre 2023, al termine di una complessa attività d'indagine coordinata dalla Procura della Repubblica

di Milano, di dare esecuzione a due misure di custodia cautelare in carcere, a carico di altrettanti soggetti di origine egiziana di 44 e 49 anni, ritenuti responsabili di partecipazione ad associazione con finalità di terrorismo ed istigazione a delinquere con finalità di terrorismo.
In particolare, l'attività investigativa condotta dalla D.I.G.O.S. di Milano - Sezione Antiterrorismo e dal Centro Operativo per la Sicurezza Cibernetica di Perugia, in collaborazione con la Direzione Centrale della Polizia di Prevenzione e con il Servizio Centrale Polizia Postale e delle Comunicazioni, ha avuto inizio nell'agosto del 2021, quando gli investigatori hanno avviato mirati approfondimenti nei confronti dei due indagati, entrambi evidenziatisi per la comune presenza all'interno di gruppi *WhatsApp* di matrice *jihadista* e riconducibili allo "Stato Islamico".
Tale attività investigativa ha confermato la centralità del *cyberspazio* e dei circuiti mediatici internazionali, nella diffusione del messaggio *jihadista* finalizzato al proselitismo ed all'esaltazione delle azioni terroristiche da parte dell'organizzazione a cui hanno aderito gli indagati.
E invero, la Polizia Postale ha riscontrato l'utilizzo della rete per una sorta di addestramento diffuso, cristallizzando a carico dei due soggetti indagati i seguenti elementi indiziari:

- pubblicazione all'interno dei profili social di copioso materiale inneggiante ad azioni terroristiche violente, in diversi casi con bambini protagonisti;
- condivisione sui propri account *Facebook* di contenuti *jihadisti*, con commenti e *like* di approvazione su profili altrui;
- presenza dei loro account all'interno di canali *Telegram* e gruppi *Whatsapp* direttamente riconducibili allo *Stato Islamico*, con la partecipazione di centinaia di utenti, registrati con numerazioni siriane, afgane, irachene, nord-africane, ma anche europee e sudamericane;
- versamenti di denaro disposti a favore di nominativi stanziati in Yemen e Palestina;
- indottrinamento religioso svolto nei confronti dei familiari, con particolare riferimento ai figli minori.

Nel corso della lunga attività di indagine, il quadro probatorio si è ulteriormente aggravato con un giuramento di fedeltà allo Stato Islamico postato su un profilo Facebook da uno degli indagati, nel maggio 2022.
A riprova dell'assoluta gravità degli elementi ricostruiti, è stata rilevata da parte degli indagati un *expertise* nell'uso delle armi e la disponibilità a dare consigli a chi volesse essere introdotto al loro impiego; inoltre, sono state individuate, sempre sul medesimo profilo *Facebook*, delle minacce dirette a cariche istituzionali italiane.

Per concludere, giova evidenziare che, con riferimento al contrasto della diffusione di contenuti terroristici *online*, il 24 luglio 2023 è stato pubblicato in Gazzetta Ufficiale il decreto legislativo n. 107, in vigore dal 26 agosto u.s., per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784.
Il quadro normativo unionale e la normativa attuativa hanno determinato per il Servizio Polizia Postale e delle Comunicazioni, Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, l'attribuzione di importanti competenze ed un ruolo cardine nel nuovo scenario nazionale ed internazionale in tale ambito operativo.
Ed invero, la Polizia Postale ha assunto specifiche competenze nelle procedure di emissione degli ordini di rimozione, nell'emissione delle decisioni di cui all'art. 5 par. 4 del Regolamento, nonché nella fase sanzionatoria.

In particolare, con riferimento all'emissione degli ordini di rimozione, la Polizia Postale è stata chiamata ad assicurare il necessario supporto tecnico ai punti di contatto delle *Autorità competenti* nell'assolvimento dei propri compiti, al fine di ottimizzare le complesse e rapide procedure di rimozione dei contenuti terroristici online, previste dal Regolamento (UE) 2021/784.

E ancora, la Polizia Postale ha il compito di portare a conoscenza l'Ordine di rimozione, adottato con decreto motivato dell'Autorità competente, ai titolari delle piattaforme di comunicazione online, destinatari del provvedimento stesso.

Inoltre, la Polizia Postale è stata individuata dal nuovo assetto normativo quale l'Autorità competente, con le seguenti competenze:

- emettere la decisione circa la valutazione se le piattaforme siano "*esposte a contenuti terroristici*" (ad esempio, per aver già ricevuto due o più ordini di rimozione definitivi nei 12 mesi precedenti);
- sorvegliare l'attuazione delle misure specifiche imposte ai titolari delle piattaforme online esposte a contenuti terroristici;
- emettere le ulteriori decisioni nei confronti del prestatore di servizi hosting che non abbia adottato misure specifiche adeguate a contrastare l'uso improprio dei suoi servizi per la diffusione al pubblico di contenuti terroristici.

Per l'adempimento delle incombenze imposte dal Regolamento europeo e dalla normativa nazionale di recepimento, la Polizia Postale assicura l'utilizzo dello strumento informatico denominato PERCI, con il coordinamento svolto dall'EU-IRU di Europol, gestendo altresì le segnalazioni ai fornitori di servizi *hosting* delle risorse web con contenuti illeciti di carattere terroristico di volta in volta interessati dalla segnalazione, previa attività di *deconfliction*, in raccordo con la Direzione Centrale della Polizia di Prevenzione.

Commissariato di P.S. Online

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

In tale ottica, il portale del Commissariato di PS online (raggiungibile attraverso la url https://www.commissariatodips.it/) permette al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli operatori della Polizia Postale e delle Comunicazioni in qualsiasi momento e ovunque si trovi.

Il sito è quindi un importante strumento di interazione con i cittadini che, **ogni giorno**, inviano in media **300 messaggi tra segnalazioni e richieste di informazioni** per segnalare siti con contenuti illegali o possibili reati informatici, ma anche esprimere il proprio disagio per un torto subito, evidenziare comportamenti che giudicano illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona; inoltre, nelle apposite sezioni "*alert*" e "approfondimenti", l'utente può informarsi consultando gli aggiornamenti pubblicati sul sito.

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

L'analisi delle oltre 105.000 richieste, tra segnalazioni e informazioni, ricevute dal portale nell'anno 2023, ha evidenziato che in molti casi gli internauti non adottano quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose.

In tal senso, al fine di migliorare l'attività preventiva, è stata ampliata la sezione dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela e prevenzione messo a disposizione del cittadino.
Per rendere ancora più incisiva ed efficace l'attività di comunicazione, è stata inoltre attivata una preziosa collaborazione con il giornalista Marco Camisani Calzolari, con il quale è stata realizzata una rubrica dedicata alla *cyber hygiene* o "igiene informatica"

con *clip video* di approfondimento sulle insidie della Rete e sugli accorgimenti per riconoscerle.

Tra i fenomeni riscontrati con maggior frequenza nell'anno 2023, si possono annoverare, a titolo esemplificativo, le truffe basate sulla tecnica dello *spoofing* che, replicando numerazioni di uffici di polizia o istituti di credito, inducono le vittime a trasferire i loro risparmi su conti fraudolenti; le campagne massive di *smishing*, sms fraudolenti che informano di presunti accessi anomali su conti correnti bancari al fine di carpire i dati di accesso delle vittime; i furti di profili social e false comunicazioni di assistenza per il recupero degli account rubati. In continua crescita il numero delle segnalazioni di estorsioni a sfondo sessuale, di truffe sugli acquisti online, che colpiscono parimenti acquirente e venditore e di false proposte di investimenti online.

L'attività più delicata riguarda la gestione delle numerose segnalazioni di cittadini che manifestano situazioni di disagio e minacciano di compiere gesti estremi. Nel 2023 gli **interventi dedicati** alla prevenzione correlata ad **intenti suicidari** sono stati **167**. 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 Centro, è richiesto un tempestivo e coordinato intervento che coinvolge anche gli uffici territoriali delle Forze dell'ordine per raggiungere nel più breve tempo possibile la persona in pericolo.
La popolarità del sito è avvalorata dal numero degli accessi[4] che, nel periodo di riferimento, sono stati 44.396.910.

ANNO 2023 **Resoconto attività** **Commissariato di P.S. Online**	**SEGNALAZIONI**	ANTITERRORISMO	1.452
		HACKING	24.372
		PEDOPORNOGRAFIA	1.635
		PHISHING	22.770
		SOCIAL	34.064
		TOTALE	84.293
	INFORMAZIONI	21.075	

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

ANNO 2023 **Resoconto sito** www.commissariatodips.it	**VISITE**	2.646.422
	ACCESSI	44.346.910

Campagne preventive di sensibilizzazione

Nell'ambito dell'attività di prevenzione svolta dalla Specialità, oltre al monitoraggio continuo della rete, la Polizia Postale e delle Comunicazioni è impegnata costantemente nella progettazione e realizzazione di campagne di sensibilizzazione e di educazione al corretto uso delle tecnologie, nel tentativo di far comprendere agli adolescenti, che talora non ne percepiscono a pieno il disvalore, le conseguenze che possono derivare dall'uso distorto della rete.

Tra le iniziative più significative, la campagna itinerante denominata "Una vita da Social", realizzata in collaborazione con il Ministero dell'Istruzione e del Merito nell'ambito del progetto "Generazioni Connesse", che nel giugno 2023 ha anche travalicato i confini nazionali, raggiungendo alcune città albanesi. L'iniziativa, giunta oramai alla sua 11^ edizione, è ripresa a pieno ritmo con l'inizio del nuovo anno scolastico. A bordo dell'iconico *truck* simbolo dell'iniziativa, che si trasforma in una vera e propria aula multimediale, sono state accolte dagli operatori della Specialità numerose scolaresche e cittadini, a cui sono state illustrate tutte le più attuali insidie della rete e forniti utili strumenti per un corretto utilizzo del *web*. L'impegno profuso in tale ambito ha consentito, nel corso dell'anno, di realizzare incontri con 2.300 istituti scolastici e di veicolare contenuti educativi a oltre 335.000 studenti, 22.936 docenti e 17.385 genitori.

Il 2 febbraio 2023 presso l'Auditorium Parco della Musica a Roma, alla presenza di più di 3000 studenti, è stato proiettato il docu-film "SENZA RETE", prodotto in collaborazione con la RAI, in cui vengono raccontate storie e testimonianze di ragazzi vittime di bullismo e *cyber-bullismo*, alcune delle quali con tragico epilogo.
Il 7 febbraio 2023 si è celebrato il "SAFER INTERNET DAY", un evento seguito da 340mila studenti attraverso la diretta *streaming*, unitamente al progetto #CUORICONNESSI, con l'obiettivo di responsabilizzare i ragazzi, soprattutto delle scuole di primo e secondo grado, sull'uso consapevole di internet. In occasione dell'evento, è stato promosso il quarto volume di "#CUORICONNESSI – cyberbullismo, bullismo e storie di vita online, la realtà delle parole", in cui i giovani si mettono a nudo trovando il coraggio di raccontare le proprie storie.

Il 5 settembre 2023, nello spazio "Italian Pavilion" al Lido di Venezia è stato presentato il progetto transmediale "A Voce Nuda", evento speciale della 80^ Mostra internazionale d'Arte Cinematografica di Venezia. A voce nuda" è un cortometraggio con Ginevra Francesconi, Luigi Fedele e Julia Magrone, e con Andrea Delogu e Mr. Rain. È un progetto sociale con uno scopo formativo e divulgativo, ideato dalla produttrice Manuela Cacciamani, per raccontare le minacce e le opportunità del digitale agli adolescenti e alle loro famiglie. È una storia di sextortion, quella della protagonista del corto, Camilla di 17 anni, alla quale, con l'illusione di una storia sentimentale, un ragazzo ha estorto immagini erotiche facendo poi richieste di denaro per non diffondere quelle immagini. In queste vicende, tutto comincia con qualche messaggio scambiato da persone gentili e affascinanti, che fanno complimenti e mettono like.

Le denunce e le segnalazioni per sextortion, raccolte dalla Polizia Postale nel 2023, descrivono un fenomeno in preoccupante crescita, che ha investito centinaia di adolescenti, soprattutto in età compresa tra i 15 e i 17 anni, trasformando l'esplorazione sessuale normale in fase adolescenziale in un incubo fatto di ricatti e somme di denaro estorte sotto minaccia.
Nel 2023 sono stati trattati 137 casi di sextortion; sebbene la maggior parte di questi sia riferibile a ragazzi della fascia di età 14-17 anni, anche il dato relativo ai minori di età compresa tra i 10-13 anni desta preoccupazione, in relazione alla particolare fragilità di queste giovani vittime.

La Polizia Postale e delle Comunicazioni ha inoltre lanciato, in occasione delle festività natalizie, una nuova iniziativa veicolata attraverso il portale e i canali social, un **"Calendario dell'Avvento Cyber"** che ha accompagnato gli utenti fino al 25 dicembre con curiosità, consigli e suggerimenti per navigare online sicuri, una nuova iniziativa per "fare rete" e diffondere la "cultura" della sicurezza digitale[5].

[5] Ogni giorno alle 18, sulla pagina Facebook e sul portale del "Commissariato di PS Online", nonché sulla piattaforma X (ex twitter), veniva aperta una casella con la pubblicazione di un post dedicato.

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 2023, ed evidenzio alcune tendenze che potremmo osservare nella prima parte del 2024. Questo lavoro è reso possibile anche grazie ai contributi del gruppo di ricerca IBM Security, IBM Security X-Force, i dati estratti dalla rete mondiale di IBM Security Trusteer e al lavoro quotidiano dei colleghi IBM Security che desidero ringraziare.

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

Un anno di cybercrime finanziario

Per alcuni anni il settore finanziario è stato il più attaccato a livello mondiale, alternando recentemente il podio con il settore manifatturiero. Anche limitando l'analisi alla sola Europa, è stato il settore finanziario il più attaccato nel corso del 2022[1], con l'Italia che ha attratto circa l'8% degli attacchi verso l'Europa, dietro Regno Unito, Germania e Portogallo [1].

Lo sfruttamento delle *public-facing applications* (tecnica MITRE ATT&CK T1190), che racchiude tutte le applicazioni con qualsiasi protocollo accessibili al pubblico tramite rete, è stato il principale vettore iniziale di accesso verso le organizzazioni europee, con il 32% di tutti gli incidenti gestiti da IBM Security X-Force, molti dei quali hanno portato come conseguenza a infezioni ransomware. A livello globale invece il principale vettore iniziale è stato il phishing (T1566), con il 41% di tutti gli incidenti gestiti da IBM Security X-Force. Tra il phishing, gli allegati di spear phishing (T1566.001) sono stati usati nel 62% degli attacchi, e i link a pagine di phishing (T1566.002) nel 33% degli attacchi [1].

Il *financial fraud*, frode bancaria o finanziaria, passa quasi sempre attraverso il furto delle credenziali d'accesso ai sistemi bancari o di pagamento, e riutilizzate per transazioni fraudolente all'insaputa del titolare. Invece di attaccare direttamente

[1] Alla data del presente articolo non sono ancora disponibili i dati riassuntivi dell'anno 2023.

l'istituzione finanziaria si preferisce attaccarne i clienti in quanto obiettivo indubbiamente più permeabile.

L'analisi delle principali campagne del 2023 mostra che la frode avviene prevalentemente attraverso i seguenti vettori:

- phishing 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 il furto dei fattori mancanti, ad esempio i fattori di autenticazione forte o codici dispositivi;
- malware per il furto di credenziali o fattori addizionali di autenticazione o manipolazione di una transazione;
- manipolazione dell'utente, ad esempio convincendolo a recarsi allo sportello e fare un'operazione dispositiva;
- hacking del dispositivo mobile tramite SIM Swap, emulazione software dello smartphone;
- e infine, ma in misura inferiore, con l'attacco diretto all'infrastruttura dell'istituzione finanziaria sfruttando vulnerabilità spesso note ma ancora non fissate.

La tecnica, o la combinazione di tecniche, varia in base alla tipologia di vittima, con differenze tra il cliente finale (retail) oppure aziendale (corporate) che vanno ad affievolirsi nel corso degli anni.

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

In generale, la tendenza di diminuzione di attacchi meramente tecnologici, e un parallelo incremento di azioni di convincimento dell'utente si osserva sia nel mercato retail che in quello corporate.

Phishing verso il settore finanziario italiano

Il settore finanziario, anche in Italia, è da sempre obiettivo privilegiato dalle campagne di phishing per il furto di credenziali, siano esse di autenticazione ad 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 1300 campagne* di furto di credenziali per servizi bancari e sistemi di pagamento italiani tra il 1° gen-

naio e il 31 dicembre 2023, 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 conclusioni.

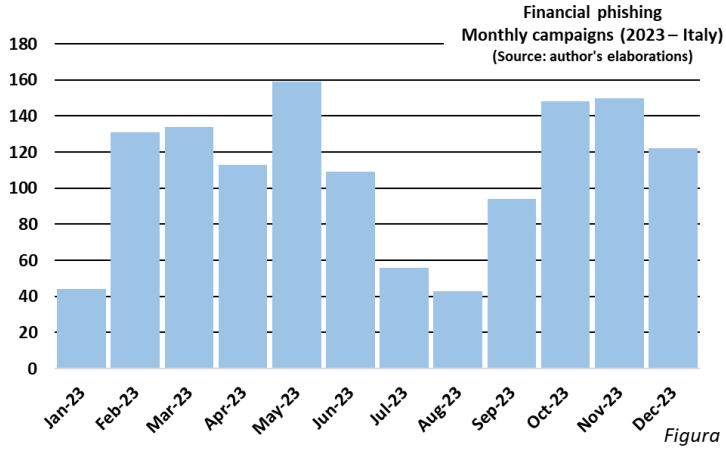


Figura 1

Limitandosi al settore finanziario italiano, in tutto il 2023 è stata osservata una media di circa 3,6 nuove pagine di phishing al giorno attivate e perfettamente funzionanti. La massima attività si è raggiunta nel mese di maggio 2023, con una media di 5,1 nuove pagine attivate al giorno. L'andamento annuale conferma tendenze molto simili osservate negli anni precedenti, con un picco minimo nel mese di agosto.

Anche se con una valenza statistica limitata, i primi giorni del 2024, fino alla data di scrittura di questo testo, sono state osservata una media di 3,5 nuove pagine di phishing al giorno, in linea rispetto alla media del 2023.

Il 43% di questi siti di phishing è stato ospitato negli Stati Uniti, un valore molto simile a quello dell'anno precedente. Provider Italiani hanno ospitato il 6% delle pagine di phishing, un valore quasi dimezzato rispetto all'anno precedente nel quale era stato dell'11%.

Il provider Namecheap, che nel 2021 da solo aveva ospitato oltre un terzo di tutte le pagine di phishing verso l'Italia, e il 17% nel 2022, si avvia ad uscire di scena ospitando ora solo il 4 % delle pagine. Una delle novità recenti del panorama phishing verso l'Italia è che circa una pagina su cinque è ospitata su Amazon.

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 take-down (disattivazione) dei domini malevoli da parte degli operatori finanziari.

Poco più di un anno fa Akamai [2] aveva stimato che circa il 20.1% di tutti i domini registrati erano stati a supporto di attività malevoli, per un totale di circa 13 milioni di nuovi domini malevoli al mese, a livello globale.

Uso del protocollo HTTPs

Altro dato che deve farci riflettere è che ormai il 99,5% delle URL di phishing usa 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.

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 [3].

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 e limitarsi a connessione solo verso siti che usino certificati di tipo Organization Validated (OV) o Extended Validation (EV).

Tutti i browser forniscono un'indicazione visiva sul tipo di validazione del certificato, purtroppo però non sempre di facile comprensione, 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 mercoledì al venerdì, pronte per attacchi che si sviluppano durante il week-end, quanto la vittima è più vulnerabile con gli sportelli bancari chiusi e gli help-desk ad orario ridotto, a cui è più difficile rivolgersi tempestivamente.

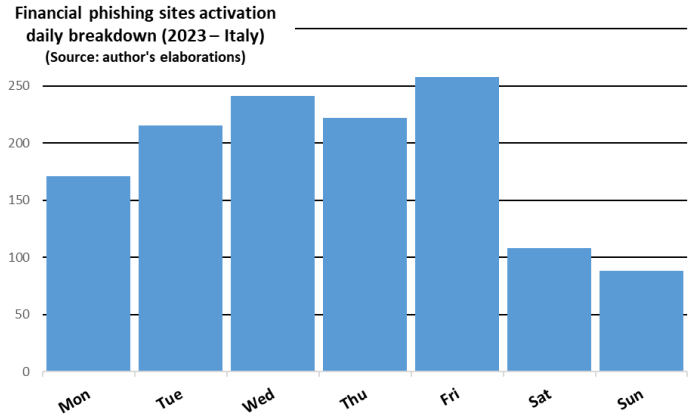


Figura 2

Il 47% delle pagine analizzate è rimasto attivo meno di 48 ore. Ci sono comunque notevoli eccezioni, con molte pagine rimaste perfettamente attive e che hanno continuato a "pescare" preziose credenziali per oltre un mese.

Molti phishing kit espongono in chiaro, tramite URL accessibili a chi ne conosce il path esatto, 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 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.

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

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.

Un piccolo Internet Service Provider con base nella Federazione Russa ha ospitato quasi 100 domini di phishing su 15 brand italiani a partire dal mese di novembre. Molti di questi domini sono protetti dallo stesso meccanismo di bot verification basato su Google reCAPTCHA per rendere più laboriosa l'analisi automatica delle pagine ospitate. Solo più laboriosa, non impossibile.

Alcune campagne di phishing multibrand, tra il mese di maggio e poi nei mesi finali dell'anno, si sono basate su un'unica pagina di atterraggio che rimandava a sezione

per il furto di credenziali di oltre 20 istituti bancari diversi. In questo caso la qualità del codice era abbastanza bassa e indubbiamente mirava a massimizzare il profitto nelle poche ore in cui la campagna è rimasta attiva.

Il phishing verso il settore finanziario italiano è veicolato principalmente tramite e-mail e SMS. 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 critica, può essere utile quando combinata con altre, per mettere a punto uno schema di attacco ripetibile su più utenti. 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.

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. Questa tecnica viene chiamata *vishing* (da Voice Phishing). 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. In particolare, questa tecnica è molto usata per convincere la vittima a dare 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 delle specifiche tecniche contenute nella direttiva 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 momento la banca invia al nostro cellulare o alla App installata sul nostro smartphone, e che lui non può avere senza il nostro aiuto.

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" [4].

Approccio simile si ha nelle finestre di chat live che cominciano a essere 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 a più alto rischio, inclusa l'immissione di bonifici.

Vista la semplicità realizzativa e il basso livello di rischio di chi la perpetra, si prevede una crescita di questa tecnica.

Per riassumere, le caratteristiche distintive delle campagne di phishing e malware sono:

- perfetta localizzazione in lingua italiana. Sono ormai scomparse le e-mail contenenti i grossolani errori grammaticali che vedevamo in passato, o tradotte in automatico;
- utilizzo frequente di chat live in lingua italiana o addetti bancari telefonici;
- i finti addetti bancari al telefono, nei casi in cui sono stati ingaggiati, parlano la lingua italiana senza alcuna inflessione straniera. Anzi spesso se ne possono riconoscere tratti dialettali regionali italiani. Questo ci porta a pensare che il fenomeno degli attacchi bancari in Italia è operato da attori cyber criminali italiani, anche se con utilizzo di infrastruttura estera e poggiandosi su money mule stranieri [6].
- necessità di furto del secondo fattore di autenticazione, che spinge necessariamente la frode ad un livello molto più avanzato di quanto non era in passato.

Nell'ambito della recente operazione Emma 9 (European Money Mule Action) coordinata da Europol, e svolta contemporaneamente in 28 nazioni, la Polizia Postale e delle Comunicazioni ha individuato 2.729 transazioni fraudolente, e identificando sul territorio nazionale 879 money mule, prevenendo frodi per oltre 6 milioni di euro [6].

L'attività investigativa sui money mule è di particolare pregio in quanto consente di individuare con esattezza l'entità delle cifre frodate o bloccate nel corso della frode. Nell'ambito di questa operazione europea le cifre effettivamente frodate sono state circa il triplo di quelle bloccate.

L'era del low cost phishing

Una frazione importantissima del 44% 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. Queste campagne, cresciute in maniera importante nel 2023, hanno colpito 26 delle 40 istituzioni finanziarie analizzate in questa analisi. È quindi da considerarsi un fenomeno generalizzato.

Questo fenomeno, già osservato lo scorso anno [8], è cresciuto in maniera considerevole nel corso dell'anno, raggiungendo il picco massimo nel mese di ottobre 2023 con oltre il 79% delle pagine di phishing ospitate su cPanel.

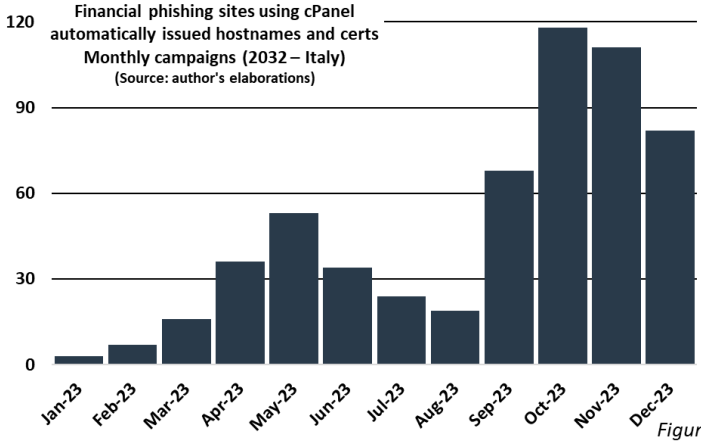


Figura 3

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) interface di cPanel non dispone di un hostname, le viene automaticamente assegnato un hostname all'interno del dominio cprapid.com generato sulla base dell'IP del server. 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

ENISA, Agenzia dell'Unione Europea per la Cybersecurity, pone i malware tra le principali minacce cyber del 2023 [10], preceduti dagli attacchi ransomware (che sono comunque malware specializzati), DDoS, e attacchi ai dati.

In questa sede ci occupiamo solo di financial malware, malware per frodi finanziarie, che sono un sottoinsieme molto specializzato di tutti i malware. Quasi un malware di nicchia se non fosse per il danno che arreca alle sue vittime.

L'obiettivo finale di questi malware è portare a termine una frode finanziaria, ad esempio un bonifico dal conto della vittima, e questo può accadere in diversi modi. È bene avere chiaro che un attacco prevede molte fasi e per questo necessariamente combina più tecniche. Esiste almeno una tecnica 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.

In passato c'era una netta distinzione tra clientela *retail* (I clienti al dettaglio come tutti noi quando come singoli individui approcciamo la nostra banca) e clientela *corporate* (aziendale). Anno dopo anno questa differenza si assottiglia sempre di più.

Nel mercato retail prosegue la veloce crescita nell'uso dei dispositivi mobili, proprio per la crescente diffusione che questi dispositivi hanno per questo tipo di clientela. A riprova di questo fenomeno quasi tutte le istituzioni finanziarie stanno lanciando banche completamente online che si rivolgono principalmente a un'utenza giovane interessata a utilizzare i servizi bancari esclusivamente online e tramite smartphone. In quest'area le tecniche sono estremamente variegate e si evolvono continuamente.

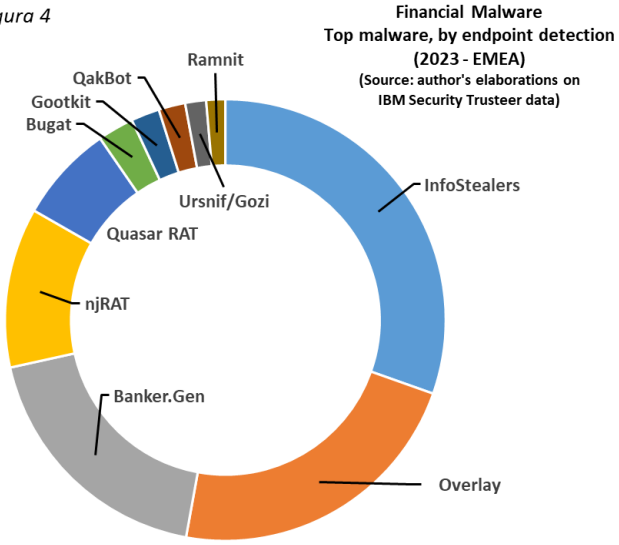
Il mercato corporate invece opera quasi sempre da una workstation, prevalentemente Windows. Per questo segmento i malware finanziari rappresentano circa il 6,4% degli attacchi [11]. Qui è anche evidente una significativa recrudescenza di truffe di tipo BEC (Business E-mail Compromise) [9] che concorrono nel 49,7% degli attacchi [11].

In entrambi i casi, retail e corporate, il numero di frodi portate a termine attraverso malware è complessivamente in decremento rispetto all'anno precedente [11] e vi è una convergenza delle frodi tra le due tipologie di vittime. Con l'aumento di efficacia dei sistemi antifrode, l'uso dell'intelligenza artificiale per individuare le transazioni sospette e la pronta analisi dei malware direttamente da parte delle istituzioni finanziarie e dei loro fornitori di sicurezza, gli sforzi dei frodatori si stanno muovendo verso la manipolazione della vittima per indurla a effettuare l'operazione, ad esempio facendoli recare allo sportello. Un'operazione allo sportello, proprio in quanto realizzata in presenza dall'intestatario del conto, evita molti dei controlli a cui sono soggette le operazioni online da remoto.

Attività dei principali financial malware nel corso dell'anno

Di seguito riportiamo dati e valutazioni sul malware per frodi al settore finanziario e alle sue declinazioni (banche, assicurazioni e finanza) limitatamente a osservazioni fatte da IBM Security Trusteer nell'area geografica EMEA (Europa, Medio Oriente e Africa) sull'intero anno 2023.

Figura 4



Anche secondo queste rilevazioni si è misurato un tangibile decremento nell'uso dei codici malware per portare a termine la frode finanziaria. Questo non ha trovato corrispondenza in una parallela diminuzione degli incidenti ma solo in una loro trasformazione. Attacchi del tipo Living off The Land (LOTL) dei quali parleremo in seguito, attacchi Business E-mail Compromise (BEC) [9], e manipolazione dell'utente sono cresciuti tutti in misura considerevole e si prevede una loro ulteriore crescita nel 2024.

Durante il 2023 è stata osservata una importante crescita nell'utilizzo di InfoStealer generici, software di Overlay e Remote Access Tools (RAT) che ha superato in utilizzo i codici malware specifici come Bugat, Gootkit, QakBot, Ursnif/Gozi e Ramnit.

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, l'anno scorso avevamo notato la comparsa di nuovi malware che sono invece subito scomparsi e soppiantati quest'anno da codici generici. 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.

Questo cambiamento segna una svolta importante in quanto abbassa il livello di competenza necessario a costruire un attacco. Se fino a qualche anno fa i malware per frodi finanziarie erano pezzi di codice molto sofisticato, di difficile scrittura e manutenzione. Secondo le più recenti osservazioni nuovi threat actors possono affacciarsi in questo ricco mercato senza la necessità di grosse competenze di programmazione e conoscenza dettagliata 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.

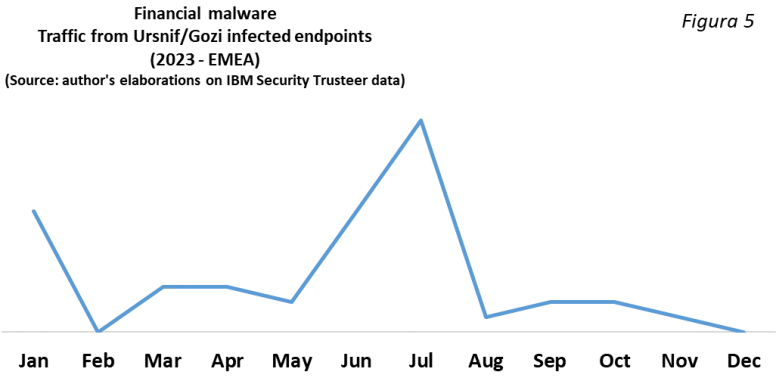
È ragionevole ipotizzare che questi cambiamenti aprano spazio all'ingresso di un numero sempre maggiore di cyber criminali con un conseguente aumento complessivo degli attacchi.

Lo SMIShing, SMS che arrivano sul telefono e invitano a visitare un link, è stato uno dei metodi più usati per infettare i dispositivi mobili. Sui sistemi Android si è abusato molto dei servizi di accessibilità dell'applicazione, 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 con lo smartphone che sono stati sfruttati in maniera malevola dai creatori di malware.

Finora scrivere malware per dispositivi iOS richiede uno sforzo, competenze e costi decisamente più elevati rispetto ai dispositivi Android. Inoltre, i dispositivi iOS sono stati anche protetti dal fatto che le applicazioni da installare possono provenire soltanto dallo store ufficiale Apple. Quest'ultimo meccanismo potrebbe venire meno nel corso del 2024 quando iOS dovrebbe consentire il *sideloading*, installazione di App anche da store non ufficiali, su pressione dell'Unione Europea attraverso la regolamentazione Digital Markets Act.

Sui sistemi Windows, Ursnif/Gozi uno dei malware bancari più antichi, malgrado in generale declino è stato al centro di numerose campagne verso utenti di online banking anche in Italia.

Figura 5



A partire da dicembre 2022 alcune campagne di e-mail verso l'Italia hanno veicolato WailingCrab, conosciuto anche come WikiLoader, per l'accesso iniziale nella macchina della vittima, e poi la successiva installazione di Gozi [12]. Nelle stesse campagne, Gozi ha usato un message broker MQTT open legittimo per comunicare con con la sua infrastruttura di Command-and-Control, mascherando così l'indirizzo dei propri server C2.

Sui clienti italiani Ursnif/Gozi è stato usato per implementare attacchi di tipo "IBAN swap", sostituendo l'IBAN del beneficiario durante una transazione utente, dirottando quindi i bonifici su conti correnti nella disposizione degli attaccanti.

Ursnif/Gozi è stato frequentemente usato in combinazione con altri malware. L'anno scorso IBM Security X-Force aveva individuato e analizzato una variante di Ursnif/Gozi [13], usata in attacchi in Italia, costruita per infettare il sistema Windows della vittima e contemporaneamente anche il suo dispositivo Android con il malware Cerberus. La componente Cerberus dell'attacco serviva a catturare i codici dispositivi inviati dalla banca attraverso SMS.

Cerberus è un malware molto attivo in Europa, in particolare in Italia, Spagna e Francia. Emerso nel 2019, era inizialmente privo di funzionalità avanzate. Ora si è evoluto fino ad incorporare meccanismi avanzati di anti-rilevamento e anti-analisi. Ha capacità di overlay attack, può intercettare SMS incluse le One Time Password inviate a verifica delle transazioni bancarie. Nelle ultime versioni Cerberus usa i servizi di accessibilità per ottenere il controllo avanzato sulle funzioni del dispositivo e manipolare le interfacce delle App.

Cerberus è distribuito come "Malware as a Service" (MaaS), affittato dagli sviluppatori ai criminali informatici per il tempo necessario a perpetrare gli attacchi.

In altre campagne, il vettore iniziale di Ursnif/Gozi sono stati documenti Office con macro malevole allegate a email artefatte, in apparenza contenenti fatture, avvisi di consegna o altra corrispondenza commerciale. Una volta infettate dal malware Ursnif e dopo aver tentato di accedere al proprio conto bancario online, le vittime ricevono un messaggio a schermo che le invita ad installare un'App di sicurezza per continuare a utilizzare i servizi della propria banca. Per questo viene mostrato loro un QR code da scansionare con il proprio telefono. Alla scansione del QR vengono reindirizzati su una pagina Google Play falsa, che usa typo-squatting o URL verosimili, e con il logo dell'App bancaria corrispondente alla banca della vittima. Questa App in realtà installa il malware Cerberus sul dispositivo mobile. L'opzione di non consentire l'installazione di App da fonti sconosciute, disabilitata di default sui dispositivi Android, limita l'impatto di queste campagne potrebbe.

La cattura delle credenziali di accesso alla posta elettronica, sia webmail che client installati sul computer o smartphone, è un'attività apparentemente anomala per un financial malware, ma è un andamento che osserviamo in crescita già da qualche anno. I gruppi cyber criminali fanno questo per avere una base dalla quale lanciare attacchi di tipo BEC, diffondendo malware da caselle elettroniche reali e spesso note alla vittima, con un'efficacia nettamente maggiore rispetto a quanto non si riesca a fare con il tradizionale phishing. I numerosi esempi di campagne veicolate tramite PEC ne sono un esempio.

Ciascun elemento, anche apparentemente insignificante, può essere utile per costruire e dare maggiore credito all'attacco, o collezionare informazioni per attacchi futuri.

La crescita degli attacchi Living off the Land

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 autosufficienti nel senso che trovano sul sistema da attaccare già tutti gli strumenti di cui necessitano.

Rientrano in questa categoria anche le macro all'interno di documenti Office, oppure comandi javascript inviati in forma più o meno occulta all'interno di e-mail. Negli attacchi LOLT i dati si esfiltrano con il protocollo FTP, la e-mail e le applicazioni che si trovano già installate sul dispositivo come ad esempio Telegram.

Il successo di questi attacchi è dovuto al fatto che richiedono un investimento davvero minimo e sono più difficilmente individuabili dagli strumenti di protezione del-

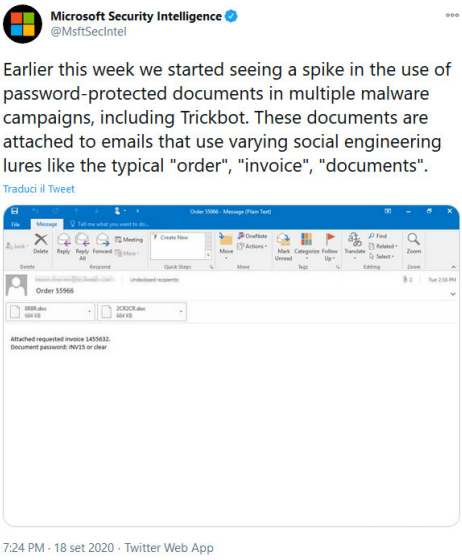
l'Endpoint tradizionali, che basano il loro funzionamento sulla ricerca di malware o script conosciute. Questi attacchi, quindi, tendono a essere più efficaci, permettendo all'attaccante di permanere all'interno dei sistemi compromessi a lungo prima di essere individuato.

Con la crescita degli attacchi LOLT 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 all'interno di documenti Office, PDF o e-mail.

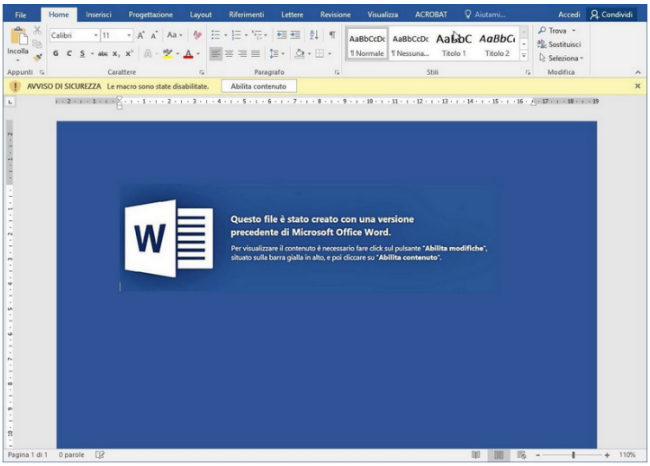
Il ruolo delle macro all'interno di documenti Office

Nel corso dell'anno i malware sono stati veicolati nella maggioranza dei casi attraverso documenti Office allegati a e-mail [10] o file .zip 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 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, 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 [14]. 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 ad 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 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.

Il furto di credenziali all'origine di molti schemi di attacco

C'è consenso da più parti sul fatto che il phishing sia uno dei principali vettori di accesso iniziale. Per vettore di accesso iniziale si indica il canale di primo accesso all'interno di una rete o un account, che non è necessariamente il canale usato per portare a termine l'attacco.

Negli incidenti gestiti da IBM Security X-Force a livello globale, il phishing (MITRE T1566) è stato il principale vettore di accesso iniziale, coinvolto nel 41% degli incidenti gestiti [1]. Per confronto, nel 2020 era stato il 33%, con una crescita di 8 punti percentuali in 3 anni. Tra il phishing, gli allegati di spear phishing (T1566.001) hanno contribuito al 62% degli attacchi, i link a collegamenti di phishing (T1566.002) al 33% degli attacchi.

IBM Security stima che il furto o la compromissione delle credenziali sia stato il vettore di attacco nel 16% dei data breach del corso del 2023 [15].

L'uso di credenziali valide è stato il vettore di accesso iniziale più comune negli incidenti di sicurezza che hanno coinvolto ambienti e servizi cloud (T1078.004 Valid Accounts: Cloud Accounts) con il 36% dei casi [16]. Le credenziali di accesso a sistemi cloud costituiscono quasi il 90% delle risorse cloud in vendita sul dark web, con un prezzo medio di $10,68 per credenziale, in lieve diminuzione rispetto al periodo di riferimento precedente [16].

Anche ENISA conferma che il phishing è il vettore di accesso più comune [10], non solo nelle frodi finanziarie, con una crescita di nuovi e più aggressivi modelli di ingegneria sociale, un approccio che consiste nell'ingannare le vittima e indurla a compiere azioni nel mondo fisico oltre che in quello elettronico.

Il CERTFin annovera il phishing come principale vettore di infezione per i ransomware, considerato tra le principali 5 minacce verso le organizzazioni finanziarie [17].

Il furto di credenziali, attraverso il phishing o più in generale il social engineering, da solo non costituisce un attacco, ma è il primo passo di molti schemi di attacco più complessi. Il MITRE pone il phishing come elemento alla base di ben 79 tecniche/sotto-tecniche [18] del framework ATTACK, principalmente nelle fasi di Reconaissance, Resource Development e Initial Access, quindi nelle fasi iniziali di un attacco. Il resto dell'attacco si sviluppa in base allo specifico obiettivo.

Il phishing bancario usa le credenziali delle vittime per poi effettuare operazioni dispositive dai conti correnti delle vittime. Il phishing verso provider Internet usa le credenziali per attivare servizi Internet, ad esempio spazio web, strumentali a costruire altri attacchi. Il phishing verso servizi di webmail serve a costruire attacchi più realistici, inserendosi in conversazioni reali della vittima. Il phishing verso clienti di aziende di recapito serve ad indurre a pagamenti per la ricezione di spedizioni. Ma ci sono attacchi che partono dal furto di credenziali e si sviluppano verso gli utenti di piattaforme di streaming TV o di gaming, o ancora di scommesse online.

Combattere il phishing e il furto delle credenziali è quindi un imperativo per la protezione di una vasta gamma di attacchi [17].

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 un attacco ad un sistema finanziario. La direttiva europea PSD2 [19] 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 anche noti come MFA – Multi-Factor Authentication, o autenticazione a più fattori [20]. 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, tutte le frodi che hanno successo, e sono molte, sono riuscite a raggirare la protezione introdotta dalla Multi-Factor Authentication.

Laddove la credenziale aggiuntiva preveda qualcosa (PIN, codice monouso) da reinserire da parte di un utente all'interno di 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. Curioso come, proprio per proteggersi dal phishing, siano stati introdotti in alcuni casi meccanismi aggiuntivi di autenticazione a loro volta soggetti a phishing.

Sempre più spesso si stanno diffondendo sistemi di MFA resistenti al phishing, i cosiddetti *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 [22] sono quelli basati su autenticazione FIDO/WebAuthn (conosciuta anche come standard FIDO2), 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 2024

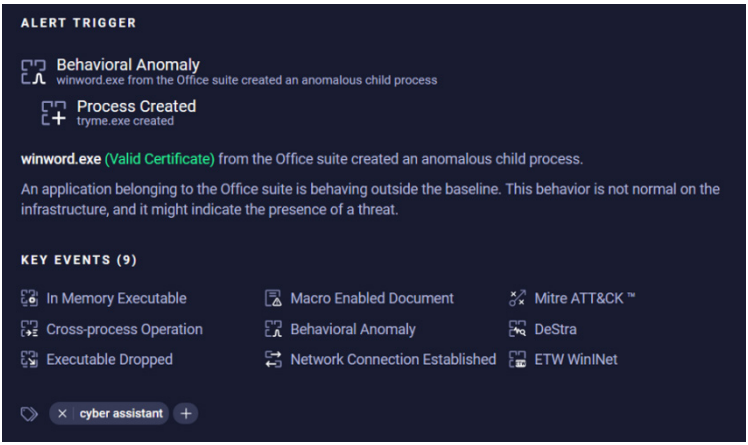
Le osservazioni degli ultimi mesi descrivono un contesto di attacchi in costante evoluzione con un contemporaneo abbassamento della soglia di difficoltà per realizzare gli attacchi. La disponibilità di molti strumenti e malware sui marketplace nel dark web, a volte anche gratuiti, e l'utilizzo dell'intelligenza artificiale generativa per la costruzione di attacchi sempre più efficaci non può che aprire la strada all'aumento del numero e della complessità degli attacchi.

È evidente la necessità di implementare soluzioni in grado di adattarsi rapidamente e automaticamente ad una minaccia estremamente mutevole.

Sul mercato si osserva una virtuosa convergenza di quasi tutte le soluzioni di sicurezza verso l'adozione di feed di Threat Intelligence [25]. I feed veicolano, quasi in tempo reale, descrizioni di attacchi e minacce e questi aggiornano costantemente

le soluzioni di sicurezza con nuove definizioni, proprio come abbiamo imparato per gli antivirus. Queste integrazioni, un tempo appannaggio solo 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.

A costo zero sia per l'utente aziendale che per la nostra connessione di casa è l'adozione dei *protective DNS services*, cioè servizi DNS progettati per proteggere la privacy e la sicurezza della navigazione, bloccando risoluzioni DNS-IP per indirizzi malevoli. Quad9 ne è un esempio virtuoso [24]. Si tratta di un servizio gratuito che sostituisce il DNS generalmente fornito dal proprio provider Internet o il DNS aziendale. Ogni volta che un dispositivo esegue una risoluzione hostname-IP, Quad9 ne analizza la reputazione e il rischio bloccando gli hostname e gli IP considerati pericolosi. Questa azione di blocco protegge, con un impatto davvero minimo, i computer, i dispositivi mobili e i sistemi IoT da un'ampia gamma di minacce come i Remote Access Tools, malware, phishing, spyware, e botnet [24].



L'incremento dei Living Of The Land attacks, la crescita nell'uso degli InfoStealer e dei Remote Access Tools continuerà a caratterizzare il panorama degli attacchi.

Non è trascurabile che tutti gli attacchi qui descritti hanno successo malgrado la presenza sull'endpoint di un antivirus, ormai a corredo di quasi tutti i sistemi operativi e dispositivi.

Le soluzioni di Endpoint Detection and Response (EDR) sono uno strumento efficace di protezione, in quanto operano attraverso indicatori di attacco (Indicators of Attack,

o IOA) anziché i soli indicatori di compromissione (IOC) e intervengono laddove l'antivirus/antimalware non riesce più ad arrivare. L'indicatore di attacco è spesso nella forma di un'indicazione di comportamento anomalo di un file, non più solo un eseguibile, durante l'esecuzione. Processi anomali creati, modifiche inattese della Registry, comunicazioni di network verso l'esterno, scritture inaspettate sul disco sono tutti indicatori che possono portare al blocco di un eseguibile individuato come malevolo.

Se le password come principale elemento di autenticazione dovevano essere abbandonate già da molti anni, è il momento di rivalutare la sicurezza effettivamente fornita da alcune implementazioni di Multi-Factor Authentication. Molte implementazioni un uso, ad esempio quelle basate su un OTP via SMS oppure una App di autenticazione che genera un codice temporaneo, sono potenzialmente soggette a phishing e al furto del fattore di autenticazione. All'atto pratico non proteggono come si sperava. FIDO è uno degli standard più promettenti per offrire un'autenticazione sicura su siti web e applicazioni tramite l'inserimento di dati biometrici o di una chiave di sicurezza, anziché una password. Se non c'è password c'è molto meno da rubare attraverso il phishing.

L'Intelligenza Artificiale contribuirà sicuramente ad aumentare il rischio informatico. E-mail di phishing scritte con il contributo dell'AI diventeranno sempre più comuni e convincenti per la vittima.

C'è una relazione quasi simbiotica tra cybersecurity e intelligenza artificiale. Se da un lato appare naturale vedere applicazioni di intelligenza artificiale a supporto della cybersecurity, e ci sono già molti esempi in questo campo, sarà sempre più necessario utilizzare la cybersecurity per proteggere l'intelligenza artificiale.

Con il ruolo crescente che stiamo dando all'intelligenza artificiale è imperativo proteggere fin da subito i dati, i modelli, e nel complesso i sistemi AI dagli attacchi, generati da utenti umani malevoli o da altri sistemi di intelligenza artificiale.

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 alla ampia scelta e flessibilità che lascia all'organizzazione, in quanto questa può decidere di far risiedere i dati e le applicazioni dove ritiene più appropriato, o dove le è economicamente più conveniente, integrando perfettamente 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.

Il tema è quantomai attuale. Il Cost of a Data Breach Report 2023 [15], mostra ormai da diversi anni consecutivi come l'intelligenza artificiale e l'automazione nella risposta agli incidenti, siano i due fattori che maggiormente contribuiscono alla riduzione del danno, e quindi dei costi associati, nel caso in cui una azienda sia vittima 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] *IBM Security X-Force Threat Intelligence Index 2023* IBM Security, February 2023

[2] *Flagging 13 Million Malicious Domains in 1 Month with Newly Observed Domains* Akamai Security Research, September 2022

[3] D. Adrian, S. Chen, J. DeBlasio, E. Stark, and E. von Zezschwitz *An Update on the Lock Icon* Chromium Blog, May 2023

[4] *Contrasto alla criminalità finanziaria - Attività della Polizia Postale contro le frodi "Alias"* Commissariato di P.S. online, novembre 2020

[5] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, maggio 2019 https://www.intesa.it/come-proteggersi-dagli-attacchi-business-email-compromise/

[6] S. Foffo *Operazione "Emma 9" contro i muli del cybercrime* Polizia di Stato, dicembre 2023

[7] *Paper trail ends in jail time for 1 013 money mules* Europol, December 2023

[8] Pier Luigi Rotondo *Elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2023 sulla sicurezza ICT in Italia, marzo 2023

[9] Pier Luigi Rotondo *Sai cosa sono gli attacchi BEC?* IBM thinkMagazine, giugno 2019

[10] *ENISA Threat Landscape 2023* ENISA European Union Agency for Cybersecurity, October 2023

[11] *Rapporto CERTFin 2023 - Come prevenire e contrastare attacchi informatici e frodi sui canali digitali* CERTFin, maggio 2023

[12] C. Hammond, O. Villadsen, K. Metrick *Stealthy WailingCrab Malware misuses MQTT Messaging Protocol* SecurityIntelligence.com, November 2023

[13] I. Chimino *Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy* SecurityIntelligence, June 2021

[14] *Macros from the internet are blocked by default in Office* Microsoft, December 2023

[15] IBM Security *Cost of a Data Breach Report 2023* July 2023

[16] *IBM X-Force Cloud Threat Landscape Report 2023* IBM, September 2023

[17] *Threat Landscape Scenario for the italian financial sector* CERTFin, July 2023

[18] MITRE Enterprise ATT&CK v12

[19] *Directive (EU) 2015/2366 of the European Parliament and of the Council* Official Journal of the European Union, November 2015

[20] 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/
[21] 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/
[22] S. Weeden *What makes FIDO and WebAuthn phishing resistant?*
[23] G. Badalucco *Identity security, la sicurezza basata sull'identità* Data Manager, settembre 2022
[24] *Quad9 Cybersecurity Trends and Insights* Quad9, May 2023
[25] 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
[26] Pier Luigi Rotondo *IBM X-Force: un passo avanti nella difesa dagli attacchi finanziari più evoluti* IBM thinkMagazine, febbraio 2018
[27] Pier Luigi Rotondo *Proteggere le risorse informative con la sicurezza cognitiva e con soluzioni in grado di adattarsi alle minacce future* ICT Security Magazine n.140/2016, October 2016
[28] Pier Luigi Rotondo *Sarà un anno sicuro, a patto che …* IBM thinkMagazine, marzo 2021 https://ibm.biz/2021sicuro
[29] Pier Luigi Rotondo *Shopping e saldi invernali più sicuri con i pagamenti elettronici* IBM thinkMagazine, dicembre 2019
[30] Pier Luigi Rotondo *Acquisti online? Ecco come farli in modo sempre più sicuro* IBM thinkMagazine, dicembre 2018

Cybersecurity in Sanità: tra aumento degli attacchi e innovazioni normative e tecnologiche

[A cura di: Sonia Montegiove, Manuela Santini, Sofia Scozzari, Anna Vaccarelli - Women For Security]

Il settore sanitario nel 2023 è il quarto più colpito dagli attacchi informatici di successo e di pubblico dominio[1], dopo Manufacturing, Professional / Scientific / Technical e ICT, con una percentuale sul totale degli incidenti censiti del 9%.

Prima di analizzare i cyber attacchi a cui il settore è più esposto può essere utile fare una brevissima panoramica sulle principali problematiche che affliggono la sanità.

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:** gli attacchi ransomware sono diventati sempre più comuni nel settore sanitario. I cybercriminali criptano i dati dei pazienti e richiedono un riscatto per sbloccarli, causando interruzioni nei servizi sanitari e mettendo a rischio la sicurezza dei pazienti.
3. **Accesso non autorizzato:** gli hacker possono tentare di ottenere accesso non autorizzato ai sistemi informatici della sanità per rubare informazioni o i dati dei pazienti.
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.
5. **Mancanza di formazione in materia di sicurezza:** il personale sanitario potrebbe non essere adeguatamente formato per riconoscere le minacce alla sicurezza informatica e prendere misure adeguate per prevenirle.
6. **Integrità dei dati medici:** gli attacchi informatici potrebbero compromettere l'integrità dei dati sulla salute delle persone, modificando i risultati dei test o i dettagli dei trattamenti.
7. **Normative e conformità:** il settore sanitario è soggetto a numerose normative e regolamenti in materia di sicurezza dei dati, tra cui GDPR e NIS2[2].

---

[1] Fonte: Hackmanac Global Cyber Attacks Report 2024

[2] https://www.garanteprivacy.it/il-testo-del-regolamento – https://digital-strategy.ec.europa.eu/it/policies/nis2-directive

I cyber attacchi verso il settore Healthcare nel 2023

L'Healthcare ha registrato 624 cyber attacchi a livello globale, oltre il doppio di quanto accaduto nel 2022 (304), con un trend in forte crescita che mostra quanto il settore sia sempre più esposto alle minacce informatiche.

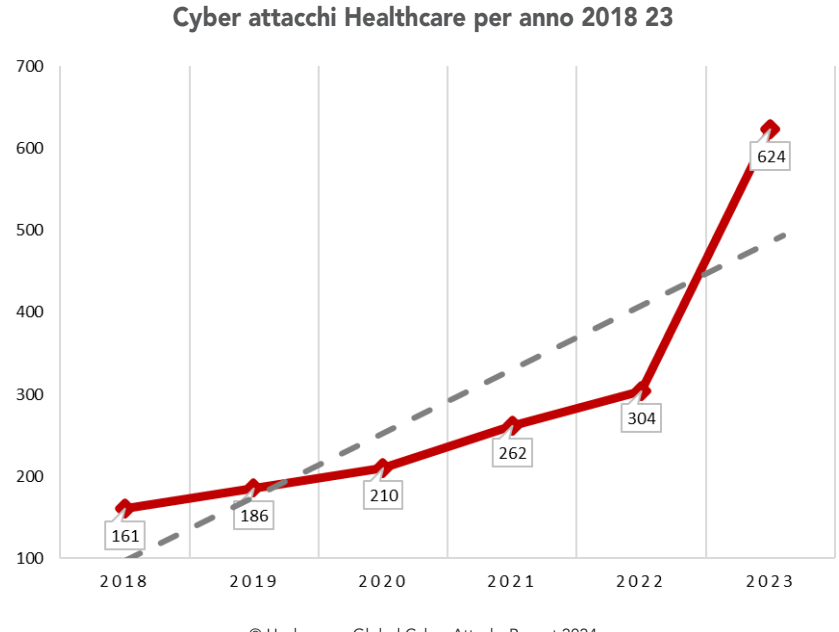


Figura 1 - Trend dei cyber attacchi nel settore sanitario nel periodo 2018 - 23

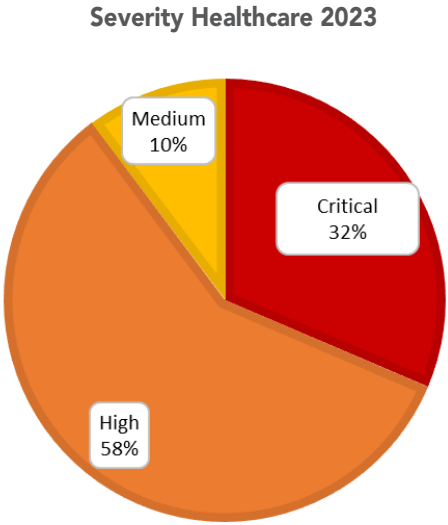
Se la criminalità informatica è, infatti, drammaticamente conscia che l'Healthcare deve minimizzare i disservizi in modo da poter offrire continuità nella sua funzione, d'altro canto non si può certamente affermare che questo settore stia investendo in maniera adeguata quando si tratta di Cybersecurity.

Da un'indagine svolta durante il primo semestre 2023 da NetConsulting cube[3] emerge che nel 46% dei casi manca una persona responsabile interamente dedicata alla Cybersecurity, con percentuali che peggiorano nella Sanità pubblica (52%), in Centro Italia (67%) e al Sud e Isole (63%). Dove invece una figura responsabile è presente, la struttura è esigua o con competenze non completamente adeguate.

[3] https://www.sanita24.ilsole24ore.com/art/aziende-e-regioni/2023-10-03/la-cybersecurity-come-presupposto-necessario-sviluppo-sanita-digitale-italia-101012.php?uuid=AF3w3K5

Uno scenario sconfortante alla luce delle minacce sempre più persistenti e mirate che affliggono il settore.

La quasi totalità degli incidenti (99%) hanno avuto una motivazione di stampo cybercriminale, mentre solo 5 cyber attacchi derivano da attività di *hacktivism*[4].



© Hackmanac Global Cyber Attacks Report 2024

Figura 2 - Severity dei cyber attacchi in ambito sanitario nel 2023

L'aspetto più preoccupante è però rappresentato dal fatto che il 90% degli attacchi ha avuto impatti gravi (58%) o gravissimi (32%) sulle strutture sanitarie colpite.

Anche in questo caso si tratta di un trend in crescita: nel 2022 gli impatti importanti si attestavano al 71%, con una percentuale di incidenti critici del 25%. Solo nel 10% degli incidenti si rilevano impatti medi, a dimostrazione del fatto che i cyber criminali che prendono di mira le strutture sanitarie puntano a creare seri danni per massimizzare la resa delle loro operazioni malevole.

A conferma di ciò, nel 2023 il Malware è la tecnica di attacco prediletta dalla criminalità informatica, utilizzato nel 57% dei cyber attacchi, con particolare riferimento ai ransomware[5].

[4] https://it.wikipedia.org/wiki/Hacktivism

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

A seguire, le "tecniche sconosciute" (perlopiù data breach[6], 20%), lo sfruttamento delle vulnerabilità (17%), incluse quelle non ancora note e risolte come gli 0-day[7].

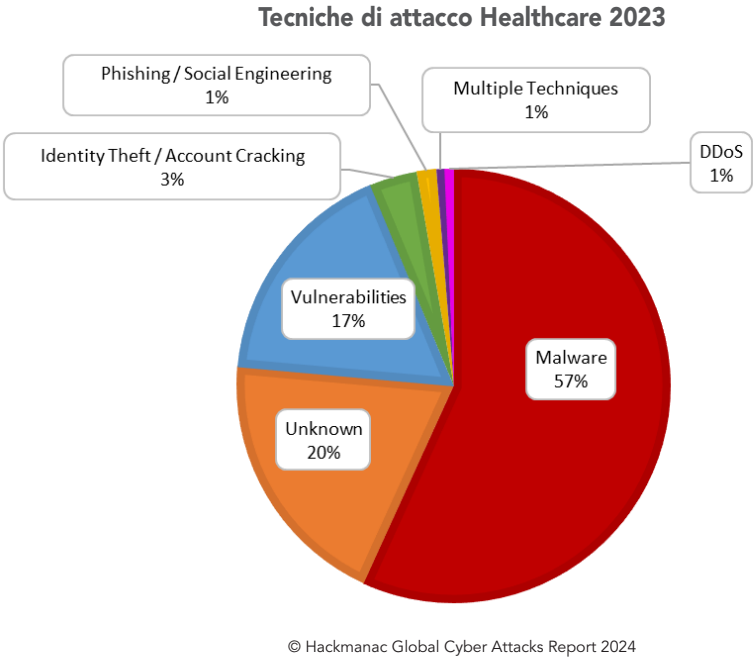


Figura 3 - Tecniche nei cyber attacchi del settore sanitario nel 2023

Rispetto agli anni precedenti, si nota come siano praticamente raddoppiati i cyber attacchi realizzati tramite malware (da 32% nel 2022), una conferma di quanto i codici malevoli, in particolare i ransomware, si stiano consolidando tra le minacce più efficaci per gli attaccanti.

Aumenta anche lo sfruttamento delle vulnerabilità, mentre diminuiscono le tecniche sconosciute, i furti di identità e il ricorso a phishing[8] e ingegneria sociale[9].

6 https://it.wikipedia.org/wiki/Data_breach

7 https://it.wikipedia.org/wiki/0-day

8 https://it.wikipedia.org/wiki/Phishing

9 https://it.wikipedia.org/wiki/Ingegneria_sociale

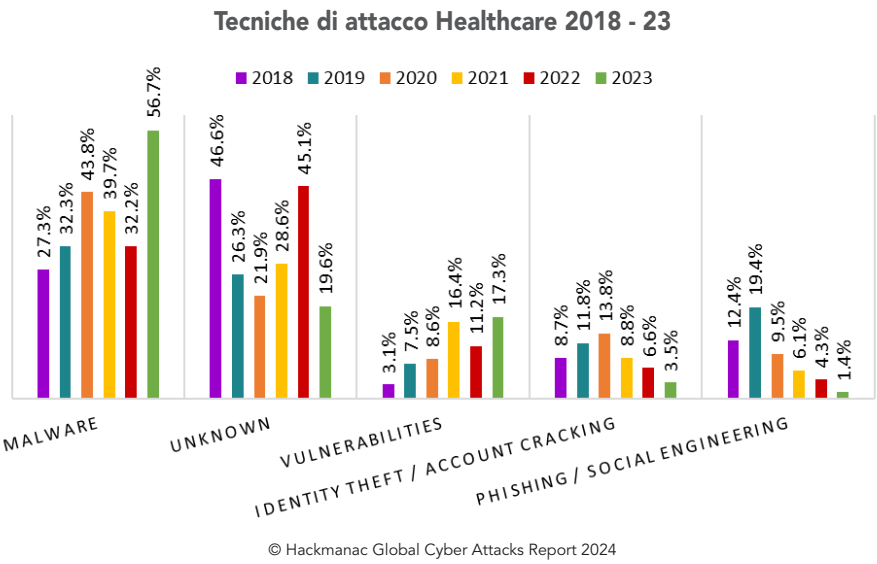


Figura 4 - Tecniche di attacco nel settore sanitario nel periodo 2018-23

La distribuzione geografica dei cyber attacchi nel settore sanitario, mostra l'America in testa con un 80% dei target colpiti, un dato che non stupisce alla luce delle normative che obbligano alla divulgazione degli incidenti che esistono da lungo tempo in questo Paese.

A seguire l'Europa con un 12% degli incidenti informatici, l'Asia (4%), l'Oceania (3 per cento) e l'Africa (1%).

Il confronto con gli anni precedenti mostra una diminuzione degli attacchi verso l'America (erano l'84% nel 2022), mentre aumentano quelli verso Europa (1 punto percentuale), Asia, Oceania (2 p.p. ciascuno) e Africa (1 p.p.).

Sparisce invece la quota di attacchi verso località multiple, a fronte del fatto che nel 2023 gli attacchi risultano maggiormente mirati.

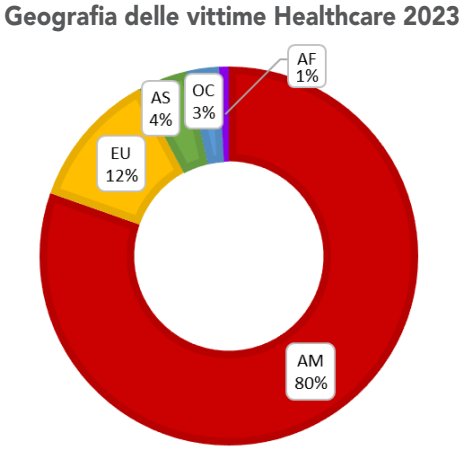


Figura 5 - Geografia delle vittime dei cyber attacchi in ambito sanitario nel 2023

La situazione italiana

In Italia i cyber attacchi di successo e di pubblico dominio verso il settore Healthcare sono aumentati fino quasi a raddoppiare nel 2023, dopo la stasi dei due anni precedenti, con una tendenza decisamente in salita evidenziata dal grafico in **Figura 6**.

Le motivazioni degli attacchi vedono sempre il Cybercrime come causa principale (93%) con un 7% extra di attività dovute ad Hacktivism che costituisce la novità dell'anno (**Figura 7**).

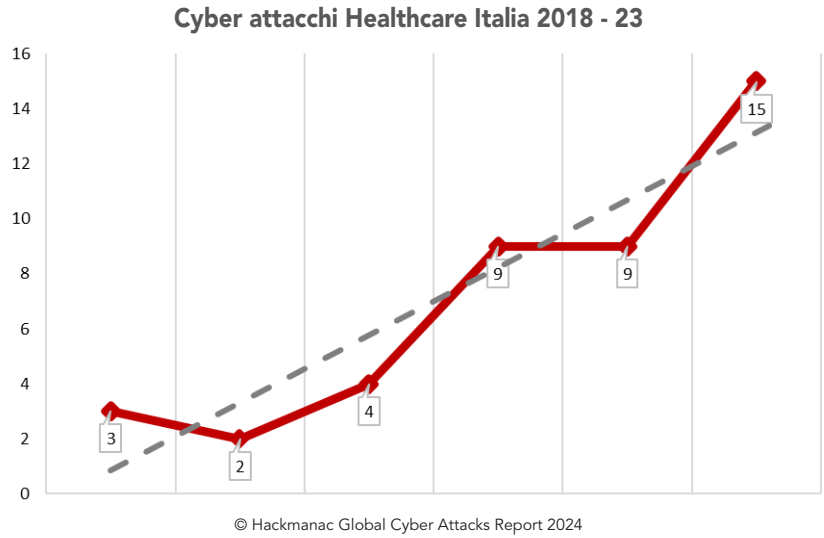


Figura 6 - Andamento dei cyber attacchi verso il settore sanitario in Italia nel periodo 2018 -23

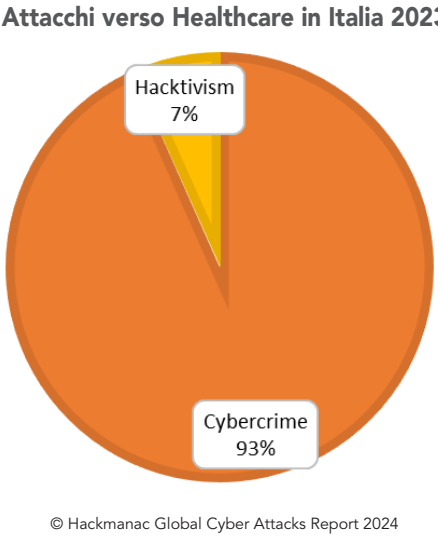


Figura 7 - Distribuzione degli attaccanti verso il settore sanitario in Italia nel 2023

Le tecniche di attacco mostrano un quadro molto più variegato rispetto agli anni precedenti: oltre all'onnipresente Malware (73% dei cyber attacchi dell'anno, in particolare ransomware), percentualmente di poco inferiore alla quota del 2022, e "Unknown" (tecniche sconosciute, per lo più *data breach*, 13%), in deciso calo (era 22% nel 2022), si aggiungono Phishing/Social Engineering e Web Attacks (7% ciascuno).

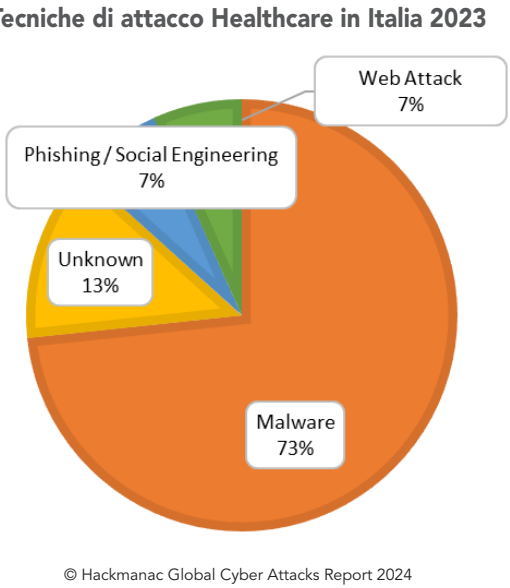


Figura 8 - Distribuzione delle tecniche di attacco verso il settore sanitario in Italia nel 2023

La gravità degli attacchi resta uno degli aspetti preoccupanti: nel 2023 il 93% degli incidenti di successo e divenuti di pubblico dominio verso il settore sanitario italiano hanno avuto impatti gravi o gravissimi.

Di questi, quasi due terzi degli attacchi (60%) hanno avuto severity critica, con impatti che si sono rivelati di particolare gravità considerata anche la priorità e la rilevanza del servizio svolto dalla vittima.

La novità rispetto agli anni precedenti è una porzione minimale di impatti medi (7%): se in passato si preferiva colpire il settore nel modo più incisivo possibile, nel 2023 una minima parte degli incidenti si "accontenta" anche di infliggere effetti lievi (Figura 9).

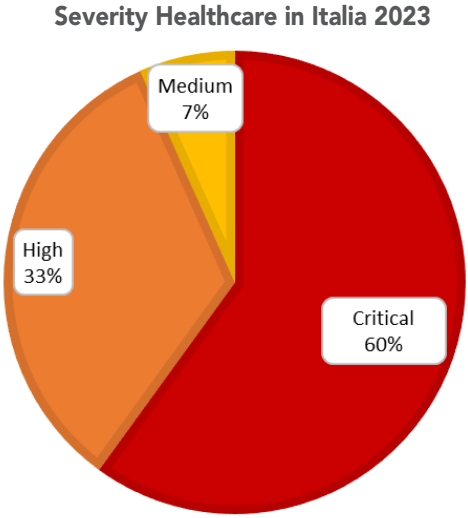


Figura 9 - Distribuzione della severity degli attacchi verso il settore sanitario in Italia nel 2023

I principali incidenti italiani

"Fragili dal punto di vista sia tecnico sia organizzativo. Si presentano così le aziende sanitarie italiane di fronte agli attacchi informatici, per lo più di tipo ransomware (cioè diretti al pagamento di un riscatto), dei gruppi criminali internazionali che, ormai da anni, le prendono di mira". Così Rosita Rijtano, in un articolo pubblicato da Guerre di Rete[10], descrive la situazione di ospedali e aziende sanitarie italiane che solo negli ultimi due mesi del 2023 - secondo quanto riportato dai siti ufficiali delle cyber gang - avrebbero visto esfiltrare e diffondere oltre **oltre 1,5 terabyte di dati sanitari (circa due milioni di file)**.

Tra queste, solo ultime in ordine di "apparizione", tre aziende sanitarie modenesi, Azienda Usl di Modena, Azienda ospedaliero-universitaria di Modena e Ospedale di Sassuolo Spa, e l'Azienda ospedaliera universitaria integrata di Verona. Per tutte l'attacco è avvenuto tramite ransomware che rende inaccessibili dati sanitari e amministrativi dei pazienti da poter riavere indietro a seguito di riscatto e rallenta i servizi erogati.

[10] https://www.guerredirete.it/i-dati-sanitari-di-migliaia-di-italiani-sono-ormai-online/

Verso una Cybersicurezza rafforzata: l'impatto della Direttiva NIS2 sul Settore Sanitario

Il settore sanitario sta vivendo una trasformazione digitale senza precedenti, con l'integrazione di tecnologie avanzate volte a migliorare la qualità delle cure e l'efficienza operativa. Gli incidenti in ambito sanitario, classificati perlopiù di gravità elevata mettono a rischio non solo i dati e la privacy dei pazienti ma anche la continuità delle cure e la sicurezza dei dispositivi medici.

La necessità di aumentare, non solo in ambito sanitario ma trasversalmente in tutti i settori, la capacità di risposta agli incidenti, così come la capacità di resilienza delle infrastrutture, nonché di raggiungere un elevato livello di cybersicurezza tra tutti gli Stati Membri, ha portato l'Unione Europea ad emanare nel 2016 la Direttiva NIS (Network and Information Security) e, nel dicembre 2022, ad aggiornarla con la Direttiva NIS2

La Direttiva NIS2 prevede obblighi in capo agli Stati Membri come la definizione di una Strategia nazionale per la cybersicurezza e la designazione di autorità competenti, SPOC (Single Point of Contact) e CSIRT (Computer Security Incident Response Team), nonché il ruolo di riferimento a livello europeo di ENISA[11]; la Direttiva NIS2 dovrà essere recepita dagli Stati Membri entro il 17 ottobre 2024.

Rispetto alla NIS1, la NIS2 estende il campo di applicazione a un maggior numero di settori e tipologie di aziende, comprese quelle del settore sanitario, includendo quindi settori e soggetti non coperti dalla precedente Direttiva. Sono inclusi tutti gli enti che operano nei Settori di Alta Criticità[12] e nei Settori Critici Addizionali[13], come delineato negli Allegati 1 e 2 della Direttiva, a condizione che rispettino determinati criteri dimensionali (anche se sono previste alcune eccezioni limitate). In particolare, tra i settori di Alta Criticità, rientra il settore sanitario, quali "*Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio* (20) —

[11] https://www.enisa.europa.eu/

[12] I "Settori di Alta Criticità" comprendono quei settori considerati essenziali per il mantenimento delle funzioni critiche della società e dell'economia. La compromissione o il malfunzionamento delle entità operative in questi settori potrebbe avere gravi conseguenze sulla salute pubblica, la sicurezza, la sicurezza economica o sociale, o su qualsiasi combinazione di questi aspetti. Alcuni esempi di settori di alta criticità includono, ma non sono limitati a, energia, trasporti, acqua potabile, sanità, infrastrutture digitali, finanza, ecc.

[13] I "Settori Critici Addizionali" si riferiscono a settori che, pur non essendo classificati come di alta criticità, sono comunque importanti per la resilienza economica e sociale. La perturbazione o il malfunzionamento delle entità in questi settori potrebbe avere un impatto significativo, sebbene forse non immediatamente grave, sulla società o l'economia. Questi settori includono, ad esempio, il settore alimentare, alcune parti del settore manifatturiero, e altri.

Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio (21)"

Tra i Settori Critici Addizionali, invece troviamo i "*Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio* (4) *e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio* (5) *ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva*"

La NIS2 introduce una nuova differenziazione tra soggetti, distinguendo tra Soggetti Essenziali, che operano nei Settori di Alta Criticità, e Soggetti Importanti che operano nei Settori Critici Addizionali o in altri settori non classificati come di Alta Criticità, ma la cui perturbazione potrebbe comunque avere un impatto significativo sulla società o l'economia.

Viene quindi superata quella fra Operatori di Servizi Essenziali[14] e Fornitori di Servizi Digitali[15] propria della NIS1, ritenuta obsoleta. Questa nuova categorizzazione permette di ridurre la discrezionalità per gli Stati Membri nel definire i soggetti in perimetro, i requisiti di sicurezza e le modalità di segnalazione degli incidenti favorendo uniformità.

In particolare, la NIS2 ha come obiettivo di assicurare uniformità tra Stati Membri in termini di misure di sicurezza previste e di risorse disponibili alle autorità di controllo e mira a rafforzare la condivisione di informazioni tra Stati Membri.

I requisiti della NIS2 possono essere raggruppati nei seguenti macro-ambiti:

- **gestione dei rischi,** che richiama i concetti di Risk-based approach e Risk-based thinking. Le aziende sono chiamate ad implementare ed adottare una metodologia di analisi del rischio (approccio multi-rischio) e misure di sicurezza idonee a mitigare tali rischi implementando controlli specifici per garantire la sicurezza dei sistemi informatici "*in linea con le norme europee e internazionali, come quelle*

[14] Gli Operatori di Servizi Essenziali sono entità che forniscono servizi considerati essenziali per il mantenimento di funzioni sociali ed economiche critiche.

[15] I Fornitori di Servizi Digitali includono tre categorie specifiche di servizi: piattaforme di marketplace online, motori di ricerca online e servizi di cloud computing.

di cui alla serie ISO/IEC 27000". Esempi di questi controlli sono backup, controllo degli accessi, Multi Factor Authentication (MFA), crittografia, buone pratiche di igiene informatica, sicurezza delle risorse umane. Le aziende sono inoltre chiamate a valutare costantemente l'efficacia delle misure di sicurezza adottate;

- **gestione della continuità operativa,** per garantire che le attività aziendali possano proseguire senza interruzioni significative, anche in caso di incidenti o emergenze. Un elemento chiave di questa gestione è ottenere una comprensione dettagliata dello stato attuale delle operazioni dell'azienda e delle sue necessità specifiche. Questo può essere realizzato, in particolare, attraverso l'implementazione di una Business Impact Analysis (BIA), al fine di capire in che misura le varie funzioni aziendali si affidano a sistemi, applicazioni e dati per operare efficacemente. In aggiunta alla Business Impact Analysis, è essenziale condurre un assessment, ovvero una valutazione sull'adeguatezza del sistema informativo esistente per supportare i requisiti identificati dalla BIA. In particolare, l'assessment dovrebbe esaminare diversi aspetti del sistema informativo, inclusa la sua resilienza, capacità di recupero, e la presenza di piani di continuità e di disaster recovery adeguati;
- **gestione degli incidenti,** in particolare un processo che permetta alle aziende di rilevare, gestire e segnalare tempestivamente gli incidenti, nonché avere un piano di risposta e gestione delle crisi. Questo approccio mira a migliorare la risposta agli incidenti ma anche a facilitare la condivisione di informazioni sulle minacce, potenziando così la resilienza collettiva;
- **governance,** le aziende dovranno adottare modelli organizzativi per la gestione della cybersecurity e responsabilizzare gli organi di gestione nonché prevedere attività formative per quest'ultimi e per tutti i dipendenti;
- **sicurezza della supply chain,** intesa come la sicurezza dell'intera catena di approvvigionamento nonché la sicurezza dei rapporti tra ciascun soggetto e i suoi diretti fornitori.

Quanto sopra richiederà un impegno significativo in termini di risorse e competenze specialistiche, presentando sfide particolari per le piccole e medie imprese (PMI) del settore.

In attesa della legge di recepimento della normativa NIS2, le aziende possono iniziare ad anticipare alcune delle attività più onerose, in modo da non doverle affrontare in tempi più stretti, nell'ambito delle attività complessive di adeguamento entro i termini che saranno fissati dalla normativa di recepimento; in particolare quelle di governance, gestione dei fornitori, gestione degli incidenti e di gestione della continuità operativa.

Analizzando gli interventi propedeutici all'adeguamento alla Direttiva NIS2, troviamo efficace iniziare ad eseguire attività di assessment, cioè attività di verifica in merito allo stato di adeguatezza dell'attuale modello di governo della cybersecurity (organigramma, ruoli e responsabilità). Le attività di assessment riguardano inoltre l'analisi della necessità di attività di formazione specifiche, dell'adeguatezza dei contratti con i fornitori, dell'efficacia dei processi di Demand Management e Incident Management, della presenza di una Business Impact Analysis (BIA) e dell'adeguatezza del sistema informativo a supportare i requisiti individuati dalla BIA.

Un'attività di adeguamento completa sarà possibile nel momento in cui tutte le informazioni necessarie saranno disponibili. Pertanto, per alcune attività è necessario attendere il recepimento della Direttiva al fine di ottenere le relative prescrizioni di dettaglio.

Le entità in perimetro NIS2 saranno chiamate a rispettare requisiti di cybersicurezza, senza differenze tra soggetti essenziali e importanti. Invece, le principali distinzioni si trovano nella rigidità delle misure di controllo e delle sanzioni applicate: le entità essenziali affrontano verifiche più rigide e sanzioni più gravose rispetto alle entità importanti. La logica di applicazione delle sanzioni è molto simile a quelle che abbiamo visto in altre normative. L'entità della sanzione, in caso di inadempienza, varia da *un massimo di almeno 10.000.000 EUR o a un massimo di almeno il 2% del totale del fatturato mondiale annuo* per le entità essenziali e *un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4% del totale del fatturato mondiale annuo per i* soggetti importanti.

Inoltre, eventuali non conformità di un'entità essenziale, nei casi più gravi, può comportare la sospensione temporanea di "*un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale*" oppure "*chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto*".

In conclusione, la Direttiva NIS2 così come le altre norme ad essa collegate (Regolamento DORA, Direttiva CER sui soggetti critici, Cyber Resilience Act, ecc.) rappresentano uno strumento importante con cui l'Unione Europea vuole guidare le organizzazioni verso una resilienza adeguata ad affrontare le difficoltà e le sfide dello scenario geopolitico attuale e futuro.

Intelligenza Artificiale: opportunità e limiti

L'Intelligenza Artificiale (IA) è una tecnologia ormai pervasiva e utilizzata in diversi settori lavorativi o di vita quotidiana, compreso quello della salute, ma come per ogni innovazione tecnologica ci sono vantaggi e svantaggi e, in particolare, è importante considerare gli aspetti legati alla sicurezza e gestione del rischio.

Gli ambiti di applicazione dell'IA nella sanità sono molteplici: quello di cui si parla di più è l'analisi di immagini diagnostiche, che riporta al medico il risultato del confronto di enormi quantità di immagini, per analizzare le quali il medico impiegherebbe giorni, consentendo quindi di risparmiare tempo e formulare più tempestivamente la diagnosi.

Un altro settore in cui l'IA è di grande aiuto è quello amministrativo: è stato stimato che in Italia un medico dedica 23 ore su 40 alla compilazione di documenti. Alcuni essi potrebbero essere redatti o completati con i dati corretti da una IA appositamente addestrata. Ne esistono alcune, in via sperimentale, che analizzano la conversazione tra medico e paziente e formulano per il medico una prima bozza di relazione che riguarda il paziente.

Esistono anche IA in grado di creare cartelle di pazienti con dati "sintetici" (che imitano quelli reali) a scopo di studio su campioni di pazienti. Sono strumenti ancora sotto test, in via di sperimentazione e verifica ma segnerebbero un importante cambiamento nell'approccio alla medicina in fase sperimentale. Ad alcune IA altamente specializzate viene affidato il compito di creare nuovi farmaci, potendo ottenere risultati in tempi molto più brevi rispetto alla elaborazione degli umani. Inoltre, l'IA è "installata" in molti dispositivi e macchine medicali. In uno scenario futuro si ipotizzano IA che possono dare informazioni mediche affidabili, sempre complementari alla presenza di personale medico, ma che potrebbero alleviare le difficoltà in quei Paesi dove l'assistenza sanitaria è sporadica e non uniformemente garantita sul territorio. L'IA generativa (tipo ChatGPT), opportunamente addestrata, potrebbe anche fornire supporto per la diagnosi, per il monitoraggio del paziente, per la sua educazione sanitaria, per suggerire terapie e,come chatbot, fornire ai pazienti informazioni e assistenza sanitaria di base.

Tuttavia, in tutti questi casi, si devono garantire precisi livelli di sicurezza, sia per quanto riguarda la riservatezza dei dati trattati (sono i dati dei pazienti e delle loro patologie) sia per eventuali vulnerabilità a cui vengono esposti i sistemi che ne fanno uso.

A questo proposito si stanno delineando precise normative: l'Organizzazione mondiale della Sanità ha emanato a ottobre un documento che dà precise indicazioni, il Regulatory considerations on Artificial Intelligence for health, elenca le principali regole a cui l'IA deve sottostare per garantire un uso sicuro, efficace e responsabile della stessa in ambito sanitario. Le sei principali sono:

1. **Documentazione e trasparenza** (Documentation and transparency): per promuovere la fiducia verso questa nuova tecnologia, la pubblicazione sottolinea l'importanza della trasparenza, che passa anche dal documentare l'intero ciclo di vita del prodotto e dal controllo dei processi di sviluppo.
2. **Gestione del rischio e approccio al ciclo di vita dello sviluppo dei sistemi di AI** (Risk management and artificial intelligence systems development lifecycle approach): per la gestione del rischio, temi quali "apprendimento continuo", "modelli di formazione" e "minacce alla sicurezza informatica" devono essere affrontati in modo esaustivo, usando modelli completi, ma più semplici possibile.
3. **Destinazione d'uso e validazione analitica e clinica** (Intended use and analytical and clinical validation): la convalida esterna dei dati e dalla chiarezza sull'impiego pratico di IA in ambito sanitario possono garantire la sicurezza e una regolamentazione omogenea e trasparente.
4. **Qualità dei dati** (Data Quality): è necessario un impegno costante per la qualità dei dati così da garantire che i sistemi non amplifichino gli errori, ad esempio attraverso una rigorosa valutazione dei sistemi prima del loro rilascio.
5. **Privacy e protezione dei dati personali e sensibili** (Privacy and data protection) – Normative come il GDPR in Europa e l'HIPAA (Health Insurance Portability and Accountability Act) negli Stati Uniti d'America pongono delle sfide impegnative su come affrontare la cybersecurity in sanità, in particolare in relazione alla privacy, al consenso al trattamento dei dati e alla loro protezione.
6. **Coinvolgimento e collaborazione** (Engagement and collaboration): promuovere il coinvolgimento e la collaborazione di tutti i soggetti presenti nel settore, quali organismi di regolamentazione, partner governativi, operatori economici e anche i pazienti, contribuisce a mantenere i prodotti/servizi conformi alle normative durante l'intero ciclo di vita.

Il 9 dicembre 2023 l'Unione europea ha approvato l'AI Act, che cerca di regolare lo sviluppo e l'utilizzo dell'intelligenza artificiale in Europa. Queste norme riguardano anche la sanità e in particolare, mentre il GDPR si focalizza maggiormente sulla protezione dei dati personali, l'AI Act si concentra sulla trasparenza e il rispetto dei diritti

fondamentali quando si usano sistemi di IA. Raccomanda l'utilizzo di una quantità minima di dati e il consenso informato ed esplicito al loro trattamento da parte dei pazienti. Inoltre, ha un impatto anche sul software dei dispositivi medici che utilizzano IA, interessando anche la supply chain. Bisogna ricordare che i dispositivi medici erano già soggetti (e continuano ad esserlo) al Medical Device Regulation (MDR) con il quale l'AI Act deve essere armonizzato; questo consentirà ai produttori di dispositivi medici di attribuirgli la giusta categoria di rischio, sia in base al loro utilizzo sia in base al software che di cui sono provvisti, coerentemente con entrambi i regolamenti.

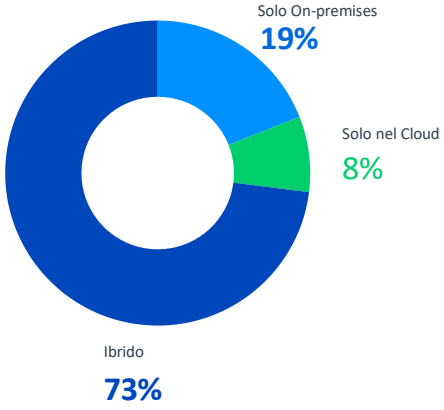
Le tendenze della Hybrid Security per il 2024

(A cura di Maurizio Tagliorettì e Dirk Schrader, Netwrix)

L'adozione del cloud è in pieno svolgimento, con ben l'81% delle organizzazioni in tutto il mondo che ora utilizza almeno un ambiente cloud. Per tenere il passo con l'evoluzione della sicurezza IT sia on-premise che nel cloud, Netwrix Research Lab ha intervistato 1.610 professionisti IT provenienti da 106 paesi tramite un questionario online nel mese di febbraio del 2023 e ha confrontato i risultati con i suoi precedenti report sulla sicurezza dei dati nel cloud del 2022, 2020 e del 2019 nonché il relativo report sulle tendenze IT del 2020. Il risultato di questo lavoro è il presente report che raccoglie suggerimenti ed indicazioni e suggerimenti per le organizzazioni per guidarle a concertare i propri sforzi di sicurezza su ciò che conta davvero.

Architettura IT

Nel 2023, con il lavoro remoto e ibrido ormai all'ordine del giorno, non sorprende che il cloud sia parte integrante dell'infrastruttura IT per la maggior parte delle organizzazioni.



69%

di coloro che attualmente rimangono solo on-premise, prevede di adottare tecnologie cloud.

37%

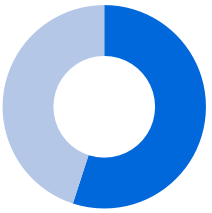
di chi attualmente rimane solo on- premise prevede di adottare tecnologie cloud entro i prossimi 12 mesi.

Architettura IT dell'organizzazione

In media, le organizzazioni riferiscono che il 44% dei loro carichi di lavoro è già nel cloud e si aspettano che tale quota aumenti fino al 55% entro l'inizio del 2024.

Qual è la percentuale dei carichi di lavoro della tua organizzazione che sono già nel cloud?

Quale percentuale dei carichi di lavoro della tua organizzazione sarà pianificata nel cloud tra 12 mesi?



Secondo i nostri intervistati, l'adozione del cloud lo scorso anno è progredita più lentamente di quanto previsto. La quota media dei carichi di lavoro nel cloud è aumentata dal 41% al 44%, e non al 54% come era stato previsto dagli intervistati del sondaggio del 2022.

Il rallentamento dell'adozione del cloud dimostra che le organizzazioni stanno affrontando questa sfida con diligenza. Il passaggio al cloud non è una cosa semplice come il copia e incolla. Richiede un'attenta pianificazione, gestione delle aspettative e risorse sufficienti per testare e reingegnerizzare i processi. I tentativi forzati di accelerare la migrazione al cloud possono portare a un notevole superamento delle spese e possono persino richiedere una costosa riprogettazione dell'architettura se i problemi vengono rilevati più avanti nel processo. Di conseguenza, è fondamentale utilizzare strumenti di sicurezza che aiutino a proteggere sia i sistemi on- premise che quelli nel cloud al fine di evitare che si verifichino degli incidenti di sicurezza proprio quando l'ambiente IT è nel suo stato più vulnerabile, cioè quando vi è in atto un cambiamento.

Nel 2022, infatti, il principale fattore che ha portato al rallentamento dell'adozione del cloud, secondo il 41% delle organizzazioni, è stata l'integrazione con l'ambiente IT esistente, e solo l'11% degli intervistati ha affermato che si sarebbe mosso verso il cloud con la rapidità necessaria.

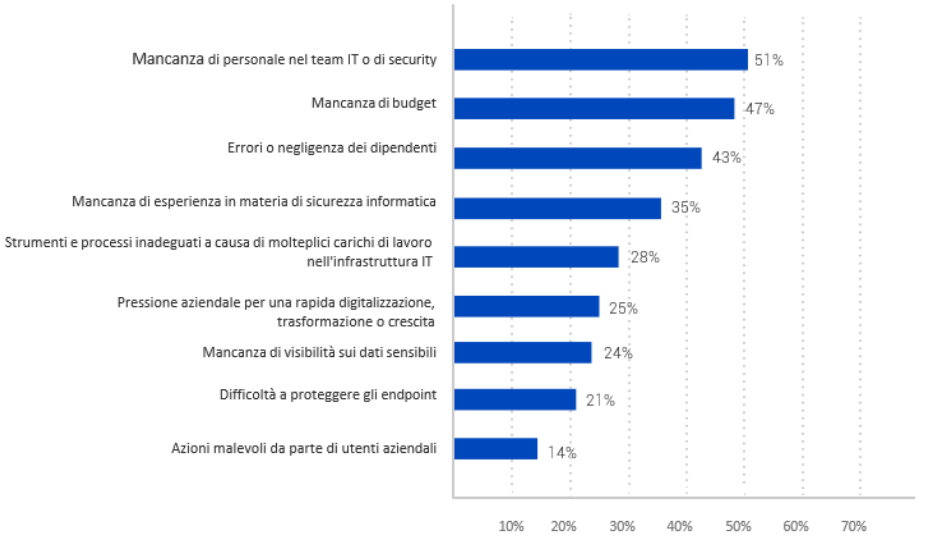
I progetti IT generalmente tendono a richiedere più tempo del previsto e la migrazione al cloud non fa eccezione. Il diavolo sta nei dettagli: le aziende hanno accumulato una significativa infrastruttura on-premise e passare al cloud mantenendo le operazioni aziendali non è facile. Il software come servizio (SaaS) è in genere l'approccio più conveniente, ma raramente i fornitori offrono soluzioni SaaS che siano completamente equivalenti ai loro prodotti on-premise. Anche i percorsi di migrazione non

sono semplici; le applicazioni aziendali possono essere profondamente integrate con altri sistemi, rendendo la migrazione costosa e dirompente. Un approccio lift-and-shift potrebbe sembrare il più semplice perché i prodotti on-premise possono essere eseguiti su macchine virtuali in un data center cloud, ma richiede ancora la migrazione e può comportare un aumento dei costi di hosting. Di conseguenza, le aziende entrano rapidamente in modalità ibrida con applicazioni native del cloud come e-mail e CRM, ma devono comunque mantenere l'infrastruttura on-premise per strumenti la cui migrazione è difficile o costosa.

Le sfide alla sicurezza

Il grafico precedente mostra le sfide alla sicurezza che le organizzazioni devono affrontare nel loro complesso. Quando abbiamo chiesto agli intervistati quali fossero le principali sfide in ciascuna delle due parti della loro infrastruttura IT, sono emerse chiare differenze. In particolare, la principale preoccupazione per le infrastrutture cloud non è la carenza di personale IT, ma la mancanza di budget, e gli errori dei dipendenti rappresentano meno un problema di sicurezza nel cloud che in locale.

Quali sono le sfide più grandi che devi affrontare mentre cerchi di garantire la sicurezza dei dati?



Quando un team IT è a corto di personale, ogni minuto lavorativo è fondamentale. Lo stress e le lunghe ore che ne derivano possono portare ad un affaticamento e possibilmente ad errori, che non sono mai una buona cosa. Un modo per affrontare questa

sfida è quello di automatizzare le attività di routine come la gestione degli accessi e la gestione dei gruppi di Active Directory. Altre misure includono l'utilizzo di prodotti di sicurezza maturi che producono meno avvisi di falsi positivi e l'affidamento ad un gruppo selezionato di fornitori che dispongano di un ampio portafogli e di un team di supporto unificato. Le organizzazioni più piccole potrebbero voler collaborare con un fornitore di servizi gestiti (MSP) per colmare le lacune.

Nel Cloud Vs On-Premises

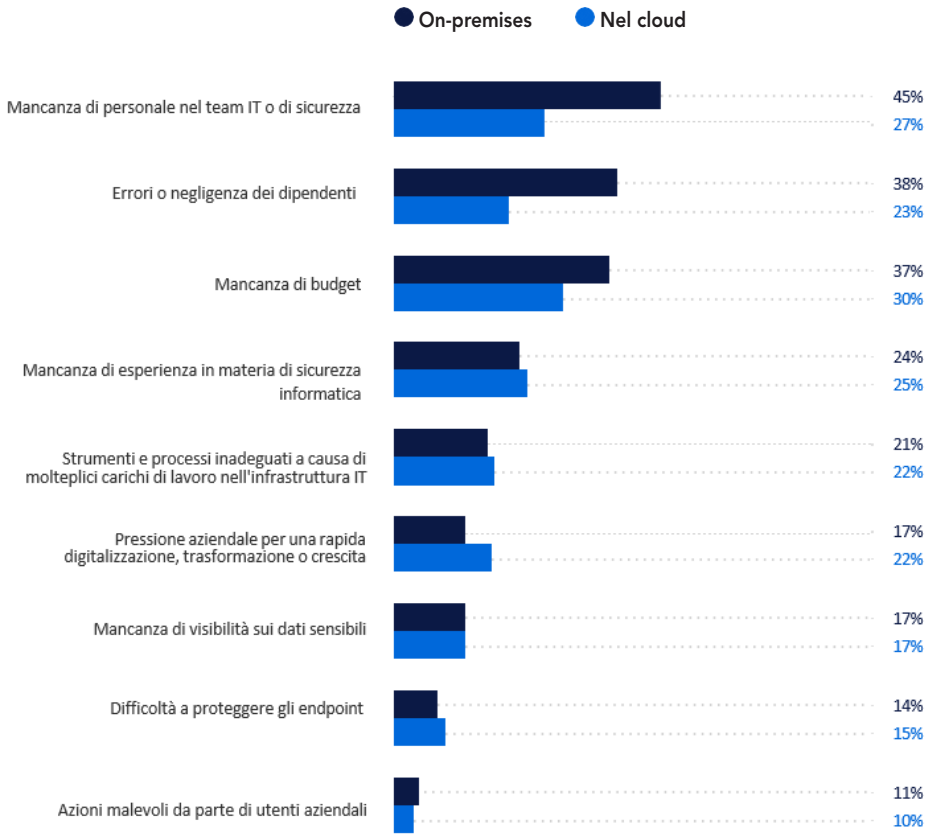
Quali sono le sfide che le organizzazioni devono affrontare per garantire la sicurezza dei dati, indipendentemente dal fatto che i dati siano nel cloud o on-premise? Abbiamo chiesto agli intervistati di stabilire le priorità per ciascuna parte della loro infrastruttura IT per chiarire le distinzioni. L'indagine ha rivelato che la principale preoccupazione per l'infrastruttura cloud è la mancanza di budget. Al contrario, la carenza di personale e gli errori dei dipendenti in termini di sicurezza nel cloud non sono visti come un peso per le loro risorse locali.

Passare al cloud spesso significa che l'attività IT come la sicurezza fisica, il networking e l'applicazione di patch vengono affidate in outsourcing al provider cloud; quindi, non sorprende che la carenza di personale nei team IT interni sia meno un problema di sicurezza per i carichi di lavoro basati su cloud. In generale, le soluzioni SaaS possono alleggerire più attività IT rispetto alle tecnologie Platform-as-a-Service (PaaS) o Infrastructure-as-a-Service (IaaS).

Gli errori o la negligenza dei dipendenti rappresentano la principale preoccupazione per le organizzazioni che si basano sul cloud

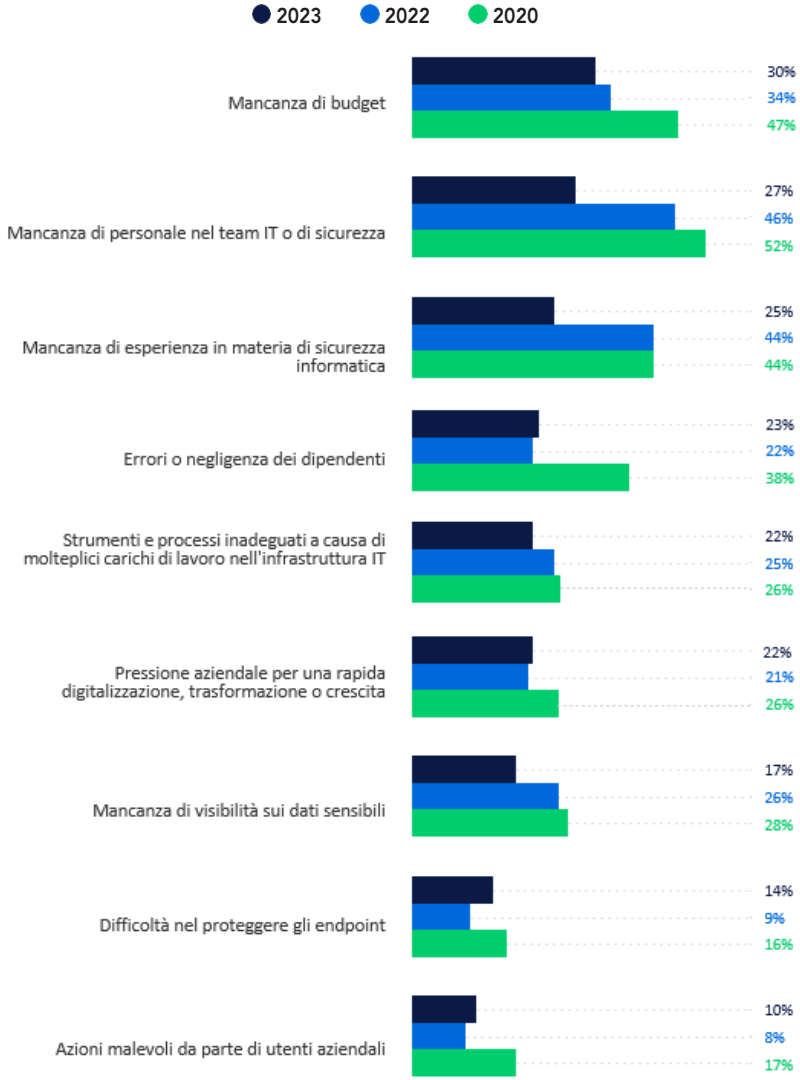
La mancanza di budget è la preoccupazione principale per le organizzazioni esclusivamente on-prem

Quali sono le sfide più grandi che devi affrontare mentre cerchi di garantire la sicurezza dei dati?



I cambiamenti delle sfide legate alla sicurezza del cloud nel tempo

Quali sono le sfide principali che devi affrontare nel cercare di garantire la sicurezza dei tuoi dati nel cloud?



Abbiamo confrontato i risultati del sondaggio di quest'anno con quelli del 2022 e del 2020. È stato interessante notare che le principali aree di preoccupazione sono rimaste invariate (mancanza di personale IT, budget e competenze in materia di sicurezza informatica insufficienti) tuttavia, molti meno intervistati ora si preoccupano di queste sfide.

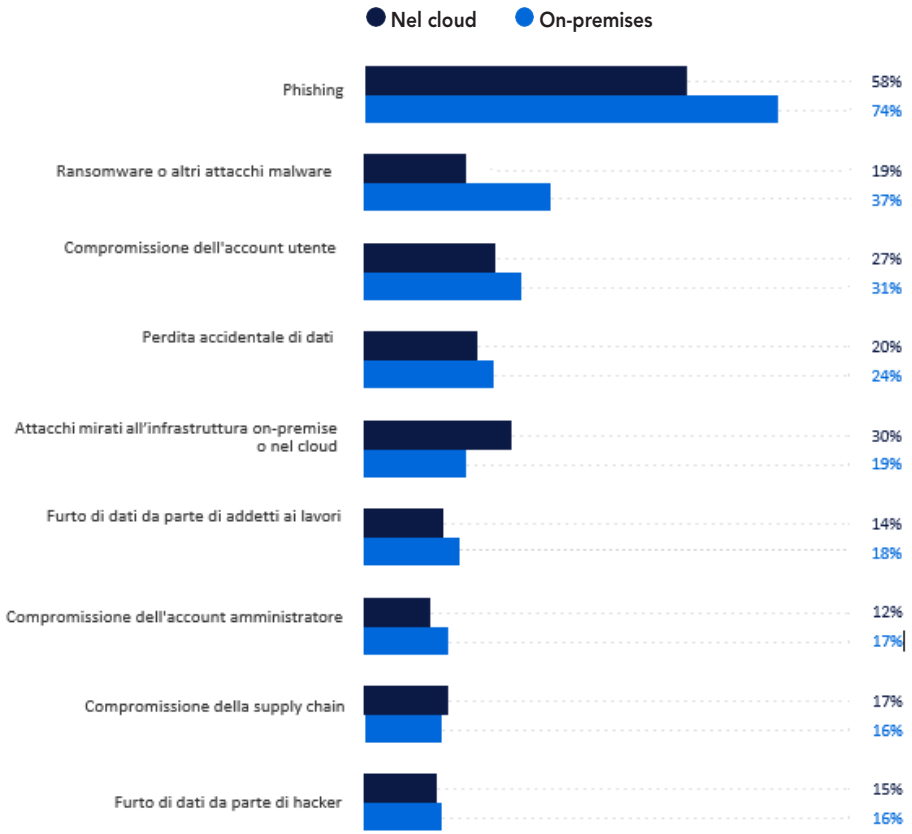
Nel 2022, più della metà (51%) degli intervistati ha indicato il miglioramento della sicurezza come obiettivo primario nell'adozione del cloud. I risultati del sondaggio di quest'anno mostrano il raggiungimento di questo obiettivo: i team IT sono più sicuri della sicurezza del proprio cloud in quanto hanno aumentato le proprie competenze e capacità in materia.

Tuttavia, l'incoerenza nella copertura delle strutture cloud e on-premise rappresenta ancora un problema. Per evitare lacune nella sicurezza e garantire una chiara visibilità, è fondamentale disporre di strumenti in grado di monitorare l'intero ambiente IT. Ad esempio, è importante utilizzare un prodotto IAM in grado di integrare le applicazioni cloud nei flussi di lavoro di provisioning e deprovisioning per unificare la gestione degli accessi cloud e on-premise.

Incidenti di sicurezza
Nel Cloud Vs On Premises

Il 68% delle organizzazioni ha subito un attacco informatico negli ultimi 12 mesi. I professionisti della sicurezza sanno che è impossibile raggiungere la piena sicurezza informatica, il che significa che il restante 32% ha avuto un anno molto fortunato o semplicemente non ha ancora individuato l'incidente. Abbiamo chiesto a coloro che hanno subito un attacco informatico di fornire maggiori dettagli su quanto accaduto. I risultati mostrano che l'infrastruttura on-premise subisce più attacchi informatici rispetto a quella nel cloud. La differenza più evidente riguarda gli attacchi ransomware ed altri malware, segnalati da quasi il doppio degli intervistati per gli ambienti on-premise (37%) rispetto al cloud (19%).

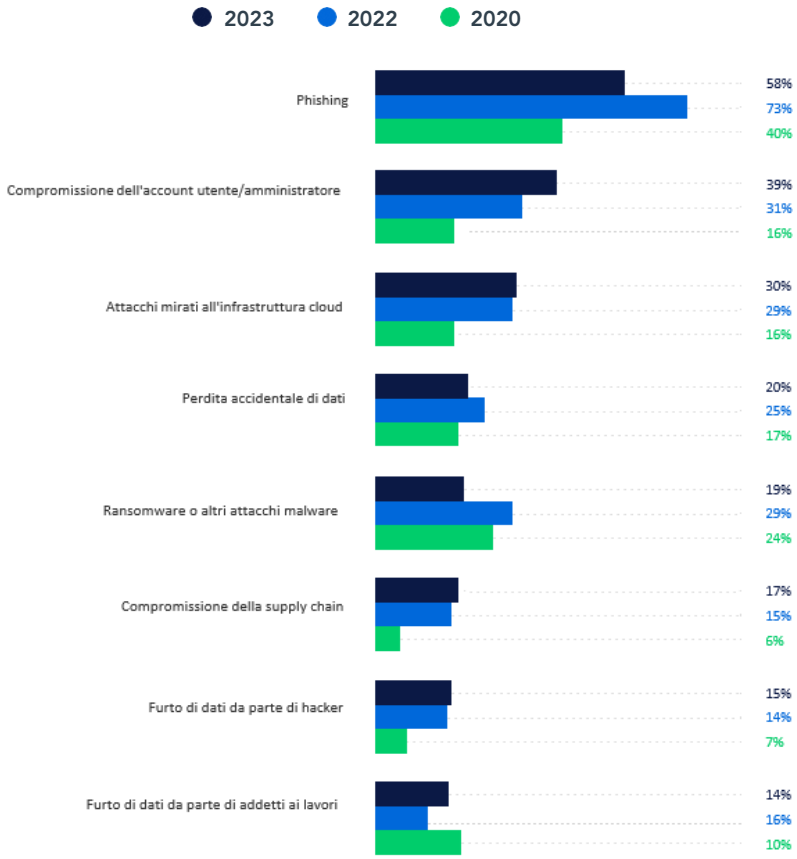
Incidenti di sicurezza più comuni



Incidenti di sicurezza nel cloud

Abbiamo anche confrontato i risultati di quest'anno sugli incidenti di sicurezza nel cloud con quelli del 2020 e del 2022. Sebbene il phishing rimanga la tipologia di incidente più comune, c'è stato comunque un movimento anche tra le altre tipologie di incidenti. La compromissione degli account utente ed amministratore, ad esempio, è ora al secondo posto, con il 39% degli intervistati che l'ha sperimentata nel 2023 rispetto al 31% nel 2022 e solo al 16% nel 2020.

Le tipologie di dati sensibili archiviati nel cloud da parte delle organizzazioni

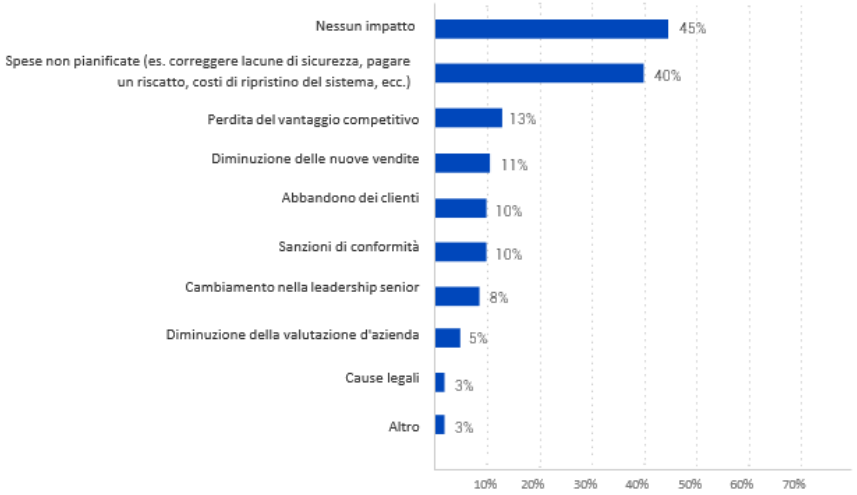


Gli aggressori cercano di compromettere gli account amministrativi perché possono usarli per diffondersi lateralmente ad altri sistemi. Ottenere un accesso privilegiato alle applicazioni ed alle infrastrutture business-critical, come i sistemi di pianificazione delle risorse aziendali (ERP) e di gestione delle relazioni con i clienti (CRM), offre agli aggressori la possibilità di distruggere i dati sensibili o di tenerli "in ostaggio" a scopo di riscatto. Di conseguenza, è fondamentale attuare un approccio zero standing privilege che consenta di avere account amministratore solo per il tempo necessario al completamento di un'attività specifica, riducendo così al minimo il rischio che un utente malintenzionato possa ottenere un accesso privilegiato.

Le conseguenze di una violazione dati

Alcuni attacchi informatici hanno conseguenze disastrose, incluso l'arresto delle operazioni per un periodo prolungato che, nei casi più gravi, può portare, purtroppo, al fallimento di un'organizzazione. Fortunatamente, la maggior parte delle organizzazioni riesce a riprendersi da un attacco subito. Infatti, il 45% degli intervistati che hanno subito un attacco informatico afferma di non aver avuto un impatto significativo sulla propria organizzazione. Tuttavia, il 40% ha dovuto affrontare spese non pianificate e circa 1 su 10 ha riportato altre gravi conseguenze, come la perdita del vantaggio competitivo, il calo delle vendite o l'abbandono dei clienti.

Quali sono le conseguenze di una violazione dati?

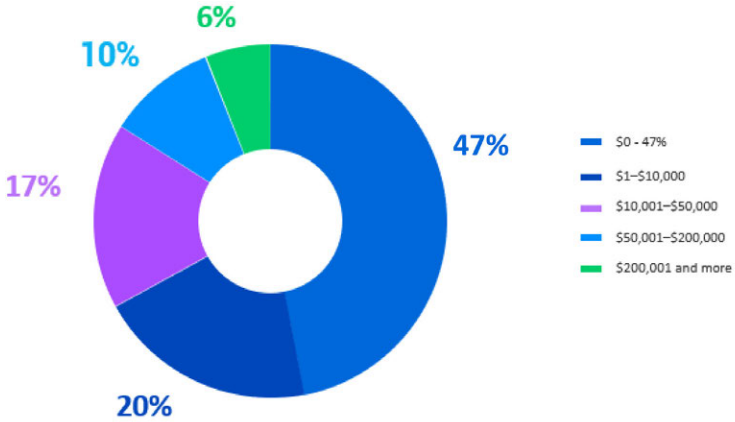


40% *delle organizzazioni che ha subito una violazione dei dati ha dovuto affrontare spese non pianificate.*

I costi di una violazione

Anche se non tutti gli attacchi comportano danni finanziari, alcuni possono essere piuttosto costosi. Infatti, quasi 1 organizzazione su 6 (16%) stima che il danno finanziario derivante dalle minacce informatiche sia pari ad almeno 50.000 dollari.

Danno finanziario stimato dovuto alle minacce informatiche

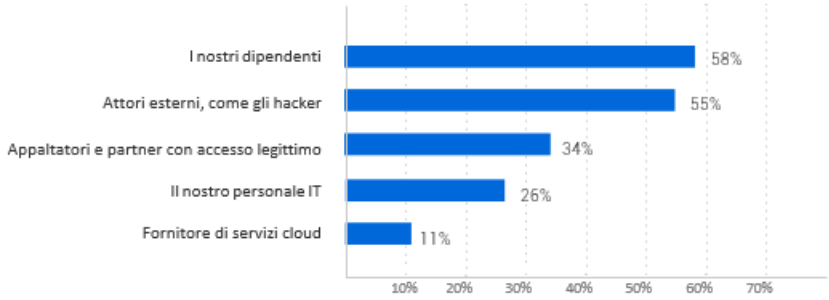


Quasi un'organizzazione su 6 ha riportato danni finanziari pari ad almeno 50.000 dollari derivanti dalle minacce informatiche.

Gli attori malevoli

per costruire un'architettura di sicurezza efficace, è fondamentale valutare chi possa rappresentare una minaccia. Dal sondaggio emerge che i professionisti IT sono preoccupati sia dei propri dipendenti che degli attori malevoli in egual modo.
Considerando che il 43% degli intervistati ha citato gli errori e/o la negligenza dei propri dipendenti come la principale sfida alla sicurezza dei dati, non sorprende che la minaccia interna sia inclusa tra le preoccupazioni principali.

Chi rappresenta il rischio maggiore per la sicurezza dei tuoi dati?



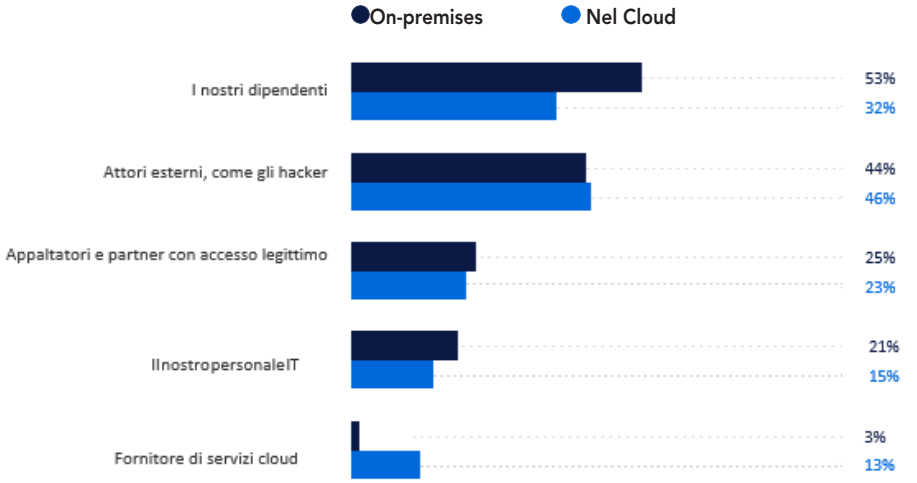
Alcuni suggerimenti dei nostri esperti su come rendere più semplice la sicurezza per gli utenti finali ed evitare soluzioni rischiose

- Applica il principio del privilegio minimo con uno strumento di governance ed amministrazione delle identità (IGA) che aiuti a garantire un provisioning, un re-provisioning ed un deprovisioning accurato dell'accesso degli utenti.
- Semplifica per gli amministratori la richiesta di un accesso privilegiato di cui hanno bisogno per completare attività particolari e rimuovere automaticamente subito dopo tale accesso.
- Costruisci un flusso di lavoro automatizzato in modo che gli utenti aziendali possano semplicemente richiedere l'accesso di cui hanno bisogno e i proprietari dei dati possano concedere o negare tali richieste.
- Implementa il single-sign-on (SSO) per ridurre la necessità di autenticarsi separatamente per ogni sistema o applicazione.
- L'implementazione di criteri per le password e software di archiviazione delle password gestiti centralmente, in particolare per quei sistemi che non supportano un

programma SSO a livello di organizzazione, rende facile per gli utenti creare password complesse e univoche, e di accedere alle risorse senza il problema di doverle memorizzare (o, peggio, annotando) le loro varie credenziali.

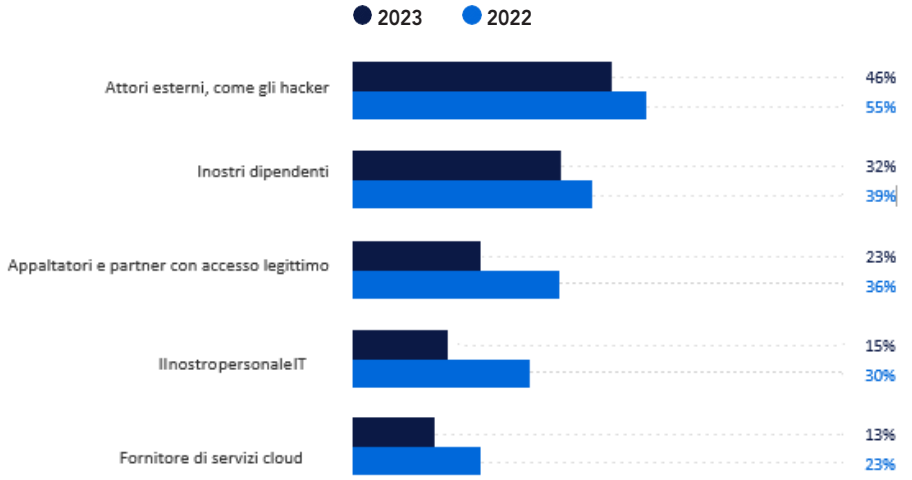
L'indagine ha, inoltre, rivelato che le organizzazioni sono molto più preoccupate per i propri dipendenti per quanto riguarda la sicurezza dei dati on-premises che nel cloud; mentre i criminali informatici sono in cima alla lista per ciò che riguarda l'infrastruttura cloud.

Chi rappresenta il rischio maggiore per la sicurezza dei tuoi dati?



Le preoccupazioni sugli attori malevoli nel cloud sono cambiate in modo significativo rispetto al sondaggio del 2022. In particolare, mentre nel 2022 il 30% degli intervistati ha indicato il proprio personale IT come la principale minaccia, da questo sondaggio è emerso che solo il 15% ha scelto questa opzione.

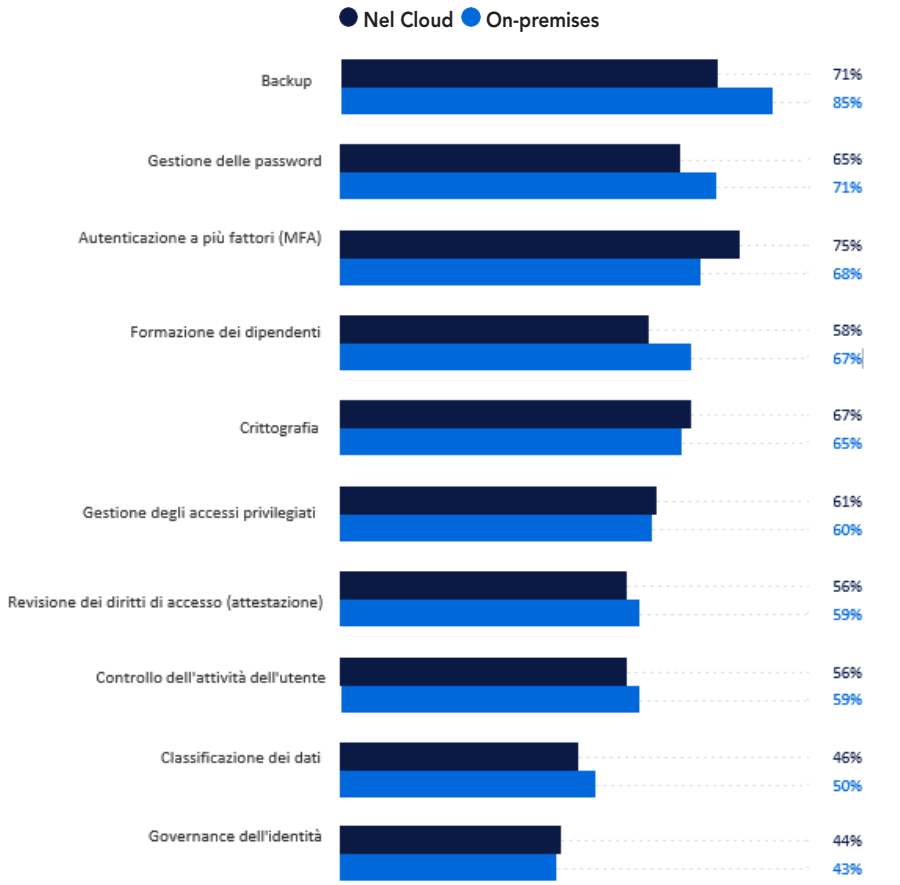
Chi rappresenta il rischio maggiore per la sicurezza dei dati nel cloud?



Le attuali misure di sicurezza

Abbiamo chiesto ai nostri intervistate quali fossero le misure che avevano adottato per proteggere i propri dati nel cloud e on-premise. Abbiamo scoperto che l'approccio è totalmente diverso. Per ciò che riguarda on-premises, le tre misure di sicurezza più comuni utilizzate sono il backup, la gestione delle password e l'autenticazione a più fattori (MFA); per ciò che riguarda il cloud, l'MFA è in cima alla lista, seguita da backup e crittografia.

Quali sono le misure che già avete adottato per proteggere i vostri dati?



Backup

Non sorprende che i backup siano in cima alla lista delle misure di sicurezza. I professionisti IT, infatti, sono sempre pronti ad affrontare per lo scenario peggiore. Ecco alcune delle best practice riguardante il backup indicate dai nostri esperti:

- limitare l'accesso ai sistemi di backup implementando l'approccio con privilegi minimi in modo che nessuna compromissione dell'account possa portare alla compromissione di un sistema di backup;

- eseguire regolarmente il backup dei dati per ridurne al minimo la perdita i caso di attacco;
- archiviare i backup offline e lontano da una rete comune per rendere più difficile l'accesso ai backup da parte degli aggressori. Un servizio di backup basato su cloud può essere un'altra opzione;
- crittografare i backup per complicare l'estrazione dei dati anche se un utente malintenzionato dovesse riuscire ad accedere ad essi;
- testare regolarmente i backup per identificare eventuali problemi, risolverli in modo tempestivo e assicurarsi del corretto funzionamento dei backup;
- utilizzare un piano di ripristino di emergenza per riprendersi da un eventuale attacco in modo rapido ed efficace. Il piano dovrebbe includere passaggi per il ripristino dei dati, la ricostruzione dei sistemi e la ripresa dell'attività;
- utilizzare strumenti di audit e di gestione delle minacce per ridurre la portata degli attacchi e valutare quali sistemi siano stati compromessi e necessitano di essere ripristinati;
- utilizzare il monitoraggio dell'integrità dei file, la gestione delle modifiche e gli strumenti di base per identificare quali sistemi siano stati compromessi a livello di infrastruttura.

Gestione password e MFA

Non sorprende, inoltre, che la gestione delle password e l'autenticazione a più fattori siano in cima alla lista delle misure di sicurezza.

Le password compromesse sono uno dei vettori di attacco iniziale più comuni. Gli hacker spesso hanno successo utilizzando elenchi di password comuni, nonché database di password trapelate perché le persone spesso riutilizzano le stesse credenziali su più siti. L'AMF offre una protezione significativa contro tali attacchi aggiungendo un ulteriore livello di difesa; le soluzioni di gestione delle password rendono più semplice per gli utenti scegliere password complesse e univoche; e SSO riduce il numero di password che gli utenti devono gestire e ricordare.

La formazione dei dipendenti

La formazione sulla sicurezza informatica è un'altra pratica comune che può essere molto efficace. Gli utenti rappresentano la più ampia superficie di attacco di qualsiasi organizzazione, quindi la sicurezza dell'identità dovrebbe rimanere una priorità per ogni team di sicurezza.

Alcuni consigli dei nostri esperti per una formazione sulla sicurezza efficace:

- obbligatoria per tutti i dipendenti a prescindere dal ruolo ricoperto;
- pertinente alle esigenze specifiche dell'organizzazione e dei dipendenti;
- rendila coinvolgente e facile da capire;
- formazione continua: la formazione sulla sicurezza non dovrebbe essere un evento una tantum, ma qualcosa di continuo;
- misurare l'efficacia per garantire che stia avendo l'impatto desiderato.

I nostri esperti aggiungono anche che non bisogna affidamento sulla formazione sulla sicurezza. È importante ridurre la superficie di attacco applicando rigorosamente il privilegio minimo e sostituendo gli account privilegiati permanenti con un accesso temporaneo. Anche se la formazione può aiutare a ridurre il numero di errori di sicurezza commessi dai dipendenti, tuttavia non elimina tale rischio. Ridurre al minimo i privilegi concessi a ciascun account riduce il danno che può derivare dalla compromissione dell'account.

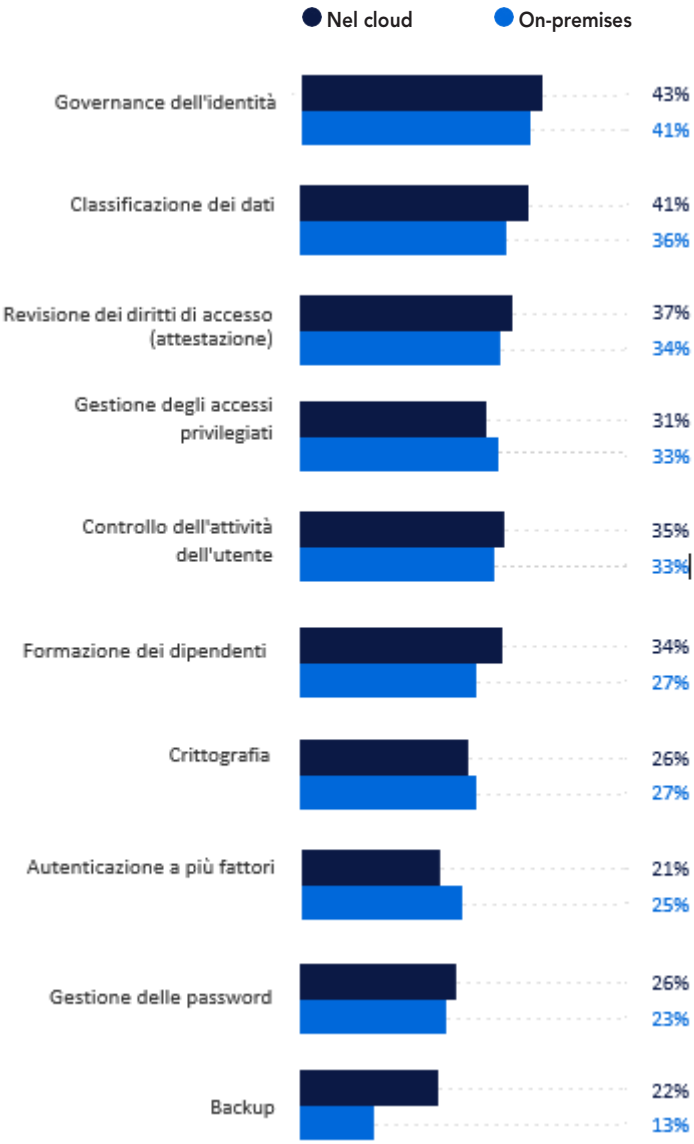
Piani per future misure di sicurezza

Priorità organizzative

La governance delle identità è in cima alla lista delle misure che le organizzazioni intendono implementare per migliorare la sicurezza informatica sia on-premise che nel cloud.

Tre delle quattro principali misure di sicurezza pianificate sono strettamente correlate: governance dell'identità, revisione dei diritti di accesso (attestazione) e gestione degli accessi privilegiati (PAM) aiutano a garantire che gli utenti giusti abbiano il giusto accesso alle cose giuste al momento giusto. L'automazione di questi processi fa risparmiare tempo prezioso al team IT e migliora la precisione, garantendo un approccio di sicurezza resiliente e agile.

Quali misure pensi di implementare per proteggere i tuoi dati?



Le priorità dei professionisti IT

Le priorità per le future misure di sicurezza cambierebbero leggermente se i professionisti IT potessero decidere in autonomia. PAM è stata la loro scelta migliore, seguita da una migliore formazione IT e da una migliore governance delle identità.

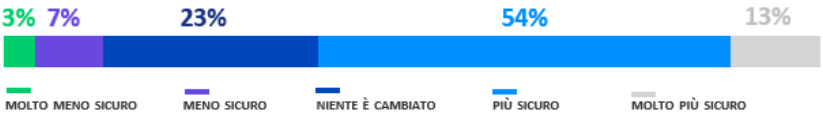
Se avessi la possibilità di poter decidere, quali misure adotteresti per migliorare la posizione di sicurezza informatica della tua organizzazione?

I professionisti IT comprendono che ridurre la superficie di attacco è fondamentale per la sicurezza della propria organizzazione. In particolare, garantire che i dipendenti utilizzino gli account amministrativi in modo responsabile può aiutare le organizzazioni ad evitare errori costosi e attacchi interni. Ancora meglio, le soluzioni PAM possono sostituire gli account amministrativi permanenti con account temporanei che dispongono di diritti appena sufficienti per l'attività da svolgere, eliminando quasi del tutto la superficie di attacco degli account privilegiati.

Le misure di sicurezza più affidabili

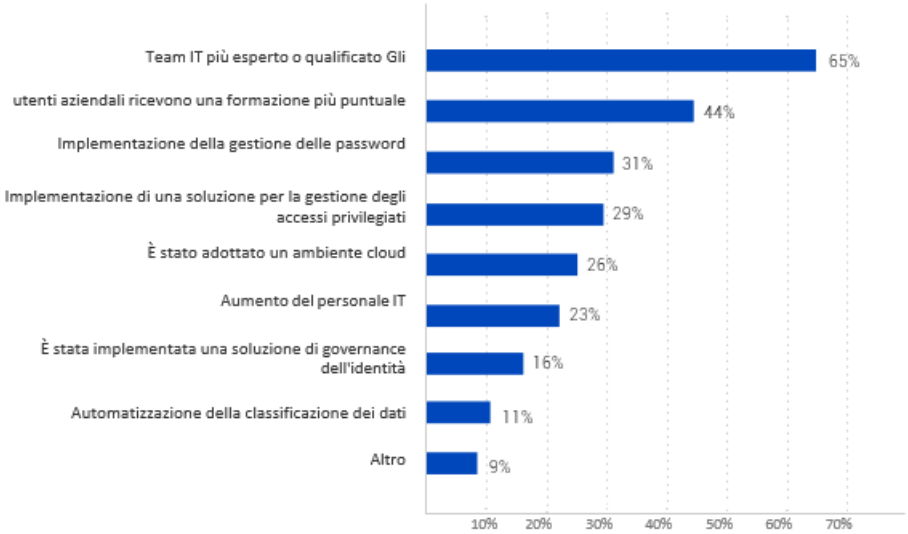
Considerato tutto il duro lavoro che i team IT stanno svolgendo per garantire la sicurezza delle proprie organizzazioni, abbiamo chiesto loro di condividere le loro il loro pensiero riguardo lo stato attuale della sicurezza informatica. Il 67% degli intervistati afferma di essere "più sicuro" o addirittura "molto più sicuro" ora rispetto a un anno fa.

Come valuti la sicurezza della tua organizzazione oggi rispetto a un anno fa?



Quindi abbiamo chiesto loro di chiarire cosa ha migliorato esattamente la loro posizione in materia di sicurezza informatica. In gran parte, hanno affermato che ciò è dovuto al fatto che sia i team IT che gli utenti aziendali ora sono meglio formati.

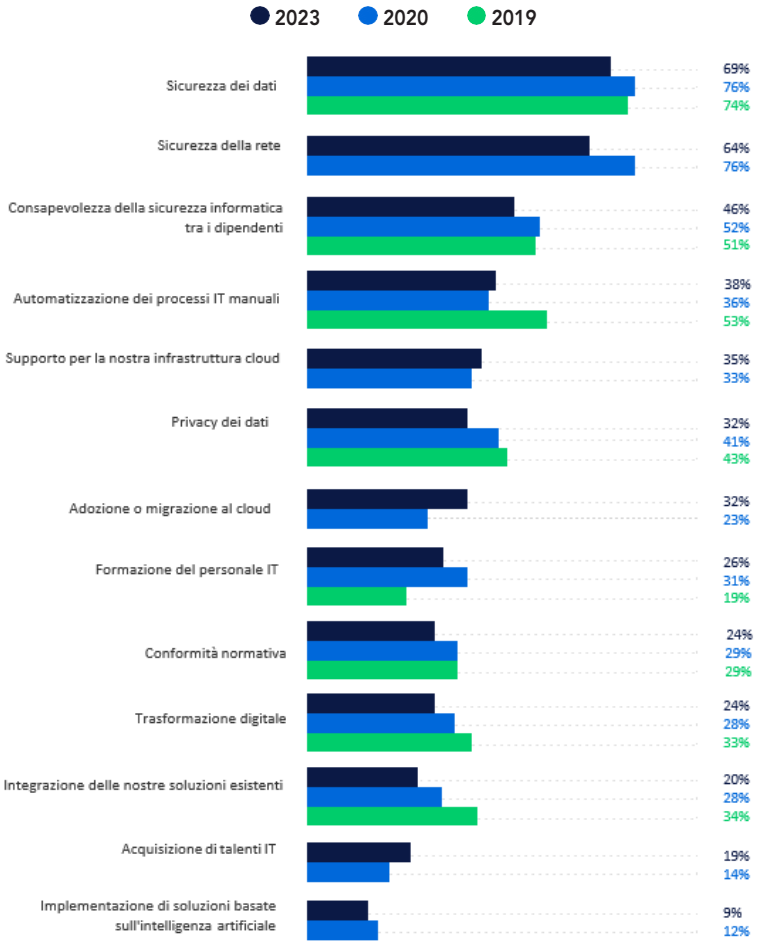
Com'è migliorata la sicurezza della vostra organizzazione?



Priorità IT più ampie

per valutare il panorama della sicurezza informatica ad alto livello, abbiamo chiesto agli intervistati quali fossero le principali priorità IT della loro organizzazione per il 2024. Abbiamo confrontato i risultati con quelli del 2019 (prima della pandemia di Covid-19) e del 2020 (quando i lockdown erano in pieno svolgimento). Le principali aree di preoccupazione sono rimaste le stesse: sicurezza dei dati, sicurezza della rete e formazione sulla sicurezza informatica. Due aree che hanno guadagnato terreno sono state l'adozione del cloud ed il supporto dell'infrastruttura cloud esistente.

Quali sono le priorità IT della tua organizzazione per il 2024?

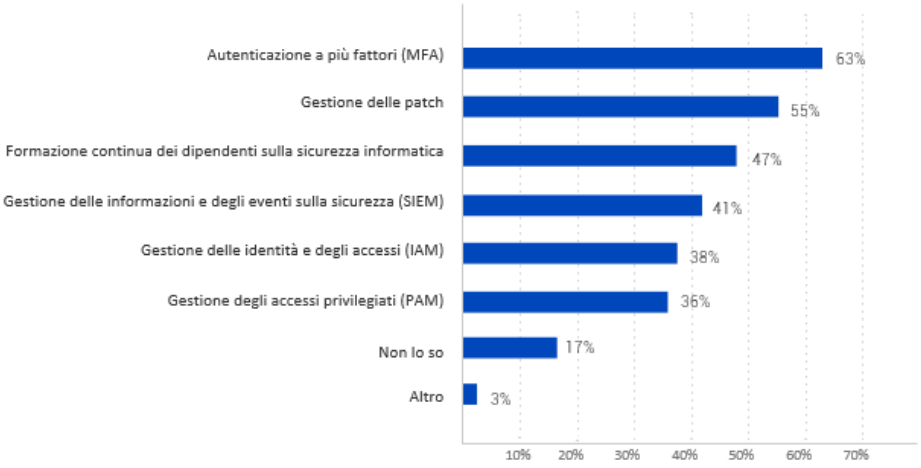


Cyber Insurance

La Cyber insurance ha lo scopo di trasferire il rischio di perdite finanziarie derivanti da una violazione dei dati ad un provider di assicurazioni. Nessuna polizza può ripristinare i dati o le operazioni di un'organizzazione, ma un risarcimento assicurativo può coprire l'impatto finanziario o addirittura prevenire il fallimento. Risulta che questo approccio alla gestione del rischio è piuttosto popolare: il 44% delle organizzazioni è assicurato e il 15% prevede di acquistare una polizza entro i prossimi 12 mesi.

Abbiamo chiesto agli intervistati che possiedono cyber insurance quali fossero i requisiti che dovevano soddisfare per poter beneficiare di una polizza. La misura più richiesta è stata l'autenticazione a più fattori, seguita dalla gestione delle patch e da regolari corsi di formazione sulla sicurezza per gli utenti aziendali.

Quali requisiti doveva soddisfare la vostra organizzazione affinché la compagnia assicurativa potesse emettere una polizza?

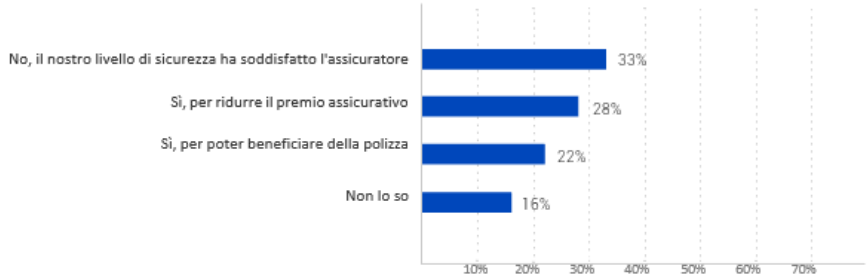


Sia la MFA che la gestione delle patch sono da tempo riconosciute come best practice che migliorano sostanzialmente il livello di sicurezza di un'organizzazione. Aiutano, infatti, a difendersi da due dei vettori di attacco più comuni: il furto degli account e lo sfruttamento delle vulnerabilità note. Pertanto, non sorprende che le compagnie assicurative verifichino che le organizzazioni abbiano implementato queste misure di sicurezza fondamentali.

59% ***delle organizzazioni ha una polizza assicurativa dedicata alla sicurezza informatica o prevede di acquistarne una entro i prossimi 12 mesi.***

Quasi 3 organizzazioni su 10 (28%) che hanno una cyber insurance hanno apportato modifiche per ridurre il premio ed il 22% di esse ha dovuto migliorare il proprio livello di sicurezza per poter beneficiare della polizza.

Avete apportato modifiche per soddisfare i requisiti della compagnia assicurativa?



Il mondo della sicurezza delle Identità

[A cura di: Michela Pesante, Giovanni Napoli, Felice Santosuosso, Pietro Valente, Claude Bazzucchi, Roberto Branz, RSA Security Italia]

L'individuo con le sue fragilità e le sue eccellenze è sempre il centro del mondo, nonostante quest'ultimo sia sempre di più digitale. Tecnologie e intelligenza sono ciò che ha fatto progredire l'umanità e ci ha elevato dai tempi bui di ignoranza e privazioni. Nei capitoli seguenti, il gruppo di lavoro ha cercato di illustrare come l'individuo e la sua identità digitale sono al centro dei ragionamenti riguardanti il progresso e la sicurezza informatica.

Perché gli attacchi partono dalle identità

In linea di principio, la risposta a una tale domanda è molto semplice:

"perché' le identità rappresentano ancora oggi la parte più diffusa e più porosa della superficie di attacco della maggior parte delle Aziende ed Organizzazioni".

Pensiamo soltanto che spesso, per ciascuna Identità associata ad una persona fisica, un'azienda deve gestire decine (se non centinaia) di Account su svariati sistemi, inserirla in diversi ruoli, fornirle una moltitudine di permessi, assicurandosi allo stesso tempo che siano esattamente quelli necessari a svolgere il proprio lavoro secondo il principio del "Least Privilege". Un principio, com'è noto, secondo il quale ciascuna identità dovrebbe avere solo, e soltanto, i privilegi ed i relativi accessi che consentono di svolgere in modo ottimale il proprio compito e per la durata prevista.

Come se non bastasse, pensiamo a quanto diventano critici i processi di Onboarding (ma anche quelli di Moving o di Leaving) di un nuovo utente, piuttosto che quelli di reset di credenziali a seguito di constatate emergenze, se gli aspetti di sicurezza non vengono adeguatamente curati.

Difatti, anche nel 2023, report come quello del World Economic Forum[1] e quello Verizon di Data Breach Investigation Report[2], rispettivamente, confermano che i rischi che maggiormente preoccupano Business Leader e Cyber Leader sono quelli derivanti da Identità compromesse e che nel 74% di breach il fattore umano è stato preponderante.

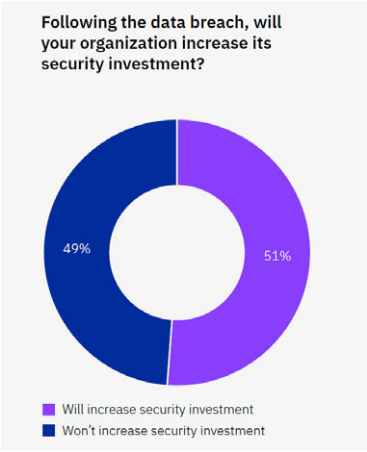
[1] https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

[2] https://www.verizon.com/business/resources/Td1d/reports/2023-data-breach-investigations-report-dbir.pdf

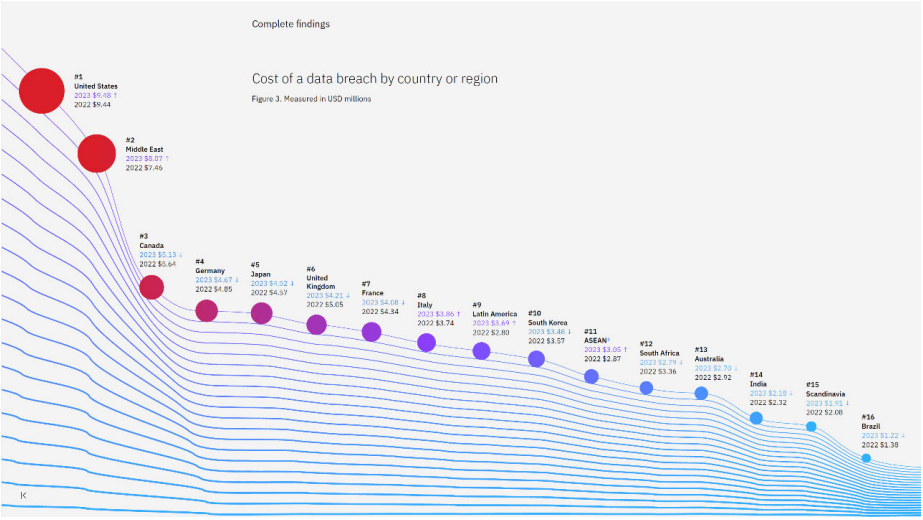
Entrando ulteriormente nel merito, proprio per il vettore di attacco maggiormente più esposto (le Identità), constatiamo che:

- l'uso delle password è ancora piuttosto diffuso.
- ci si fa tentare dell'adozione di una soluzione di Multi Factor Authentication (MFA) che sia solo "good enough" e adatta principalmente a smarcare esigenze di compliance più che a coprire anche ad aspetti di sicurezza, di interoperabilità, di easy-to-use, di fall-back in condizioni critiche o emergenziali.
- probabilmente un solido governo delle identità e del loro corretto ciclo di vita ancora non rientra tra quei controlli prioritari a mitigazione di rischi così importanti.
- pur rendendoci conto dell'impegno che un qualsiasi progetto di ammodernamento della gestione delle identità digitali possa comportare, continuiamo a mantenere in Azienda una complessità eccessiva e che poi diventa nemica della vera capacità di mitigazione dei rischi.

Secondo "The Cost of a Data Breach Report 2023" [3][3], il costo di un Data Breach, in generale, continua a salire, anche in Italia (vedi grafico riportato). Ed a seguito di una breach, nel 51% dei casi (vedi ancora grafico riportato), gli investimenti aumentano, giustamente aggiungo, soprattutto in aree come Incident Response (IR), Training, Threat Detection & Response. Tuttavia, è d'obbligo ricordare che, proprio perché le Identità rimangono ancora il maggior vettore d'attacco, parte (o aggiunte) di quegli investimenti dovrebbero forse indirizzare il "top concerning risk" evidenziato dal report del World Economic Forum del 2023: Identity Theft e ciò che ne consegue.



[3] https://www.ibm.com/downloads/cas/E3G5JMBP



L'identità sotto attacco (esempio MGM)

Uno degli attacchi Cyber che nel 2023 ha fatto più scalpore è stato quello verso la catena di Resorts e Casinò di MGM[4], non fosse altro per la perdita stimata di circa $100 milioni di dollari[5] e per la richiesta di riscatto (non pagato) di circa $30 milioni di dollari.

A settembre del 2023, un gruppo noto come APLHV penetra la rete MGM e cifra oltre un centinaio di hypervisors ESXi, forzando l'Azienda ad uno spegnimento dei principali servizi a supporto del proprio business.

L'attacco parte con un'attività di Social Engineeering che sfocia con l'ottenere, sui rispettivi tenant MGM, i privilegi di super admin di Okta ed i privilegi di Global Administrator di Microsoft Azure.
Secondo dichiarazioni dello stesso Threat Actor Group, dopo aver constatato la mancata intenzione da parte di MGM di pagare il riscatto, questi lanciano l'attacco Ransomware il giorno 11 settembre promettendo di rendere pubblici i dati rubati.

4 https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/

5 https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft/

Da sottolineare il fatto che poco tempo prima, un'altra catena di Resort e Casinò, Caesars Entertainment, aveva subito un attacco simile[6] e stante ad esperti di Cybersecurity, da parte dello stesso Threat Actor di MGM. Diversamente però da MGM, l'attacco a Caesars Entertainment aveva fatto meno "rumore" grazie al fatto di aver negoziato a $15 milioni di dollari il riscatto poi pagato, al posto dei $30 milioni inizialmente richiesti[7].

Potremmo sbrigativamente categorizzare l'attacco Ransomware ad MGM e Caesars come l'ennesimo ben riuscito e con un Threat Actor fortemente spinto da motivazioni economiche, fine della storia.

Tuttavia, ci sono diversi aspetti, anche etici, che meriterebbero una considerazione e un breve approfondimento:

- che tipo di organizzazioni criminali vengono finanziate con una mole a volte enorme di riscatto pagato? I rischi indiretti su altre Aziende e Organizzazioni o, addirittura, sulla popolazione potrebbero essere davvero rilevanti;
- questo Threat Actor (APLHV affiliato al gruppo BlackCat, anch'esso specializzato in Ransomware) è conosciuto nell'ambito della Community di Cybersecurity sotto diversi nomi: Scattered Spider (secondo Crowdstrike), 0ktapus (secondo Group-IB) piuttosto che UNC3944 (secondo Mandiant). Quali Tactics Techniques and Procedures (TTP) sono state solitamente osservate finora e che sono magari degne di nota proprio nel dominio Identity?

Relativamente al primo punto, la diffusione di cryptovalute che non consentono alcun tracciamento favoriscono purtroppo anche pesanti attività illecite.

Riguardo al secondo punto, tra le TTP del Threat Actor troviamo:

- attività di Social Engineering verso il Team di Help Desk dell'Azienda target dell'attacco;
- l'uso di phishing kit specifici come "Oktapus" che include l'invio di un SMS contenente un alert ed il link ad una pagina di phishing che, a sua volta, impersona una pagina di login di Okta collezionando sia le credenziali dell'account oggetto di phishing sia il secondo fattore di autenticazione[8];

[6] https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/

[7] https://www.wsj.com/business/hospitality/caesars-paid-ransom-after-suffering-cyberattack-7792c7f0

[8] https://www.bleepingcomputer.com/news/security/twilio-hackers-hit-over-130-orgs-in-massive-okta-phishing-attack/

- l'uso di "Bring Your Own Vulnerable Driver" per elevare privilegi di accesso (fino ad admin) sul dispositivo compromesso. In questo caso si è osservato l'uso di kernel driver di Microsoft Windows impropriamente firmati grazie al furto di credenziali di account presso "Microsoft's Windows Hardware Developer Program"[9].

Quante delle suddette Tactics Techniques and Procedures (TTP) verrebbero rese meno efficaci o addirittura vanificate da soluzioni con un approccio "security first" + "zero-trust" e, soprattutto per supportare quei processi e workflow critici come, ad esempio, il reset di credenziali piuttosto che l'onboarding di un nuovo utente?

Proprio per questi motivi alcune aziende della Cyber Security in tema Identity hanno l'accortezza di:

- Implementa, "Code Matching" per la Push Notification: un codice viene visualizzato sulla pagina di richiesta di MFA e lo stesso codice deve essere poi selezionato sull'applicazione mobile di autenticazione.
- Supporta l'integrazione con noti Provider di Identity Proofing.
- Include nell'applicativo MFA la verifica di compromissione del device su cui è installata.
- Suggerisce l'adozione di una piattaforma completa di Identity Management che guarda anche agli aspetti di Governance e Lifecycle oltre a quelli di Autenticazione.

L'Identity al tempo della ondata AI

L'*Artificial Intelligence (AI)* è nata negli anni '50, esattamente nel 1956 e da allora, ha avuto un impatto significativo su molte aree della nostra vita, soprattutto in ambito IT offrendo nuove opportunità e sfide.

Nel 2022 in Italia il mercato dell'AI ha avuto una crescita molto consistente intorno al 35% (oltre il 10% rispetto anno precedente) e si stima che sia destinata ad avere un tasso di crescita annuale del 37,3% anche tra il 2023 e il 2030[10].

Questi numeri dimostrano la crescente fiducia nel potenziale dell'AI come strumento in grado di trasformare i processi aziendali dall'automazione di attività ripetitive, all'ottimizzazione dei processi aziendali, alla gestione delle risorse umane fino ad avere un impatto importante anche nell'ambito della ricerca e sviluppo. Le crescenti aspettative che hanno le aziende convinte che l'AI contribuisca ad un generico aumento della produttività fa sì che ci sia un utilizzo sempre più frequente dell'AI in svariati ambiti IT.

---

[9] https://www.bleepingcomputer.com/news/security/malicious-windows-kernel-drivers-used-in-blackcat-ransomware-attacks/

[10] https://www.forbes.com/advisor/it/business/trend-ai-statistiche/#scrollto_fonti_section

In particolare, l'AI può offrire un ampio spettro di possibilità per supportare la *Digital Trasformation* anche nel settore dell'identità digitale. Infatti, siamo consapevoli che anche nel campo della protezione dell'identità digitale, l'AI giocherà un ruolo fondamentale per poterci garantire che solo utenti legittimi abbiano accesso ai servizi digitali a cui sono autorizzati. Ad esempio, l'AI può supportare il monitoraggio in tempo reale del comportamento degli utenti per contrastare efficacemente gli scostamenti rispetto a pattern definiti di comportamento, oppure, può essere utilizzata per difendere, assistere e supportare la resilienza degli esseri umani automatizzando processi per la difesa contro gli attacchi di Social Engineering.

È importante comprendere però che l'AI è sempre più sfruttata anche da malintenzionati per progettare e condurre attacchi sofisticati di molteplici tipologie come ad esempio:

- creazione identità fake dove l'AI è utilizzata per creare identità false ma realistiche (note come deepfake) da utilizzare per lanciare attacchi di phishing o diffondere disinformazione;
- analisi comportamentale, dove vengono sfruttate capacità di AI per comprendere il comportamento delle vittime creando attacchi personalizzati;
- eludere sistemi di autenticazione, dove l'AI è utilizzata per aggirare meccanismi di controllo accessi come ad esempio i sistemi di riconoscimento vocale, facciale o i sistemi CAPTCHA;
- sviluppo di malware e ransomware evoluti, dove l'AI viene utilizzata per generare automaticamente codici malevoli difficili da rilevare che eludono le difese aziendali;
- individuazione automatica di vulnerabilità, dove AI è utilizzata per automatizzare la scoperta delle vulnerabilità e la creazione di exploit. Ad esempio, strumenti di scansione automatizzati vengono utilizzati su larga scala per identificare le vulnerabilità di siti Web;
- chatbot evoluti sempre basati su AI che possono impersonare il servizio clienti di organizzazioni e aziende al fine di acquisire informazioni sensibili dalle vittime. In alcuni casi, questi chatbot sono stati utilizzati per indurre le persone a inviare denaro a conti fraudolenti[11].

Risulterà quindi fondamentale non focalizzarsi solo sui benefici dell'AI ma anche sulle possibili minacce che può generare cercando di mitigarle attraverso una combinazione tecnologica, di processi, di regolamentazione e di awareness (educazione e presa di coscienza) degli utenti.

[11] Attacchi sofisticati: difendersi con intelligenza artificiale, machine learning e automazione - Cyber Security 360 [1]

Analisi degli attacchi che partono da furto o compromissione delle identità

Qual è il modo migliore per entrare a casa di qualcun altro? Farsi dare le chiavi di casa. A volte non serve molta complessità per raggiungere i propri obiettivi. Lo sanno bene i criminali informatici.

Come si nota dalla statistica "Verizon 2023 Data Breach Investigations Report", il 74% di tutte le violazioni includono l'elemento umano, con le persone coinvolte attraverso, errori, privilegi di accesso, uso di credenziali rubate e social engineering. 83% delle violazioni include figure esterne e la motivazione principale degli attacchi riguarda il denaro, per il 95% degli attacchi. Le principali modalità con cui i malintenzionati riescono ad accedere a un'organizzazione sono: credenziali di accesso rubate, phishing e vulnerabilità.

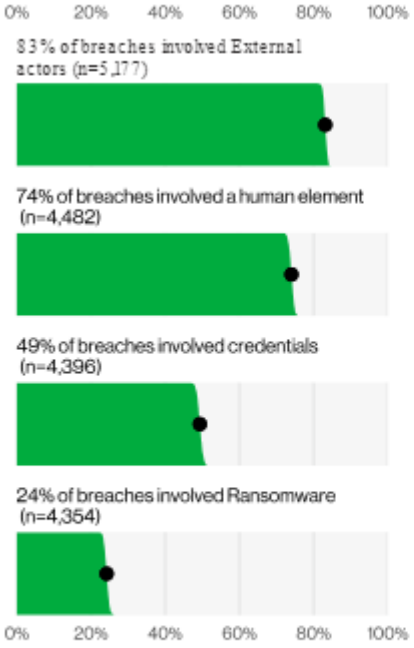


Figure 6. Select key enumerations

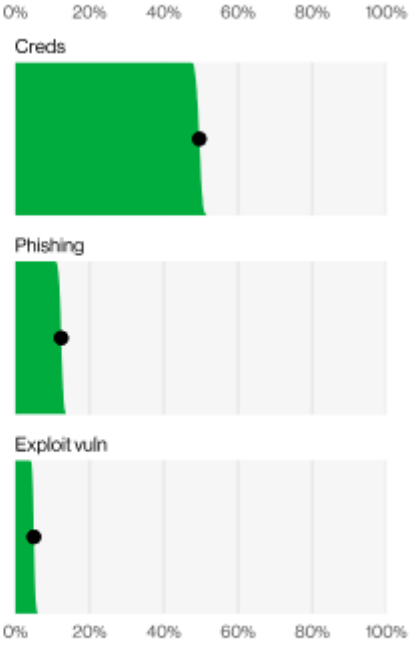


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

Gli Skill e la percezione del rischio

Come descritto fino ad ora, è chiaro che gli attacchi informatici sono sempre più complessi e sofisticati anche per effetto dell'avvento della AI. La protezione efficace dell'identità necessita di adeguati skill alla base dei quali deve esserci una forte formazione in materia *cybersecurity*. Sappiamo che una formazione forte e costantemente aggiornata (pensiamo alla conoscenza dei principi NIST, della normative GDPR, etc..) consente di ridurre il divario tra rischio reale; basato su dati statistici, e dunque oggettivi, che la propria identità possa essere compromessa dalle moderne tecniche d'attacco social engineering, brute force, eccetera; e rischio percepito, basato sulla sensazione di sicurezza o insicurezza che le persone hanno riguardo alla protezione delle proprie credenziali e delle proprie risorse sensibili online.

Solo attraverso l'educazione alle minacce più recenti, le dimostrazioni pratiche, le simulazioni di un attacco, una comunicazione chiara, l'adozione di buone pratiche di "Identity Security", possiamo mitigare il rischio di una compromissione delle identità. Dunque, non solo soluzioni di autenticazione multi fattore ma anche soluzioni di gestione delle adeguate politiche degli accessi, di governo e di gestione dell'intero ciclo di vita delle identità.

Una buona indicazione del livello di consapevolezza e di maturità degli utenti in materia di *identity security,* ci viene data dal sondaggio condotto da RSA [2] tramite il quiz RSA ID IQ 2023 [3]. Il sondaggio consiste in 15 domande a risposta multipla, condotto tra aprile e maggio 2023. Il quiz 2023 ha campionato più di 2.350 intervistati, da oltre 90 paesi, che lavorano in una varietà di settori, sia all'interno che all'esterno della cybersecurity e dell'IAM.

È conclamato ormai che l'identità è al centro di un rapido cambiamento, quello dell'epoca in cui viviamo, caratterizzato dallo sviluppo di nuove tecnologie, nuovi standard, nuove *best practice* - che usiamo per proteggere le nostre risorse - il tutto in continua, rapida evoluzione. L'identità è al centro di ciascuna di queste tendenze. Essa stessa sta subendo enormi evoluzioni, più velocemente di quanto la maggior parte della gente possa seguire.

È comprensibile quindi che il 48% dei partecipanti al Quiz RSA abbia risposto in modo errato ad almeno la metà delle domande. È anche un fatto che l'identità è la parte più bersagliata e compromessa della superficie di attacco di un'organizzazione.

Il già citato rapporto Verizon Data Breach Investigations 2023 [4] rileva chiaramente che ormai da cinque anni le credenziali utente compromesse "sono diventate il punto di ingresso più popolare per le violazioni". L'Identity Defined Security Alliance [5] ha rilevato che l'84% delle organizzazioni ha subito una violazione legata all'identità

nel 2022. Più dei tre quarti delle organizzazioni che forniscono servizi di infrastrutture critiche hanno subito una minaccia informatica guidata da insider nel 2022. Dunque, ancora una volta, possiamo asserire che le lacune nella conoscenza degli utenti danno ai cybercriminali un'apertura alla violazione, e ci sono chiare correlazioni tra le tendenze nelle risposte al quiz RSA ID IQ 2023 e i rischi più ampi della sicurezza informatica. Quasi due terzi (64%) di tutti i partecipanti al quiz ID IQ non hanno selezionato le tecnologie quale buona pratica per ridurre il phishing; allo stesso modo, il 65% dei cosiddetti esperti di Identity Access Management (IAM) non ha selezionato correttamente le migliori pratiche di prevenzione del phishing. Solo il 57% dei partecipanti ha selezionato la *compromissione delle credenziali* come la causa più frequente di una violazione dei dati. Queste lacune nella conoscenza degli utenti rendono più semplice il "lavoro" degli attaccanti. Verizon ha rilevato che il phishing è uno dei modi preferiti dagli "attaccanti per accedere ad un'organizzazione". Questo si giustifica nel fatto che gli attaccanti di solito scelgono la via della minore resistenza usando ciò che funziona - ciò si traduce, sempre più spesso, nell'attaccare gli esseri umani e nel rubare le loro credenziali invece di cercare di attaccare la tecnologia che li protegge.

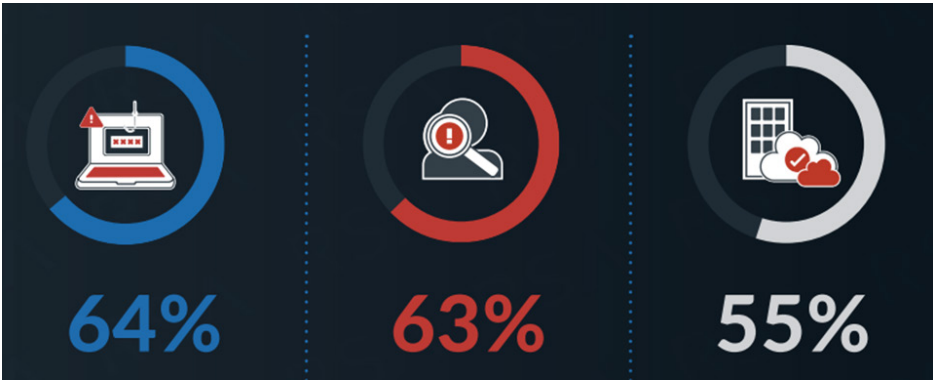
Ad aver messo in difficoltà i partecipanti non sono state solo le *best practice* tecnologiche ma anche le domande più ampie su strategie di cybersecurity: il 64% dei partecipanti al quiz ID IQ non è stato in grado di selezionare i componenti dell'Identità necessari per avvicinarsi alla strategia *zero trust security*. Si tratta di una prestazione deludente, soprattutto considerando il mandato del governo statunitense che impone alle agenzie di soddisfare i requisiti dello zero trust entro la fine dell'anno fiscale 2024. L'identità ha un ruolo critico nell'approccio *zero trust*. Il modello Zero Trust Maturity Model Version 2.0 (cisa.gov) [6] redatto dall'Agenzia per la Cybersicurezza delle Infrastrutture Informatiche (CISA) elenca l'identità come il primo dei cinque pilastri di cui le organizzazioni del settore pubblico necessitano per avvicinarsi allo *zero trust*, sottolineando che le agenzie hanno bisogno di capacità di sicurezza dell'identità per "garantire e far rispettare l'accesso degli utenti e delle entità alle risorse giuste, al momento giusto e per lo scopo giusto, senza concedere un accesso eccessivo".

Allo stesso modo, più della metà dei partecipanti (55%) non ha compreso a pieno l'importanza di adottare una strategia di sicurezza della Identità che sia completa, al fine di mitigare il più possibile il rischio dalle minacce all'identità - in sintesi, non ci si deve focalizzare solo sull'autenticazione a più fattori (MFA), ma bisogna considerare anche il sinlgle sign on (SSO), il governo e l'amministrazione dell'identità (IGA), il controllo dell'autenticazione e dell'accesso, il rilevamento delle minacce di identità e relativa tempestiva risposta.

Se gli utenti non comprendono la necessità di adottare una capacità di sicurezza dell'identità a tutto spettro, o se non configurano correttamente tutte le componenti, allora le organizzazioni sono a rischio di violazioni dei dati. Se pensiamo all'MFA, per esempio, essa rappresenta ancora la migliore prima linea di difesa ma da sola non basta per difendersi dagli attacchi moderni. Nel 2022, infatti, abbiamo visto gli attori delle minacce eludere la MFA [7] mirando alle lacune nelle soluzioni di identità o alle loro errate configurazioni. Questi attacchi all'infrastruttura di identità [8] hanno sottolineato perché le organizzazioni hanno bisogno di una piattaforma di identità unificata [9] per rimuovere le lacune e i punti ciechi dell'identità che gli attori delle minacce sono pronti a sfruttare.

Ciò che non conosci può compromettere la sicurezza della tua identità

Sulla totalità dei paesi partecipanti al quiz:

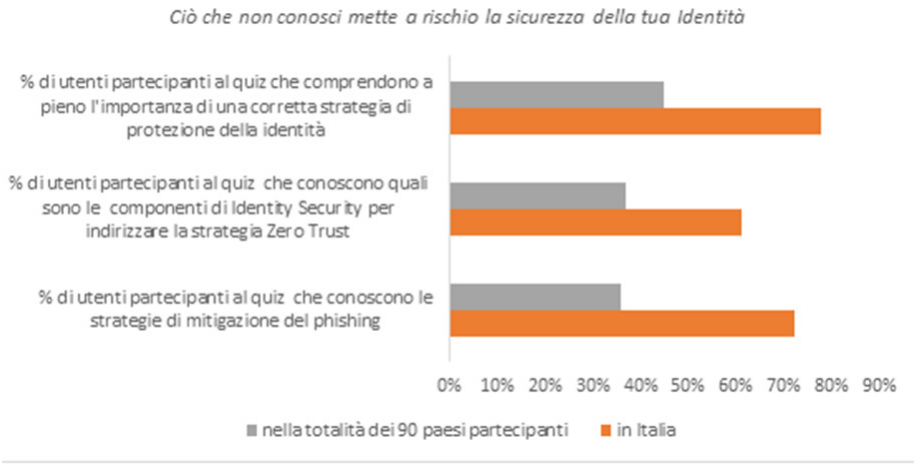


Il 64% non ha selezionato le tecnologie di best practice come strumento per mitigare il phishing

Il 63% non conosceva quali fossero le componenti di identity security necessarie per indirizzare la strategia Zero Trust

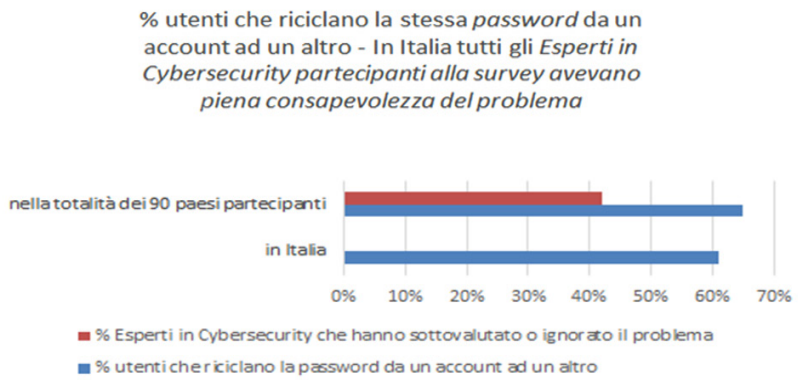
Il 55% non ha compreso a pieno l'importanza della gestione dell'identity per innalzare la postura di sicurezza di un'organizzazione

In Italia si osserva un valore percentuale sensibilmente più alto in merito alla conoscenza delle tecniche di mitigazione del phishing, alla conoscenza delle componenti di "*Identity security*" orientate verso la strategia "*zero trust*" nonché all'importanza di un approccio di gestione completo verso la sicurezza delle identità. Ciò è giustificato in parte dal fatto che, sulla totalità del campione italiano partecipante al Quiz, il 78% era costituito da soggetti autodefinitisi Professional e/o Esperti in Cybersecurity; invece, sulla totalità dei campioni analizzati il peso di questa valutazione di esperti era rappresentato solo dal 26%.



Si evince inoltre che quasi due terzi (65%) degli utenti partecipanti al Quiz ammettono di riciclare la stessa password [10] su più account. Questo è di per sé un grave rischio per la sicurezza informatica: ancora una volta, Verizon ha rilevato che le credenziali utente compromesse sono state il "punto di ingresso più popolare per le violazioni" negli ultimi cinque anni.

Forse ancor peggiore rispetto a questa pratica è il fatto che gli esperti che dovrebbero anticipare quel cattivo comportamento non sanno quanto frequentemente si verifica. Emerge, infatti, che il 42% degli esperti di IAM che hanno partecipato al quiz RSA ID IQ non sapevano o hanno sottovalutato significativamente la frequenza con cui gli utenti ammettono di riciclare le loro password. È un altro motivo per cui le organizzazioni dovrebbero trovare qualsiasi modo possibile per ridurre l'uso delle password e andare verso l'approccio *passwordless* [11].

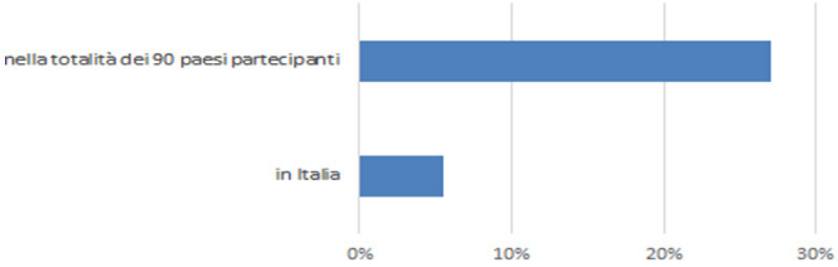


Altro elemento, i dispositivi non gestiti sono diventati obiettivi principali per la compromissione dell'identità: quasi tre quarti di tutti i partecipanti (72%) al sondaggio RSA ID IQ 2023 [12] credono che le persone usino frequentemente dispositivi personali per accedere a risorse professionali. Quasi tutti gli esperti di cybersecurity (97%) credono che gli attori delle minacce prendano di mira i dispositivi mobili non gestiti. In Italia l'intero campione di esperti in cybersecurity ritiene che gli attacccanti cyber prendano di mira i dispositivi mobili non gestiti.

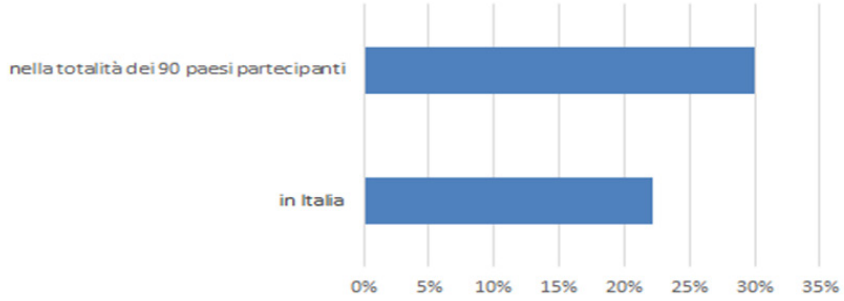
Questo si allinea perfettamente con il rapporto 2023 Global Mobile Threat Report [13] di Zimperium sulle minacce mobili globali, tale rapporto ha evidenziato che l'utente medio ha una probabilità da 6 a 10 volte maggiore di cadere in un attacco di phishing via SMS rispetto a un attacco basato su allegato email.

Altro elemento interessante analizzato dalla survey: quasi i tre quarti dei partecipanti al quiz non sapeva o sottovalutava notevolmente il costo di un reset della password, inclusa quasi la metà di tutti coloro che si sono definiti esperti di IAM. Con ogni reset della password che costa più di $70, i reset possono rappresentare quasi la metà di tutti i costi del servizio di assistenza informatica. Il fatto che il 73% dei partecipanti non sia in grado di valutare con precisione questa spesa o di capirne l'impatto sulla domanda di assistenza informatica potrebbe portare a costi fuori controllo, sottolineando il valore di utilizzare una soluzione di identità unica sia per l'autenticazione che per l'accesso. I risultati del quiz hanno anche rivelato come una governance e un'amministrazione dell'identità (IGA) inadeguate danneggino la produttività organizzativa: quasi un terzo (30%) di tutti i partecipanti ha riferito di essere stato impedito ad accedere ai sistemi necessari per svolgere il proprio lavoro almeno volta alla settimana.

% di utenti che conoscono con precisione l'incidenza economica del password reset per un'organizzazione

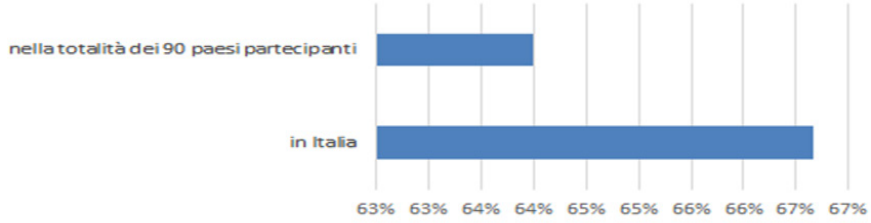


% di utenti a cui è impedito l'accesso ai sistemi almeno una volta a settimana

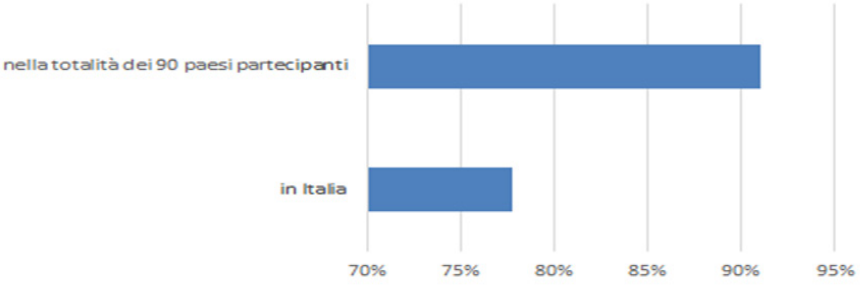


Quasi due terzi (64%) dei partecipanti al quiz RSA ID IQ [14] ripongono più fiducia nella tecnologia, per mantenere la sicurezza delle proprie informazioni sensibili online, rispetto a quanto ne ripongano nel loro partner, amico più stretto e/o consulente finanziario. Le risposte ottenute sul potenziale dell'AI per la cybersecurity sono ancora più forti: una schiacciante maggioranza - il 91% dei partecipanti al quiz RSA ID IQ - ha convenuto che l'AI ha un ruolo cruciale da svolgere nel migliorare la sicurezza dell'Identità. Che si tratti di segnalare irregolarità nell'autenticazione, nell'autorizzazione, nelle attribuzioni dei ruoli o nell'uso o nell'automatizzare le risposte alle minacce, è chiaro che l'AI ha un ruolo nel futuro della cybersecurity ed è altrettanto chiaro che gli utenti si aspettano che la implementiamo.

% di utenti che si fidano più della tecnologia che dei propri partner/consulenti finanziari/amici intimi per tutelare la sicurezza dei propri dati sensibili



% di utenti che confida nell'AI quale ruolo cruciale per migliorare la sicurezza dell'identità



I nuovi attacchi anche in presenza di MFA

La sicurezza informatica è una preoccupazione crescente in un mondo sempre più interconnesso. Tra le varie strategie per proteggere l'accesso alle informazioni sensibili, la Multi Factor Authentication (MFA) si è presentata subito come un'opzione molto promettente, con parecchi punti di forza a suo favore:

- **maggiore sicurezza:** la MFA offre una sicurezza superiore rispetto all'autenticazione a singolo fattore, poiché richiede più di una forma di verifica per confermare l'identità dell'utente. Questo significa che, anche se un malintenzionato dovesse ottenere una password, non sarebbe in grado di accedere a un account senza le altre forme di autenticazione;
- **protezione contro il phishing e altri attacchi:** la MFA può proteggere efficacemente contro gli attacchi di phishing e altri tipi di attacchi che mirano a rubare le credenziali degli utenti. Anche se un utente viene ingannato a rivelare la sua password, l'attaccante avrebbe ancora bisogno di superare gli altri fattori di autenticazione;
- **conformità normativa:** molte normative sulla sicurezza informatica e sulla privacy dei dati, come il GDPR, richiedono l'uso della MFA. L'implementazione della MFA può aiutare le organizzazioni a soddisfare questi requisiti;
- **flessibilità e scalabilità:** la MFA può essere implementata in molti modi diversi, utilizzando una combinazione di qualcosa che l'utente conosce (come una password), qualcosa che l'utente ha (come un token hardware o un telefono cellulare) e qualcosa che l'utente è (come un'impronta digitale o un riconoscimento facciale). Questo rende la MFA flessibile e scalabile per soddisfare le esigenze di sicurezza di diverse organizzazioni;
- **riduzione del rischio di accesso non autorizzato:** con la MFA, il rischio di accesso non autorizzato a sistemi e dati critici è notevolmente ridotto. Anche se un fattore di autenticazione viene compromesso, gli altri fattori forniscono ulteriori livelli di protezione.

Tuttavia, come tutte le misure di sicurezza, la MFA non è infallibile e deve essere implementata come parte di un approccio di sicurezza a più livelli. Tra i suoi punti deboli possiamo elencare:

- **complessità dell'utente:** la MFA può essere vista come un ostacolo da parte degli utenti a causa della necessità di fornire più forme di autenticazione. Questo può portare a frustrazione e resistenza all'adozione;
- **disponibilità dei fattori di autenticazione:** se un utente perde il suo dispositivo di autenticazione (come un telefono cellulare o un token hardware), potrebbe non essere in grado di accedere ai suoi account. Allo stesso modo, se un utente non ha accesso al suo dispositivo (ad esempio, se la batteria è scarica), potrebbe essere bloccgato;
- **implementazione e gestione:** la MFA può essere complessa da implementare e gestire, specialmente per le grandi organizzazioni. Può richiedere risorse significative per la formazione degli utenti, il supporto tecnico e la manutenzione continua;

- **attacchi MFA fatigue:** gli utenti che ricevono frequenti richieste di autenticazione possono diventare insensibili e approvare automaticamente le richieste senza verificarle attentamente. Questo può essere sfruttato dagli aggressori per ottenere l'accesso.

L'attacco MFA Fatigue funziona in questo modo:

- *Inizio dell'attacco*
  L'aggressore inizia inviando ripetutamente richieste di autenticazione MFA alla vittima. Queste richieste possono apparire come notifiche push sul dispositivo dell'utente, richiedendo di confermare o negare un tentativo di accesso.
- *Induzione della fatica*
  L'obiettivo è indurre la "fatica MFA" nell'utente, un termine che si riferisce alla tendenza degli utenti a diventare insensibili alle frequenti richieste di autenticazione. Quando un utente riceve costantemente queste richieste, può iniziare a approvarle automaticamente senza esaminarle attentamente.
- *Accesso non autorizzato*
  Una volta che l'utente ha approvato una richiesta di autenticazione inviata dall'aggressore, l'aggressore ottiene l'accesso al conto o al dispositivo dell'utente.

Facendo riferimento a quest'ultimo tipo di attacco abbiamo un esempio chiaro fornito dal caso UBER avvenuto nel settembre 2022, ecco come è avvenuto l'attacco in sintesi:

- **acquisizione delle credenziali:** gli aggressori hanno acquistato le credenziali di accesso di un dipendente di Uber sul dark web;
- **bombardamento di richieste MFA:** gli aggressori hanno iniziato a inviare ripetutamente richieste di autenticazione MFA al dipendente, sperando che alla fine approvasse una delle richieste;
- **inganno tramite social engineering:** dopo più di un'ora, gli aggressori hanno contattato il dipendente su WhatsApp, fingendosi del personale IT di Uber. Hanno detto al dipendente che le notifiche MFA si sarebbero fermate una volta approvata una delle richieste.

Una volta che il dipendente ha approvato la richiesta, gli aggressori hanno ottenuto l'accesso alla VPN, a quel punto sono stati in grado di sfruttare diverse impostazioni di configurazione della sicurezza non ottimali all'interno della rete e individuare uno script PowerShell che conteneva credenziali del sistema di gestione degli account privilegiati (PAMS) codificate in modo fisso. Una volta all'interno del PAMS, l'intruso è stato in grado di accedere a molteplici strumenti e aree di archiviazione contenenti milioni di record di autisti e utenti Uber (Multi-Factor Authentication Fatigue Key Factor in Uber Breach - infoq.com [15]).

ISACA ha incluso l'attacco a UBER tra i principali attacchi informatici del 2022 (Top Cyberattacks of 2022: Lessons Learned - isaca.org [16]).

Secondo il Rapporto sulle violazioni dei dati di Verizon 2022, l'82% delle violazioni dello scorso anno ha coinvolto l'elemento umano. (Ransomware threat rises: Verizon 2022 Data Breach Investigations Report | News Release | Verizon [17]).

Questo è un numero astronomico e dimostra che gli esseri umani sono ancora l'anello più debole nella sicurezza informatica, e rafforza ulteriormente l'idea di applicare i principi di zero trust e least privilege per garantire l'accesso dei dipendenti a dati e codici sensibili.

Alcuni modi in cui un'azienda può mitigare il rischio di attacco MFA Fatigue:

- **limitare il numero di richieste di autenticazione per utente:** se un utente riceve un numero eccessivo di richieste di autenticazione, l'account può essere bloccato o l'amministratore del dominio può essere avvisato;
- **cambiare la password:** se un utente riceve notifiche di autenticazione non sollecitate, può cambiare la password per bloccare la ricezione di ulteriori notifiche;
- **disattivare le notifiche push o attivare il "number matching":** questo comporta la visualizzazione di un numero da inserire nell'app di autenticazione;
- **utilizzare una chiave di sicurezza hardware:** questo può fornire un ulteriore livello di protezione, anche se la compatibilità non è garantita con tutti i servizi;
- **passare all'autenticazione FIDO senza password:** questo è un altro metodo per evitare questi attacchi.

L'importanza dell'Identity access e management nell'approccio "Zero Trust"

Zero Trust di cui si sente parlare tanto negli ultimi anni è un modello strategico applicato alla sicurezza informatica che ha l'obiettivo di proteggere i sistemi basandosi sul principio di "mai fidarsi, verifica sempre". Questo modello presuppone che la sicurezza della rete o dei sistemi all'interno di un'organizzazione sia sempre a rischio di minacce interne ed esterne di conseguenza qualsiasi collegamento, flusso, accesso ai dati, apertura di documenti, invio di messaggi e tutto quanto riguarda l'interazione con dati e processi aziendali, deve essere sempre verificato ed autorizzato.

L'approccio zero trust se ben applicato permette di mitigare i rischi ottenendo una protezione continua e adattiva per gli utenti, asset gestendo in maniera proattiva le minacce e riducendo in maniera consistente la superficie di attacco.

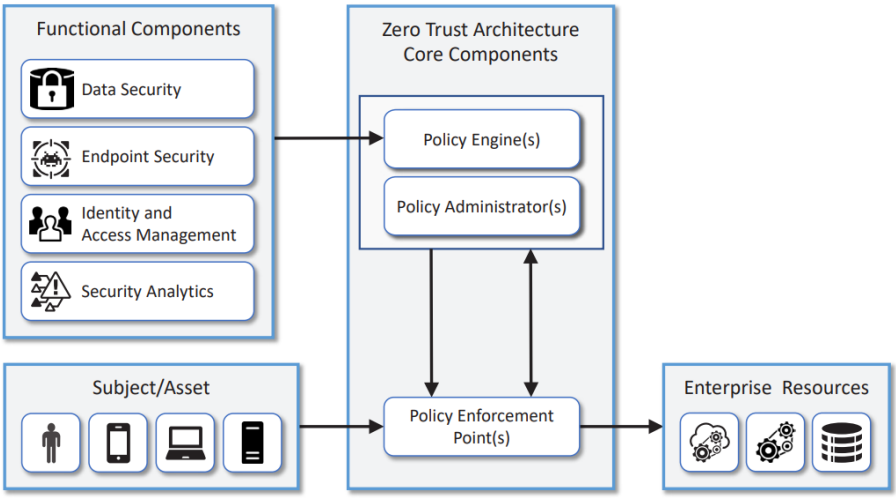
Le aziende moderne stanno sempre più considerando l'utilizzazione di questo modello strategico che per essere implementato presuppone un impegno a livello

organizzativo, con necessità di catalogare dati e asset IT ma soprattutto non può prescindere dalla gestione di identità e accessi quindi dall'avere un sistema di "*Identity and Access Management (IAM)*" e dall'implementazione di una "*Multifactor Authentication (MFA)*".

Infatti, un sistema di *Identity and Access Management* garantisce Autenticazione (anche a più fattori, MFA), Autorizzazione e Monitoraggio continuo in modo da notare fin da subito la compromissione degli account tramite richieste ed azioni insolite sfruttando anche algoritmi avanzati di Intelligenza Artificiale.

Di conseguenza, l'integrazione di un sistema di IAM in un modello Zero Trust può rafforzare significativamente la cyber security all'interno delle realtà aziendali moderne.

Nel 1994, il termine "zero trust" fu coniato da Stephen Paul Marsh nella sua tesi di dottorato sulla sicurezza informatica presso l'Università di Stirling. Il lavoro di Marsh ha studiato la fiducia come qualcosa di finito che può essere descritto matematicamente, affermando che il concetto di fiducia va oltre i fattori umani come la moralità, l'etica, la legalità, la giustizia e il giudizio.



National Cybersecurity Center of Excellence [18]. «Implementing a Zero Trust Architecture» [19]. NIST [20].

Una piattaforma unica di gestione delle identità

Il cambiamento in atto nel mondo digitale trasforma il modo in cui facciamo affari, il modo in cui interagiamo con i clienti e gli utenti esterni e il modo in cui i dipendenti accedono ai dati e alle applicazioni. Il cambiamento deriva anche dalle dinamiche di mercato in evoluzione, dai nuovi obiettivi aziendali e dalle tecnologie emergenti.

Nel corso degli anni, le organizzazioni hanno scoperto che le soluzioni di gestione delle identità e degli accessi (IAM) possono soddisfare una vasta gamma di complessi bisogni informatici, consentendo la gestione centralizzata dei ruoli utente, dei gruppi e dei diritti di accesso. In questo periodo, le organizzazioni hanno spostato i carichi di lavoro e i servizi locali nel cloud, creando un modello di identità altamente distribuito in cui ogni servizio cloud e app utilizza il proprio sistema di provisioning per gli utenti e le autorizzazioni. Questo ha notevolmente ampliato l'impatto che gli errori umani possono avere sulle esperienze degli utenti individuali e può causare significative incongruenze nel modo in cui due utenti con la stessa classificazione di ruolo accedono ai servizi. Queste incongruenze nell'autenticazione, nell'accesso e nella gestione creano rischi inutili, costi maggiori e impatti negativi sulla produttività.

Nell'adattarsi rapidamente ai nuovi requisiti tecnici, tra cui il supporto al lavoro ibrido, la creazione di esperienze digitali e la modernizzazione delle infrastrutture IT, molte organizzazioni hanno dovuto investire in soluzioni di identità puntuali che affrontano solo una componente di un piano di identità molto più complesso e integrato. Nel tempo, queste soluzioni puntuali hanno contribuito a un debito di identità: una miscela di complessità, contratti costosi e maggiore rischio derivante dagli attacchi dei criminali informatici alle credenziali degli utenti.

Il modo più efficace e veloce per affrontare il **Debito di Identità**, rimuovere la complessità, semplificare l'esperienza dell'utente, ridurre i costi e mitigare i rischi e le minacce IT è tramite una **piattaforma di identità unificata**. Tale piattaforma rappresenta un approccio unico per consolidare le esigenze di autenticazione, accesso, ciclo di vita e governance delle organizzazioni.

Queste piattaforme possono incorporare motori di intelligenza artificiale, che forniscano approfondimenti dettagliati e contesto sui rischi legati all'utente e al dispositivo, contribuendo così ad automatizzare processi critici legati all'identità. Le qualità di queste piattaforme aiutano le organizzazioni a fronteggiare le sfide che spesso sorgono durante l'implementazione delle capacità chiave per i casi d'uso più importanti:

1. **fornire autenticazione sicura e accesso alle applicazioni e ai dati;**
2. **rilevare e rispondere ai rischi e alle minacce focalizzati sull'identità;**
3. **abilitare la tracciabilità end-to-end e la gestione del ciclo di vita.**

In sintesi, l'approccio "zero trust" incorporato nelle piattaforme di gestione delle identità si basano sulla filosofia di "**Zero-Trust, continuos verification**", garantendo che gli utenti e i dispositivi non siano considerati attendibili per impostazione predefinita, indipendentemente dalla loro posizione fisica3. Questo contribuisce a proteggere l'accesso alle risorse sensibili e a gestire l'identità in modo rigoroso in un mondo digitale complesso.
Tali indicazioni sono contenute anche nel recente report "Market Guide for Identity Governance and administration" di Gartner [21].

Conclusioni

L'attenzione che le organizzazioni devono avere rispetto alle identità digitali gestite siano esse quelle dei dipendenti, delle terze parti o dei loro clienti finali, va al di là della semplice identificazione delle credenziali utente e della correlazione con l'umano che le utilizza.

Vanno pensati e automatizzati tutti i processi che servono per creare, cancellare distribuire, modificare e tenere sotto controllo i privilegi che queste identità gestiscono nella loro vita utile aziendale, anche quanto queste identità non siano legate ad un umano ma siano utilizzate da macchine o software che contribuiscono allo sviluppo aziendale.

Sitografia

[1] https://www.cybersecurity360.it/soluzioni-aziendali/attacchi-sofisticati-difendersi-con-intelligenza-artificiale-machine-learning-e-automazione/
[2] https://www.rsa.com/
[3] https://www.rsa.com/it/resources/reports/2023-rsa-id-iq-report/
[4] https://www.verizon.com/business/resources/reports/dbir/
[5] https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/
[6] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
[7] https://www.bigmarker.com/RSA/Anatomy-of-the-Attack-The-Rise-Fall-of-MFA
[8] https://www.rsa.com/multi-factor-authentication/when-mfa-wasnt-enough-rsa-conference-preview/
[9] https://www.rsa.com/zero-trust/secure-access-improve-user-experiences-prevent-security-breaches-with-a-unified-identity-platform/
[10] https://www.bleepingcomputer.com/news/security/enforcing-password-history-in-your-windows-ad-to-curb-password-reuse/
[11] https://www.rsa.com/passwordless/ds100-smoothing-the-path-to-passwordless-authentication/
[12] https://www.rsa.com/it/resources/reports/2023-rsa-id-iq-report/
[13] https://get.zimperium.com/2023-global-mobile-threat-report/
[14] https://www.rsa.com/it/resources/reports/2023-rsa-id-iq-report/
[15] https://www.infoq.com/news/2022/09/Uber-breach-mfa-fatigue/
[16] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/top-cyberattacks-of-2022-lessons-learned
[17] https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report
[18] https://en.wikipedia.org/wiki/National_Cybersecurity_Center_of_Excellence
[19] https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
[20] https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
[21] https://www.gartner.com/en/documents/3994045

Attività della Task Force Cisco Talos in difesa dell'Ucraina

[A cura di: Elio Biasiotto, Carmelo Califano, Pier Paolo Glave, Giuseppe Massa, Cisco]

Cisco è impegnata nella protezione delle persone e delle infrastrutture critiche ucraine dal 2015, ben prima dell'inizio del conflitto Russo-Ucraino sul campo, offrendo supporto e assistenza in differenti modi.

In particolare, il gruppo di threat intelligence e incident response Cisco Talos è in prima linea, fornendo monitoraggio continuo, analisi delle minacce, nonché risposta, attraverso una speciale task force creata apposta per l'Ucraina.

Questo articolo evidenzia le principali attività della task force, fornendo un'analisi dei principali attacchi e dei threat actor ritenuti più attivi, e dando un quadro delle tendenze complessive delle minacce associabili al conflitto a livello internazionale.

Primi ingaggi e preparativi di guerra: 2015-2022

La storia del rapporto di Talos con l'Ucraina risale a molti anni fa. Nel 2015 fu condotto un attacco verso la rete elettrica ucraina che risultò in un blackout completo nell'intera nazione. L'attacco, in seguito attribuito al threat actor Sandworm, utilizzò un malware noto come BlackEnergy. Lo stesso threat actor è stato ritenuto responsabile di molti altri attacchi destabilizzanti, tra cui

- i tentativi di interrompere le elezioni in Francia;
- l'attacco NotPetya che ha causato danni per miliardi di dollari in tutto il mondo;
- Olympic Destroyer, in cui è stato utilizzato un malware distruttivo per interrompere la cerimonia di apertura delle Olimpiadi invernali in Corea del Sud.

Dopo questi attacchi, Talos, tramite il team Cisco in Ucraina, ha contattato i principali partner di cybersecurity, le agenzie governative e i ricercatori di sicurezza locali e ha offerto aiuto per la protezione dagli attacchi informatici verso le infrastrutture ucraine. Dopo un periodo di studio volto a creare e consolidare i legami e la fiducia reciproca, Talos ha iniziato a lavorare per la protezione dell'Ucraina.

Circa tre mesi prima dell'invasione russa, assistendo ai preparativi e alle ricognizioni sulle infrastrutture TLC ucraine nel cyberspazio, Talos ha ampliato il suo supporto in Ucraina, schierando una task force a protezione delle infrastrutture ucraine dagli attacchi informatici proprio mentre i piani di evacuazione per il personale Cisco con sede nel paese iniziavano a prendere forma.

Fig. 1 - Supporto offerto da Cisco all'Ucraina dall'inizio del conflitto

Questa squadra comprende numerosi volontari da varie parti della struttura Talos, fra cui threat hunters, malware reverse engineers, incident responders, data scientists, e rappresenta un prototipo da impiegare nella risposta a futuri eventi globali con potenziali e significativi impatti positivi in termini di cyber sicurezza. Un grande lavoro che ha generato preziose conoscenze sugli avversari russi che serviranno a migliorare le future analisi a beneficio di tutti i clienti.

Cisco ha offerto, inoltre, alle organizzazioni governative e alle infrastrutture critiche ucraine, la fornitura gratuita di software e servizi di sicurezza e assistenza tecnica dedicata.

Cyberwar e minacce nel 2022

Lo scenario ucraino è caratterizzato da un'elevata diversità e fluidità: avversari con motivazioni molto differenti, cambiamenti continui nelle Tattiche, Tecniche e Procedure (TTP), minacce nuove ed in evoluzione e, non ultima, la difficoltà ad attribuire la responsabilità a specifici gruppi.

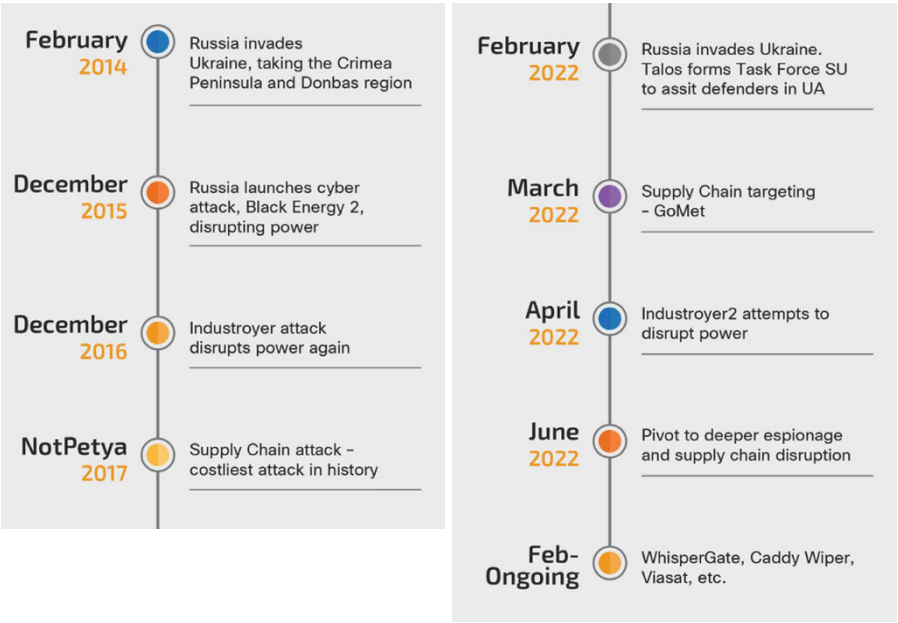


Fig. 2 - Principali Eventi Cyber nel Conflitto Russo-Ucraino

I cyber criminali hanno sfruttato, in maniera opportunistica, le tecniche più disparate per sfruttare la situazione di crisi. Qualche esempio: e-mail con contenuti legati ai temi del conflitto, messaggi che invitavano ad inviare aiuti umanitari e a partecipare a raccolte fondi,

un falso tool per DDoS (Distributed Denial of Service), "Liberator" offerto tramite Telegram allo scopo di attaccare siti di propaganda russi, attacchi di tipo "supply-chain" ("GoMet") e malware APT come ad esempio "Gamaredon".

"Altri" attori hanno usato la guerra a loro vantaggio inducendo le vittime ad installare i loro malware. Un esempio è il gruppo cinese "Mustang Panda" che ha iniziato a condurre campagne di "phishing" contro obbiettivi europei, incluse organizzazioni russe. Alcuni dei messaggi contenevano inviti ad agire mascherati da report ufficiali dell'Unione Europea (EU) sulla guerra e gli effetti sui paesi NATO. Altri messaggi invece trasportavano falsi rapporti del governo ucraino. Tutti con il fine ultimo di installare malware sul computer dell'utilizzatore finale.

Inoltre, numerose minacce, non attribuibili ad alcun attore specifico, testimoniano la varietà degli avversari e dei malware che coesistono in questo scenario.

Nel periodo immediatamente precedente e successivo all'invasione russa dell'Ucraina, attori malevoli hanno incominciato a distribuire un numero di "wipers" ed altri tipi di malware ad obbiettivi ucraini, ad esempio: WhisperGate, HermeticWiper, CaddyWiper, DoubleZero e CyclopsBlink. Sulla base delle analisi di Talos e di rapporti del Governo USA, alcune di queste minacce sono state ragionevolmente distribuite da gruppi "state-sponsored". Piu di recente, la "task unit ucraina" di Talos ha identificati un vasto gruppo di simili software, spaziando da esempi comuni quali IcedID ("commodity loader") e Sality ("malware") ad altri più specializzati come WannaCry ("ransomware"), Industroyer2 ("malware OT"), GrimPlant ("backdoor") e GraphiSteel ("information stealer").

Col proseguire della guerra, si è notato l'emergere di nuovi gruppi spinti da evidenti motivazioni politiche, dimostrando ancora una volta il legame fra minacce cyber e scenario geopolitico. Uno di questi è Killnet, un gruppo "hacktivist" che conduce attacchi DDoS in supporto agli interessi russi.

Un esame dei dati provenienti dagli endpoint Cisco fra gennaio e settembre 2022 ha condotto alla comprensione di tendenze storiche legate alle minacce dall'inizio del conflitto. Questi risultati sono basati su dati di **Behavioral Protection** (BP), un componente di Cisco Secure Endpoint che rileva e blocca attività malevole sulla base di regole dinamiche. Sulla base di questi dati è stata ricavata una lista delle 10 principali "signatures" adoperate negli attacchi contro obbiettivi ucraini.

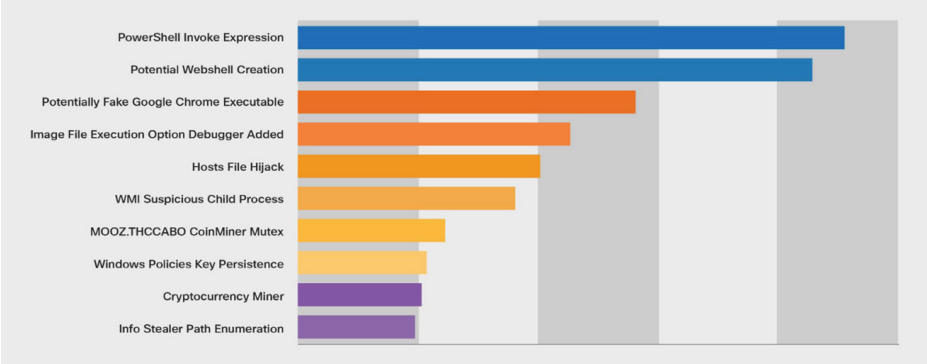


Fig. 3 - Regole BP più attive in clienti ucraini dotati di Cisco Secure Endpoint

Il grafico mostra dati aggregati, tuttavia, è interessante notare quali strumenti (PowerShell, WMI), tecniche (Windows Policies Keys, falsi eseguibili di Google Chrome) e

malware (information stealer, crypto miner) sono stati più frequentemente utilizzati durante il conflitto.

La revisione dei dati di **Exploit Prevention** (EP), fornito dalla telemetria di Cisco Secure Endpoint, mostra che il numero di rilevamenti per "signed binary proxy execution using rundll32" ha avuto un netto incremento a partire dal maggio 2022.

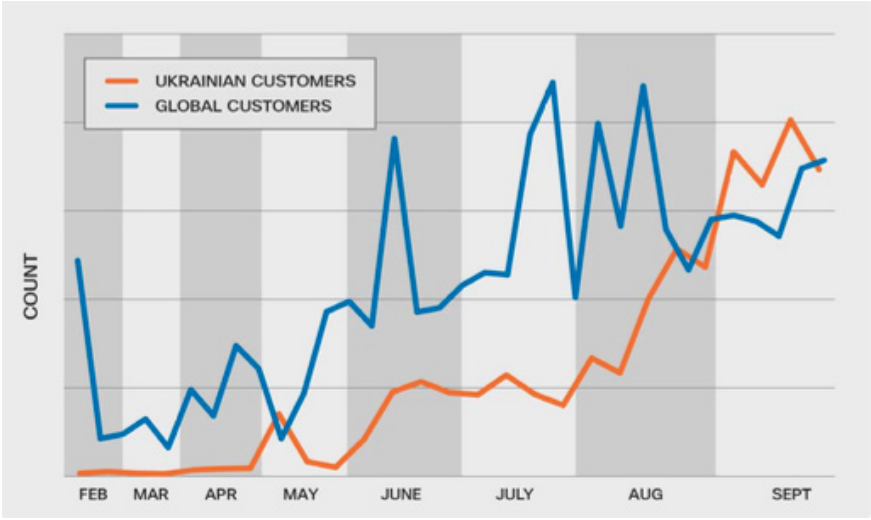


Fig. 4 - Confronto dei rilievi EP effettuati per "Signed binary proxy execution using rundll32" fra clienti ucraini e globali

Questa attività ha una precisa corrispondenza con la tecnica MITRE ATT&CK "System Binary Proxy Execution: Rundll32" (T1218.011) che ha lo scopo di far girare del codice malevolo evadendo le procedure di difesa. Secondo MITRE, un ampio numero di "threat actors" utilizza la stessa tecnica inclusi gruppi legati in maniera ufficiale alla Russia come Gamaredon, APT28 ("Fancy Bear") ed APT29 ("Cozy Bear").

Principali Threat Actor nel 2023: Gamaredon e Turla

Cisco Talos segue da vicino le attività associate a **Gamaredon**, un threat actor sospettato di essere una squadra di risorse supportate dal governo russo con base in Crimea. Sebbene il gruppo negli ultimi mesi abbia concentrato gli sforzi sul cyber spionaggio contro entità ucraine, essi prendono di mira anche entità globali, senza un focus specifico se paragonato ad altri APT russi che operano in questo settore.

La maggior parte delle vittime di Gamaredon si trova in Nord America, seguita poi da Europa Occidentale e Medio Oriente. Gamaredon ha colpito principalmente i settori dell'industria dei servizi pubblici e dei trasporti, probabilmente per causare la massima interruzione alle entità strategiche occidentali coinvolte negli sforzi logistici per supportare l'Ucraina. Nel settembre e dicembre 2022 e settembre 2023, Talos ha notato tre chiari picchi di attività di Gamaredon (**Figura 5**), che potrebbero rappresentare gruppi di operazioni mirate specifiche. In particolare, l'attività di Gamaredon dell'agosto 2023 è coerente con i livelli di attività del gruppo, segnalati nel rapporto del Centro Nazionale di Coordinamento per la Cybersecurity dell'Ucraina (NCCC).

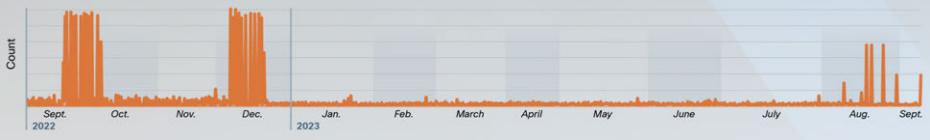


Fig. 5 - Attività di download malevola collegata a Gamaredon *(Sett. 22-Sett 23)*

Gamaredon è la minaccia dominante a cui la task force di Talos per l'Ucraina ha dovuto rispondere (**Figura 6**). Il gruppo ha più di tutti, preso di mira principalmente le entità ucraine, in particolare quelle responsabili della difesa, della diplomazia e della sicurezza interna del paese.

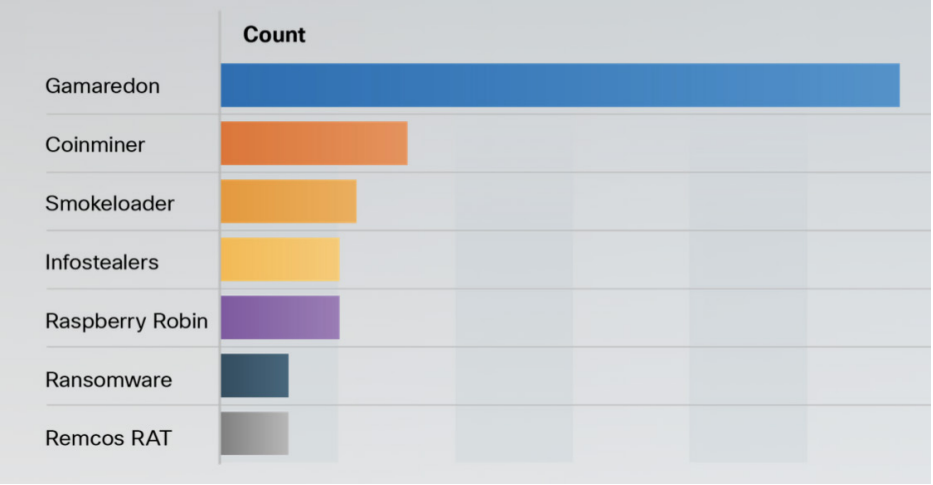


Fig. 6 - Minacce principali affrontate dalla task force Talos in Ucraina

Gamaredon, e parti della sua catena di attacco, compaiono costantemente nei principali allarmi di threat hunting segnalati da Cisco Secure Endpoint che sono stati poi notificati ai partner ucraini di Cisco. A livello di comportamenti, si evidenzia l'uso costante di LoLBins e le tecniche ad essi associate, come l'esecuzione di Wscript, un legittimo processo Windows probabilmente utilizzato per mascherare il dispiegamento di malware sotto le spoglie di un'attività prevista.

Anche il threat actor **Turla** conduce operazioni a lungo termine di spionaggio ed esfiltrazione di dati. A differenza di Gamaredon, che è stato osservato prendere di mira una serie ampia di settori nel 2023 (**Figura 7**), Turla è noto per operazioni molto più mirate contro un numero minore di entità di importanza strategica.

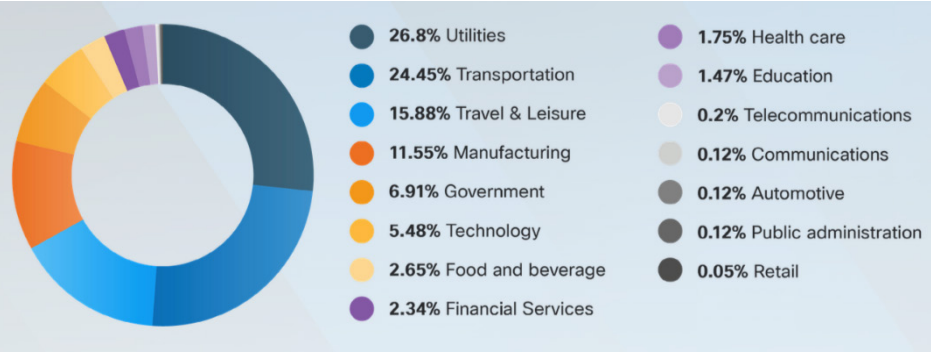


Fig. 7 - Settori verticali bersaglio di Gamaredon

Turla, che si ritiene operi per conto di un'unità diversa da quella di Gamaredon, vale a dire nell'FSB (Federal Security Service della Federazione Russa), è probabilmente in grado di compromettere uno spettro molto più ampio di entità in tutto il mondo, ma limita le sue operazioni a quelli che percepisce come obiettivi di alto valore.

Fig. 8 - Settori verticali bersaglio di Turla

Riguardo a Turla, va detto che si è osservata una diminuzione dell'attività di questo gruppo, a partire da Maggio 2023. Questa data coincide con lo smantellamento del malware Snake, operata dal Dipartimento di Giustizia degli Stati Uniti. Per quasi 20 anni, Turla ha utilizzato Snake per rubare ed esfiltrare dati da sistemi mirati, attraverso numerosi nodi di rilancio sparsi in tutto il mondo.

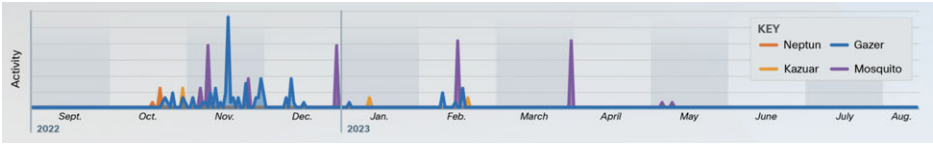


Fig. 9 - Attività collegate a Turla nel 2023

Altre attività di monitoraggio del 2023, l'esempio di Smokeloader

Gamaredon e Turla non sono le uniche minacce a cui la Task Force ha dovuto dare risposta.

Un altro esempio è costituito da **Smokeloader**, un "downloader" utilizzato da vari gruppi di attaccanti, a cui la Task Force di Talos ha risposto ripetutamente durante l'anno (vedi **Fig. 10**).

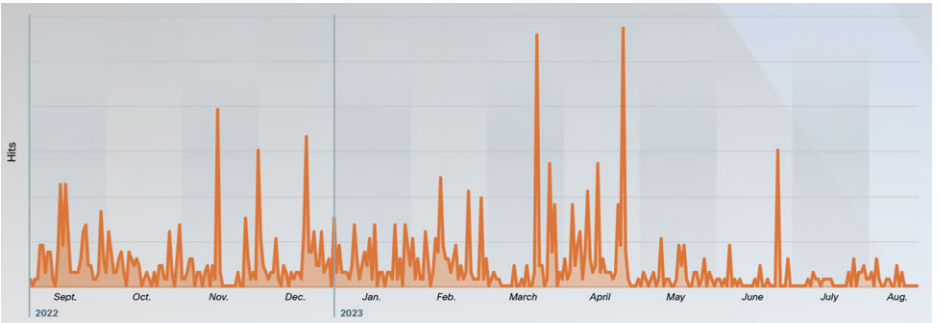


Fig. 10 - Attività di Smokeloader nel 2023

Solitamente distribuito via e-mail, SmokeLoader rilascia malware sulle macchine infette e, da inizio maggio, è stato costantemente segnalato dal Computer Emergency Response Team dell'Ucraina (CERT-UA), sottolineando ulteriormente il suo uso persistente nel panorama delle minacce. Talos ha osservato un picco di attività di SmokeLoader alla fine di aprile e all'inizio di maggio, in linea con la segnalazione del CERT-UA.

Sebbene la Task Force abbia risposto continuamente a una miriade di minacce informatiche dall'inizio della guerra tra Russia e Ucraina, l'attività osservata nel 2023 si è rivelata essere molto meno sofisticata di quella che normalmente si associa agli avversari che ci aspetteremmo di vedere in questo contesto di guerra reale.

L'attività è stata dinamica, ma non riflette l'intera gamma di capacità distruttive informatiche che la Russia ha precedentemente dimostrato contro l'Ucraina e/o i suoi alleati NATO.

Le ragioni dietro a ciò sono state dibattute dagli esperti del settore, ed è probabile che la causa principale sia da individuare negli sforzi combinati del settore della cybersecurity, del governo degli Stati Uniti, dei partner stranieri e dell'impegno dell'Ucraina a proteggere la propria popolazione e infrastrutture.

Da segnalare inoltre che Talos ha anche registrato e contrastato attività più comune, associata a criminali informatici motivati finanziariamente, come il dispiegamento di mining di criptovalute e il furto di informazioni. Attività minori, ma che continuano ad avere un impatto sulle organizzazioni ucraine in numerosi settori, a testimonianza della vasta gamma di minacce che l'Ucraina deve affrontare.

Il progetto PowerUp: garantire la luce in Ucraina

All'arrivo del primo inverno dall'inizio dell'invasione, quasi la metà della rete elettrica ucraina era stata distrutta, lasciando milioni di persone senza elettricità e riscaldamento nei mesi più freddi dell'anno.

Ad inasprire gli effetti del deficit energetico ha contribuito una tattica offensiva conosciuta come "jamming", che consiste nel disturbo delle comunicazioni radio finalizzato alla diminuzione del rapporto segnale/rumore. In particolare, questa tattica è stata utilizzata dall'offensiva Russa verso il segnale GPS per interferire con il corretto funzionamento dei sistemi che lo utilizzano, come ad esempio droni o missili radio-controllati.

Tuttavia, il segnale GPS è anche ampiamente utilizzato per la sincronizzazione degli "orologi interni" degli apparati in uso nelle stazioni elettriche ad alta tensione, gestite in Ucraina da Ukrenergo. Sebbene comunemente associato alla navigazione, il GPS viene infatti utilizzato per l'accuratezza con la quale trasmette il segnale di tempo inviato dal satellite. Questo permette di misurare il dato del tempo con una precisione inferiore ai 100 nanosecondi senza l'utilizzo di sistemi costosi come gli orologi atomici. Il dato del tempo viene utilizzato negli apparati dal componente chiamato PMU (Phasor Measurement Unit), di importanza fondamentale per la visibilità dello stato della rete. Queste interruzioni del segnale GPS, dunque, ostacolavano la sincronizzazione tra i PMU provocando interruzioni e guasti, specialmente durante i periodi di picco della domanda e nei picchi di utilizzo.

Al fine di trovare una soluzione rapida e poco costosa per rendere le stazioni resistenti al disturbo del segnale GPS, gli ingegneri della sezione IOT (Internet of Things) di Cisco hanno modificato uno switch di rete commerciale, lo switch Ethernet industriale Cisco. Quest'ultimo contiene un sistema di misurazione del tempo che, nonostante non vicino all'accuratezza del GPS, garantisce un dato sufficientemente preciso. Tra i problemi riscontrati fin da subito nella modifica di questo apparato, i principali riguardavano l'interoperabilità tra uno switch commerciale e il PMU, e il suo funzionamento in assenza di segnale GPS. Infatti, durante il disturbo del segnale GPS, il PMU non invia più dati e appare interrotto. Modificando i metadati inviati dallo switch al PMU e creando nuovi algoritmi di "clock recovery", gli ingegneri di Cisco hanno modificato gli switch rendendoli in grado di sopperire alla mancanza del segnale GPS.

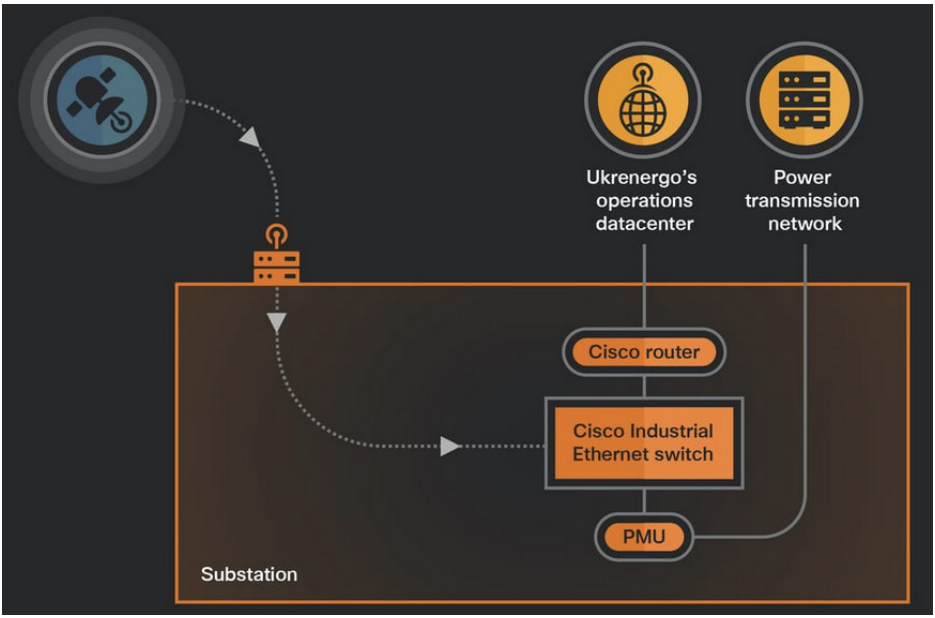


Fig. 11 - Diagramma che mostra come lo switch sia stato integrato nell'infrastruttura

Dopo mesi di sviluppo e coordinamento con vari partner, i dispositivi sono stati consegnati all'Ucraina e installati nelle stazioni elettriche di tutto il paese, un'impresa non da poco in una zona di guerra attiva.

Il progetto, denominato **Project Powerup**, è un esempio ulteriore di come gli sforzi di Cisco abbiano contribuito a proteggere l'infrastruttura critica dell'Ucraina da gravi attacchi cibernetici russi nel 2023.

Conclusione

È ragionevole concludere che il livello di rischio per il governo ucraino ed i paesi alleati rimarrà elevato per tutta la durata della guerra.

I dati telemetrici, i rapporti dei gruppi di lavoro, la caccia a nuove minacce non mostrano alcuna indicazione che l'aggressione cyber all'Ucraina possa rallentare nel breve periodo. Mentre la diversità delle minacce che i suddetti obbiettivi dovranno fronteggiare continuerà ad essere ampia, Talos sospetta, sulla base dei comportamenti registrati, che approcci più distruttivi entreranno in azione. I cyber criminali russi probabilmente sposeranno la stessa linea di condotta allo scopo di influenzare l'esito della guerra e questo scenario è destinato a rimanere tale anche in caso di cessate il fuoco o fine del conflitto armato.

Per ulteriori approfondimenti

- *Cisco Talos task Force per l'Ucraina*
  https://www.cisco.com/c/m/en_us/crisissupport.html#~faq
- *Talos – Year in Review 2022 - Ukraine*
  https://talosintelligence.com/resources/587
- *Talos – Year in Review 2023*
  https://blog.talosintelligence.com/content/files/2023/12/2023_Talos_Year_In_Review.pdf
- Cisco Powerup Project
  https://blog.talosintelligence.com/project-powerup-ukraine-grid/
- LolBins
  https://blog.talosintelligence.com/hunting-for-lolbins/
- Smantellamento del malware Snake
  https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled
- Disturbo Segnale GPS
  https://www.forbes.com/sites/davidaxe/2023/10/31/the-russians-installed-a-gps-jammer-in-ukraine-the-ukrainians-blew-it-up-with-a-gps-guided-bomb/.

Secure Access Service Edge (SASE)

(A cura di Aldo Di Mattia, Fortinet)

Gli ultimi anni hanno visto una rapida evoluzione del concetto di "hybrid workforce" che sempre più si afferma come la modalità di lavoro più efficace e congeniale per le aziende.

Per garantire maggior dinamicità, il singolo lavoratore dovrebbe essere in grado di usufruire di tutte le funzioni aziendali indipendentemente da dove si trovi (in ufficio, a casa, in viaggio), il tutto in maniera trasparente e senza limitazioni. Di fatto, la flessibilità del cosiddetto "work-from-anywhere" ha però ampliato in modo significativo la superficie di attacco a cui un'azienda si espone, incrementando i rischi relativi alla sicurezza dell'azienda stessa.

Parallelamente, la trasformazione digitale ha modificato in maniera significativa il modello di definizione ed erogazione dei servizi infrastrutturali, in particolare il luogo in cui risiedono le applicazioni aziendali, con un'adozione sempre più significativa delle soluzioni Cloud nei vari modelli: IaaS, PaaS, SaaS (Infrastructure/Platform/Software as a Service).

La presenza e la distribuzione dei servizi aziendali su infrastrutture diverse ed eterogenee tra loro, tuttavia, richiedono una completa rivoluzione del tradizionale modello di sicurezza: non è più sufficiente proteggere solo l'accesso al proprio Data Center, tipicamente attraverso un Firewall perimetrale, ma è anche necessario ampliare il perimetro di sicurezza alle infrastrutture di Private Cloud, Public Cloud e ai servizi SaaS, garantendone la consistenza, sia in termini di protezione che di accesso tra i vari ambienti.

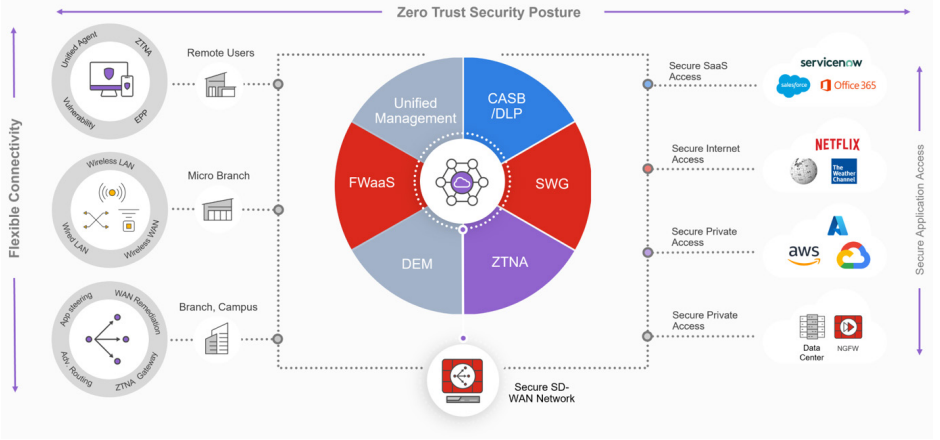
D'altra parte, la forte distribuzione e diversificazione degli scenari di accesso e delle soluzioni infrastrutturali porta spesso le organizzazioni ad affrontare grosse difficoltà nell'applicare in modo coerente le politiche di sicurezza corrette in maniera trasversale, garantendo, allo stesso tempo, un'esperienza di lavoro ottimale per gli utenti. Le soluzioni presenti, pensate in passato per coprire degli scenari puntuali, riescono difficilmente ad indirizzare tutte le esigenze correnti.

Questa rappresenta oggi una delle principali sfide per le aziende, le quali incontrano enormi difficoltà nel fornire un approccio di sicurezza distribuito e coerente sulle varie infrastrutture. La causa principale è dovuta al fatto che tali evoluzioni aziendali sono avvenute in maniera molto repentina, senza una vera e propria crescita organica, che inevitabilmente ha abbassato il livello di sicurezza lasciando spazio a potenziali

vulnerabilità, sfruttate avidamente dai cyber criminali. Inoltre, tradizionalmente, le organizzazioni hanno sempre posto bassa priorità agli aspetti legati alla visibilità e al controllo puntuale degli utenti, dei dispositivi e delle applicazioni, favorendo inevitabilmente l'aumento delle minacce e delle lacune di sicurezza.

Per indirizzare tutte queste criticità affrontate dalle aziende in tema di accesso sicuro e protezione è stato definito il modello SASE (Secure Access Service Edge). Alla base del concetto di SASE c'è l'integrazione dei servizi di networking e security, orchestrati adeguatamente per ottenere la massima efficacia in termini di protezione delle varie infrastrutture eterogenee e per fornire la miglior user-experience agli utenti in qualsiasi scenario di lavoro (casa, viaggio, ufficio). Il SASE integra fondamentalmente due componenti: SD-WAN e SSE (Security Service Edge). La componente SSE è basata su un framework che al suo interno ingloba diversi servizi e funzionalità, tra i quali, principalmente: FWaaS, CASB, ZTNA, SWG. A queste si aggiungono le funzionalità di monitoraggio, sicurezza avanzata e analisi basata su AI, intelligence oltre che sui servizi di sicurezza, quali: Digital Experience Monitoring, Sandboxing, Digital Risk Protection, Incident Response, SOCaaS (Security Operation Center as a Service), etc.

Per gestire una gamma di servizi così ampia è richiesta una correlazione ottimale di tutte le informazioni e gli eventi in rete. Diventerebbe estremamente complicato se i servizi di sicurezza di una soluzione SASE fossero erogati in modo indipendente, con soluzioni puntuali e tecnologie diverse che hanno difficoltà a cooperare e interagire tra loro. Da qui la necessità, emersa negli ultimi anni, di virare verso un modello SASE di tipo "Single-Vendor", dove le varie funzionalità ed i vari servizi, erogati da un unico vendor, possono sfruttare un layer di orchestrazione comune. Ciò semplifica la gestione e la configurazione, consentendo inoltre di correlare tutti gli eventi di sicurezza catturati sia a livello utente che infrastrutturale, andando ad implementare la migliore soluzione di protezione e riduzione dei rischi di sicurezza, il tutto attraverso l'esecuzione di meccanismi di Machine Learning e Artificial Intelligence.



SASE framework

Ulteriori vantaggi possono essere ottenuti da soluzioni Single-Vendor SASE "unificate", che permettono non solo di avere una convergenza completa tra networking e sicurezza in una soluzione integrata (che include anche strumenti di Digital Experience Monitoring), ma aggiungono analisi di sicurezza avanzata AI-based (Sandbox), Sicurezza applicativa (WAF) e soprattutto un agent unificato per il controllo dei dispositivi (EDR-XDR-EPP), chiaramente offrendo al contempo tutti i servizi e le funzionalità già citate (SD-WAN, FWaaS, CASB, ZTNA, SWG, Digital Risk Protection, Incident Response, SOCaaS, etc.).

L'implementazione SASE permette così una protezione dell'accesso alla rete Internet, garantendo all'utente remoto la stessa security posture presente in rete aziendale. Inoltre, utilizzando un approccio ZTNA, le organizzazioni possono garantire un accesso granulare e puntuale alle applicazioni fornendo un continuo controllo dello stato di sicurezza del dispositivo; questo consente di implementare nel dettaglio un modello di accesso di tipo Zero-Trust, dove ogni singolo accesso alle risorse viene valutato e garantito solo al verificarsi di specifiche condizioni. Allo stesso tempo è necessaria un'integrazione nativa e trasparente con le reti SD-WAN, per trovare automaticamente il percorso più breve verso le applicazioni aziendali supportate. Nel modello SASE, infatti, la componente SD-WAN gioca un ruolo fondamentale per garantire la migliore esperienza utente possibile, riducendo al minimo latenze e jitter e sfruttando al meglio la banda disponibile nelle varie sedi.

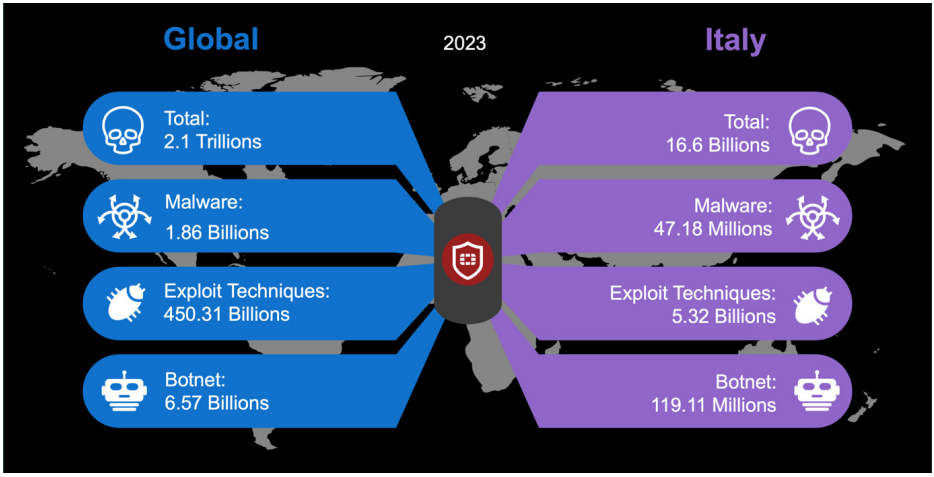
Sebbene il paradigma del SASE sta diventando sempre più un modello di riferimento tra le aziende, tuttavia, rappresenta una soluzione che indirizza requisiti ben specifici e si rivolge esclusivamente ad ambienti in cui la migrazione infrastrutturale verso il mondo cloud è ben avviata. Solo in questi casi, infatti, spostare il punto di enforcement della sicurezza all'interno del cloud può generare un vantaggio reale. Viceversa, il paradigma SASE si sposa poco con scenari tradizionali, dove i servizi vengono erogati all'interno di Data Center privati e gli utenti sono opportunamente protetti dalle soluzioni di sicurezza d'accesso, all'interno degli uffici e delle varie sedi.

L'elemento chiave di qualsiasi tipologia di architettura resta comunque invariato: garantire una protezione adeguata e costante alle organizzazioni ed i propri utenti, indipendentemente che questa sia erogata in cloud o meno, per poter contrastare in maniera efficace la continua crescita delle minacce, come illustrato di seguito.

FortiGuard Labs Threats Report 2023

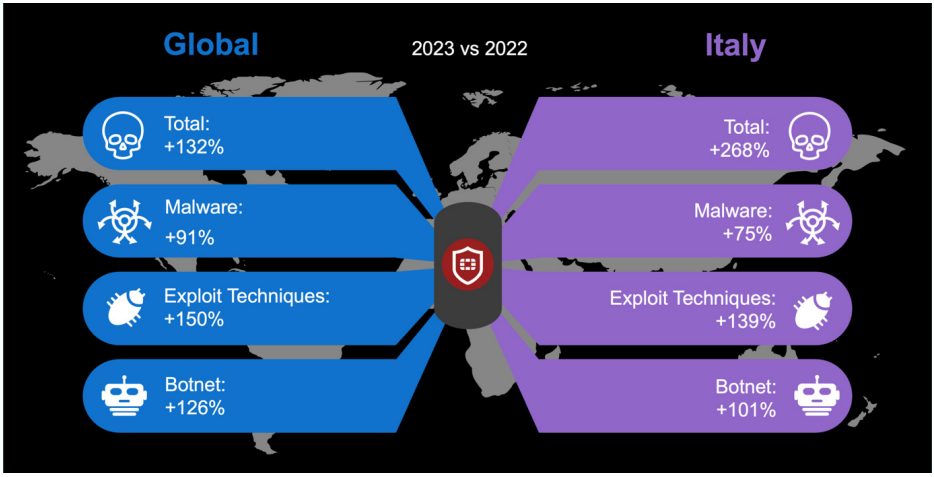
Analizzando i dati estratti dai FortiGuard Labs Fortinet si evince che, in termini percentuali, l'Italia è stata impattata dallo 0,79% delle minacce totali (0,50% nell'anno precedente). Esaminando le minacce specifiche, rispetto ai dati globali, in Italia sono state riscontrate le seguenti percentuali:

- 2,5% dei malware individuati complessivamente (2,8% nel 2022)
- 1,18% dei tentativi di exploit globali (1,2% nel 2022)
- 1,81% delle botnet intercettate nel mondo (2% nel 2022)



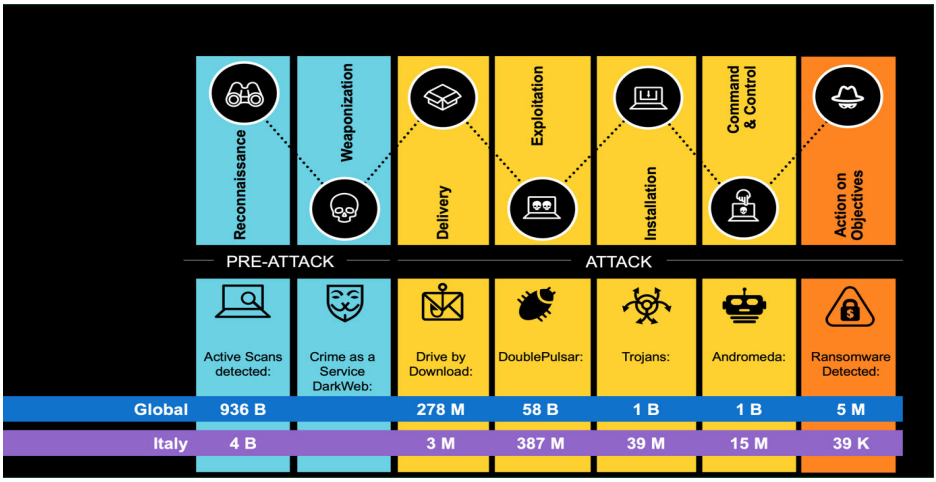
Minacce riscontrate in Italia e nel mondo nel corso del 2023

Come di seguito riportato, sorprende la crescita, in termini percentuale, delle minacce totali e specifiche individuate in Italia e nel mondo, nel corso del 2023 rispetto l'anno precedente. Il dato ancora più sconcertante è che lo stesso 2022 era stato un anno che aveva fatto registrare numeri da record.



Crescita delle minacce riscontrate nel 2023 rispetto il 2022

Andando a collocare le modalità di attacco individuate, in Italia e nel mondo, nel MITRE ATT&CK Framework, si hanno i seguenti risultati. Anche nel 2023 fa riflettere il dato legato alle attività di *Reconnaissance*: "La ricognizione consiste in tecniche che coinvolgono gli avversari che raccolgono attivamente o passivamente informazioni che possono essere utilizzate per supportare l'attacco. Tali informazioni possono includere dettagli dell'organizzazione, dell'infrastruttura o del personale della vittima." È proprio qui che si può e si deve perfezionare la strategia difensiva: Deception, Intelligence e AI sono ormai dei validi alleati, troppo spesso ignorati o ridimensionati. I dati sono espressi con l'abbreviazione angloamericana: B = miliardi, M = milioni, K = migliaia.



MITRE ATT&CK Framework - Minacce riscontrate in Italia e nel mondo nel corso del 2023

Analisi delle minacce riscontrate in Q3 e Q4 2023 in Italia e nel mondo

Nel corso dell'ultimo trimestre del 2023, FortiGuard Labs ha condotto un monitoraggio dettagliato e analisi approfondite sulle attività malevoli nel campo della sicurezza informatica, con l'obiettivo principale di fornire una panoramica completa delle minacce informatiche globali. Questo studio è stato effettuato grazie all'analisi dei dati ottenuti da diversi sistemi di monitoraggio, tra i quali AntiMalware, AntiBotnet e Intrusion Prevention, che hanno registrato numerosi tentativi di attacco.

La variazione percentuale totale delle minacce nell'area EMEA, considerando tutti i Paesi e tutti i tipi di telemetria, ha registrato un aumento del 42% rispetto al trimestre precedente. Sebbene in Q3 si sia registrata una diminuzione degli attacchi, i numeri attuali mostrano un aumento rispetto a quanto osservato in Q2. Il principale fattore che ha contribuito a tale incremento è stato l'aumento dei rilevamenti di Botnet ed exploit.

Riguardo l'identificazione di malware, è stata riportata una diminuzione del 6% rispetto al Q3, mentre c'è stato un aumento del 42% sia nei rilevamenti di Botnet che di Exploit. Complessivamente, nel quarto trimestre sono stati osservati 133 miliardi di attacchi nell'area EMEA.

Malware Detections

Esaminando i malware individuati nel quarto trimestre del 2023, è emersa una notevole presenza di minacce legate a Microsoft. Tra le più rilevanti spiccano MSOffice/CVE_2018_0798.BOR!exploit, MSExcel/CVE_2017_11882.7584!exploit, MSExcel/CVE_2017_11882.605E!exploit e MSExcel/CVE_2017_11882.D313!exploit.
Nonostante si tratti di vulnerabilità vecchie la loro persistenza suggerisce che gli attaccanti continuino a trovarle sfruttabili. Un esempio fra tutti è la recente scoperta da parte dei FortiGuard Labs Fortinet di una campagna di phishing che distribuisce una nuova variante del malware Agent Tesla; tale malware impiega un .Net-based Remote Access Trojan (RAT) e un data thief per l'accesso iniziale e viene spesso utilizzata come Malware as a Service (MaaS). Anche in Italia il malware MSExcel/CVE_2017_11882.605E!exploit è stato tra i primi tre più rilevati, insieme a JS/ScrInject.B!tr e MSIL/GenericKDS.61009645!tr.

Da sottolineare che nel corso dell'anno la distribuzione di malware attraverso i file di Office, come Excel, Word e PowerPoint, ha rappresentato quasi il 50% dei riscontri totali. Pertanto, si dovrebbe ritenere opportuno implementare strategie di sensibilizzazione e controlli come Antispam, AntiMalware e EDR/XDR, tra gli altri, per rilevare e mitigare efficacemente queste attività malevole.

È importante tenere presente che gli attaccanti sempre più sfruttano l'apertura di file malevoli da parte di utenti inconsapevoli. Attraverso tecniche di social engineering, le vittime troppo spesso vengono ingannate e indotte ad aprire file che possono poi portare all'esecuzione di codice dannoso. Questo comportamento degli utenti è spesso osservato come una fase successiva agli attacchi di Spearphishing. Gli attaccanti utilizzano per lo più le seguenti tipologie di file: .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif e .cpl.

Botnet Activity

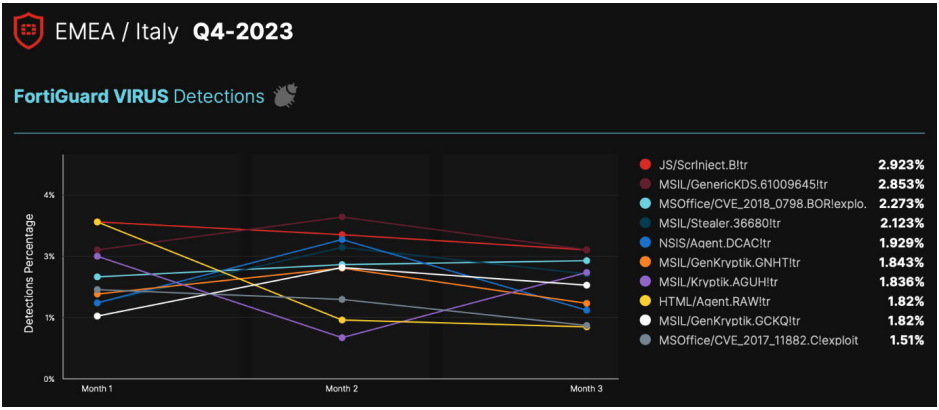
l trio di botnet, composto da Mirai, Gh0st e Bladabindi, continua a dominare la classifica delle prime 10 minacce. Tuttavia, SystemBC ha mostrato un costante aumento nel corso dell'ultimo anno, tanto che nel quarto trimestre è riuscito a posizionarsi anche nella top 3 in molti Paesi. SystemBC è stato identificato per la prima volta nel 2019. La sua caratteristica principale è quella di trasformare i computer infetti in proxy, consentendo agli attaccanti di comunicare con i loro bot all'interno delle reti interne. I Cyber criminali si connettono così alla macchina proxy, che instrada i dati al bot selezionato. Le versioni più recenti di SystemBC sono in grado anche di scaricare e eseguire file e shellcode. Un'altra tendenza interessante è che Xtreme RAT ha iniziato ad avvicinarsi al top in molti Paesi. La top 10 Botnet italiana riporta SystemBC

tra i primi tre più rilevati, insieme a Mirai e Gh0st; Bladabindi è posizionata al quarto posto.

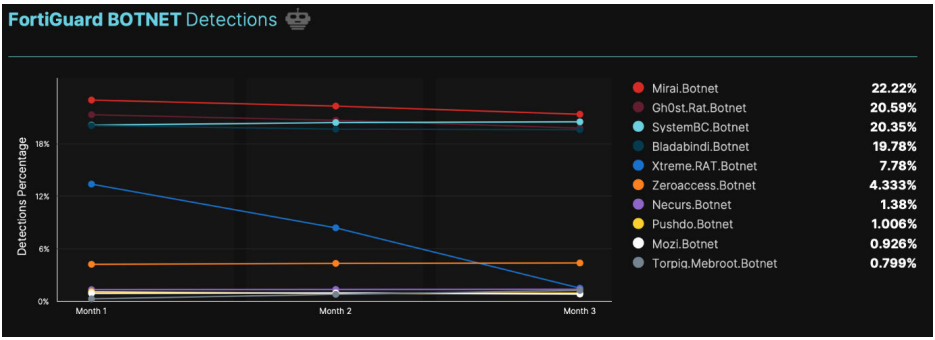
Vulnerabilities and Exploits

Nel terzo trimestre abbiamo osservato una diminuzione nello sfruttamento delle vulnerabilità di Log4J, tendenza che è proseguita nel quarto trimestre. In molti Paesi, questa vulnerabilità non è più presente nella top 10. Sebbene questo sia un segno positivo, indica anche che gli attaccanti si stanno concentrando sullo sfruttamento di nuove vulnerabilità. Una di queste è la vulnerabilità Zyxel.zhttpd.Webserver.Command.Injection, una command injection contro dispositivi Zyxel che consente agli aggressori di eseguire comandi arbitrari. Gli attaccanti hanno rapidamente identificato questa vulnerabilità e ne hanno sfruttato l'ampia diffusione. Questo fenomeno si sta registrando anche in Italia, dove la vulnerabilità occupa il primo posto sia nel terzo che nel quarto trimestre.

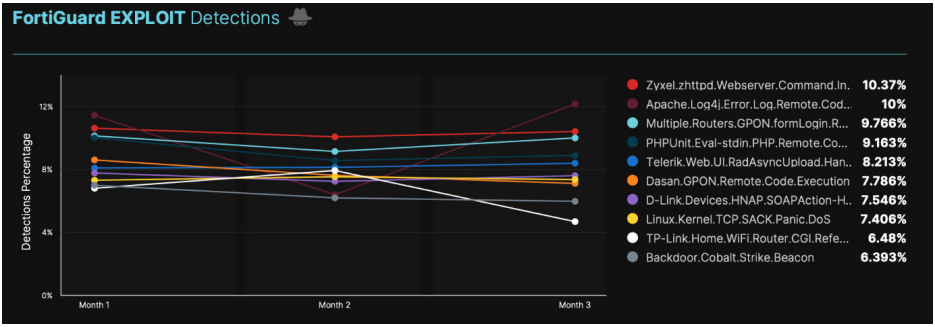
Tutti i dati indicati sono stati estratti dai FortiGuard Labs, l'organizzazione Fortinet globale di threat intelligence e di ricerca sulle minacce. Nei seguenti grafici è possibile vedere il nome delle minacce individuate da Fortinet; sul sito web https://www.fortiguard.com, nel campo di ricerca "search threats advisories", può essere inserito il nome delle firme mostrate così da avere tutti i dettagli, aggiornati in tempo reale.



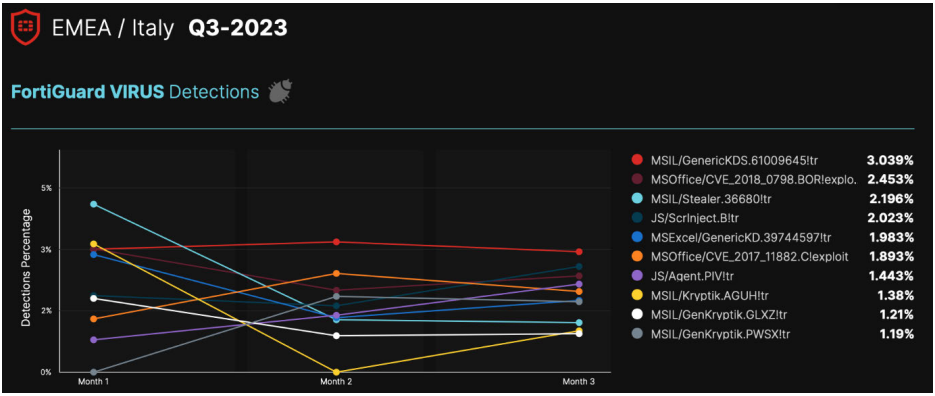
Malware più riscontrati in Italia nel corso del quarto trimestre 2023



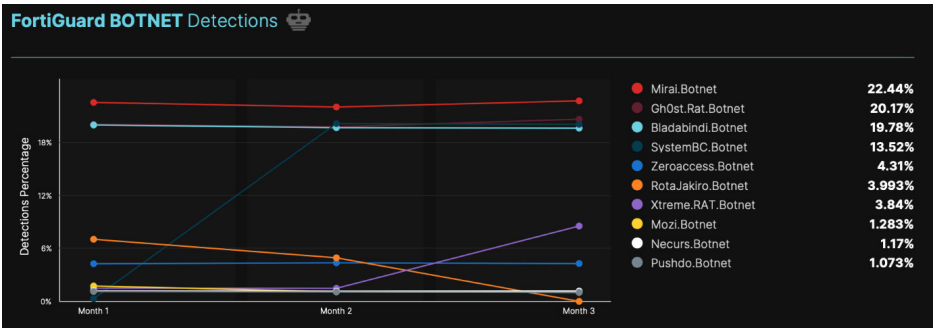
Botnet più riscontrate in Italia nel corso del quarto trimestre 2023



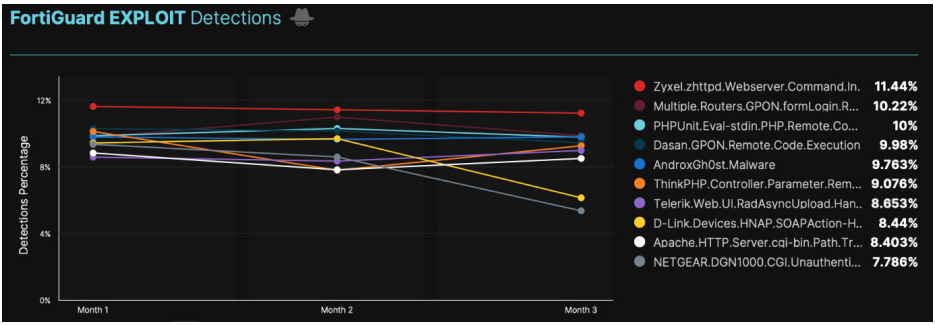
Exploit più riscontrate in Italia nel corso del quarto trimestre 2023



Malware più riscontrati in Italia nel corso del terzo trimestre 2023



Botnet più riscontrati in Italia nel corso del terzo trimestre 2023



Exploit più riscontrati in Italia nel corso del terzo trimestre 2023

Fortinet Threat Predictions 2024

L'analisi evolutiva del Cybercrime ci indica che i "classici" modelli di attacco non sono scomparsi, al contrario, evolvono e crescono via via che gli attaccanti ottengono l'accesso a nuove risorse. Attacchi di tipo Denial of Service (DoS), estorsioni e *Advanced Persistent Threats* (APT) continuano ad aumentare e a perfezionarsi, favoriti anche dall'evoluzione dell'Intelligenza Artificiale (AI) generativa. La trasformazione dell'AI in strumento di attacco sta infatti offrendo agli attaccanti un mezzo semplice ed estremamente efficace per potenziare molte fasi delle loro offensive. Come previsto nei precedenti report, si sta assistendo a un utilizzo sempre più esteso dell'intelligenza artificiale da parte dei criminali informatici per supportare attività dannose con nuove logiche, che vanno dal contrastare il rilevamento del "social engineering" all'imitazione del comportamento umano (Deep Fake). Mentre le Organizzazioni criminali strutturate si affideranno sempre più a tecniche e tattiche collaudate per ottenere il

massimo ritorno economico, gli aggressori non appartenenti a gruppi specifici hanno a disposizione un numero crescente di strumenti "*à la carte*" che li aiutano nell'esecuzione degli attacchi. Nel mezzo di questo grande processo evolutivo del CyberCrime, si prevede il proliferare di diverse nuove tendenze nel 2024. Si riportano di seguito quelli che potranno essere dei plausibili scenari:

Playbook di livello superiore: negli ultimi anni, gli attacchi ransomware in tutto il mondo sono cresciuti esponenzialmente, rendendo ogni organizzazione, indipendentemente dalle dimensioni o dal settore, un bersaglio. Tuttavia, mentre un numero crescente di criminali informatici lancia attacchi ransomware per ottenere un ritorno economico, alcuni gruppi stanno rapidamente esaurendo gli obiettivi più piccoli e potenzialmente vulnerabili. Guardando al futuro, si prevede che gli aggressori adotteranno un approccio "go big or go home", dove gli attaccanti rivolgeranno la loro attenzione a settori critici, come la sanità, la finanza, i trasporti e i servizi pubblici, così da ampliare il loro potenziale ritorno economico. Contestualmente si assiste ad un'evoluzione dei loro strumenti di attacco, che renderanno le loro attività ancora più aggressive e distruttive.

Rinnovato interesse per gli zero-day: mentre le organizzazioni espandono il numero di piattaforme, applicazioni e tecnologie su cui fare affidamento per il business quotidiano, i criminali informatici hanno un'opportunità unica per scoprire e sfruttare le vulnerabilità dei software. Nel 2023 sono stati osservati numeri record di "zero day", nuove vulnerabilità ed esposizioni comuni (CVE) e, questi numeri, sono in costante aumento. Considerato il grande valore che gli zero-day hanno per gli aggressori, ci si aspetta un incremento considerevole di "broker zero-day", ovvero gruppi criminali specializzati nella vendita di zero day sul dark web a chiunque ne faccia richiesta.

Introduzione agli attacchi "we the people": cresceranno le minacce legate ad eventi sociali e geopolitici, come le elezioni statunitensi del 2024 e i giochi di Parigi 2024. Sebbene gli attaccanti abbiano sempre sfruttato i grandi eventi, ora i criminali informatici dispongono dell'IA generativa che potenzia notevolmente la natura di queste minacce e aumenta le preoccupazioni, oltre che la difficoltà nell'individuarle e contrastarle opportunamente.

Cloud adoption e superficie d'attacco: aumentare la visibilità e la protezione contro gli attacchi nell'infrastruttura e nelle applicazioni cloud

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

Le minacce alla sicurezza relative al cloud continuano ad aumentare e gli avversari non mostrano segni di cedimento. Come rivelato nel Global Threat Report 2024 di CrowdStrike, il numero di attacchi che hanno coinvolto infrastrutture cloud è aumentato del 75% nel 2023 ed i gruppi criminali specializzati nel prendere di mira esclusivamente gli ambienti cloud sono aumentati del 110%: si parla infatti di avversari "cloud-conscious".

Gli attaccanti continuano a diventare più intelligenti e veloci mentre migliorano le loro abilità per sfruttare le lacune nella sicurezza del cloud. Secondo il Global Threat Report 2024 gli avversari impiegano in media solo 62 minuti per iniziare l'attività di movimento laterale, con il tempo di breakout più veloce osservato di soli 7 minuti.

In questo contesto, l'efficacia della sicurezza del cloud dipende dalla capacità dei difensori di raccogliere, correlare ed analizzare i dati in ambienti distribuiti: on-premise, ibridi e multi-cloud. In poche parole, i team di security moderni devono essere in grado di trovare punti deboli potenzialmente sfruttabili prima che lo facciano gli avversari. Gli approcci convenzionali non sono peró in grado di fornire la visibilità ed il controllo granulari necessari per gestire il rischio di ambienti cloud cloud, in particolare il rischio associato ai microservizi.

Le implementazioni ibride con componenti distribuite tra più ambienti cloud e sistemi on-premise creano una complessità che porta a un allungamento dei tempi di risposta e ad un sovraccarico operativo eccessivo. L'adozione di soluzioni multiple di monitoraggio e protezione e la creazione di silos distinti apre la strada a lacune di copertura e punti ciechi di visibilità che rendono difficile rilevare minacce, assegnare priorità e correggere i rischi; questo allunga i tempi di identificazione e risposta alle minacce, penalizzando i team di difesa nei confronti degli attaccanti.

Per combattere l'enorme volume e l'evoluzione della sofisticazione dei moderni attacchi cloud, le organizzazioni devono adottare un approccio più intelligente e veloce alla sicurezza, implementando soluzioni che siano nativamente pensate per ambienti dinamici e sfaccettati come quelli propri degli sviluppi applicativi moderni. Questo nuovo approccio deve dotare i difensori di una copertura di visibilità continua e dell'intelligence accurata per comprendere le tattiche utilizzate dagli avversari

per l'accesso iniziale, il movimento laterale, l'escalation dei privilegi, l'evasione della difesa e l'esfiltrazione dei dati. Nel farlo, deve nel contempo consentire ai difensori di superare in velocità e destrezza gli attaccanti.

CNAPP: ovvero come proteggersi dalle minacce cloud moderne

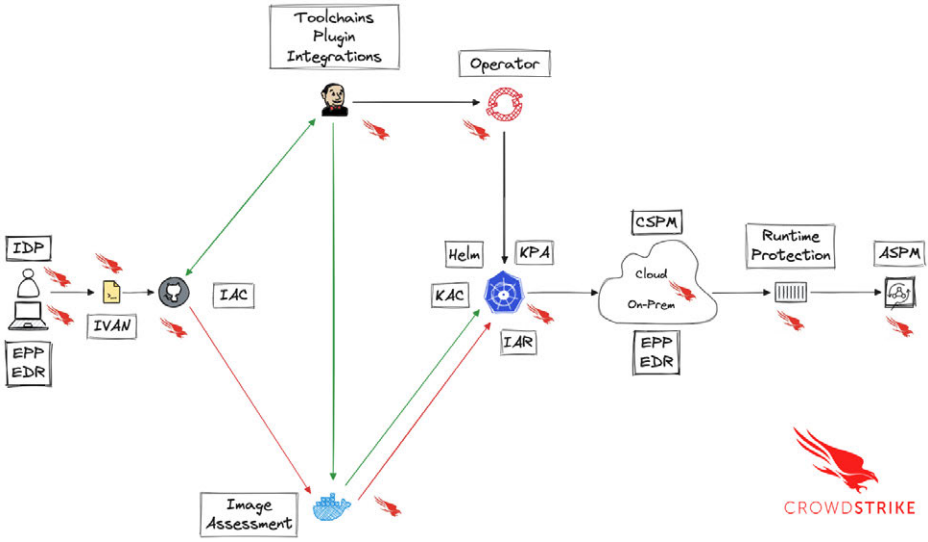
Le implementazioni cloud devono affrontare un'ampia gamma di minacce che sfruttano configurazioni errate del sistema, vulnerabilità del software e pratiche di gestione delle identità fallaci od incomplete. Una piattaforma di protezione delle applicazioni cloud-native (CNAPP) riunisce più funzionalità di sicurezza e protezione in un'unica piattaforma incentrata sull'identificazione e la definizione delle priorità dei rischi nell'intero ambiente cloud.

Un approccio CNAPP restituisce tempo ai difensori con un approccio consolidato, intelligente e altamente automatizzato alla sicurezza.

"Le CNAPP sono un insieme unificato e strettamente integrato di funzionalità di sicurezza e conformità, progettate per proteggere le applicazioni cloud-native in fase di sviluppo e produzione". (Gartner)

Mentre i team di sicurezza possono adottare l'approccio CNAPP, anche i team di sviluppo e di prodotto che forniscono applicazioni svolgono un ruolo importante. Un moderno approccio "shift-left" è in grado di seguire l'intera pipeline di integrazione continua/distribuzione continua (CI/CD) ed evidenziare ambiti sin dalle prime fasi tramite la scansione IaC (Infrastructure-as-Code) ed altre funzionalità di scansione pre-image all'inizio del ciclo di vita dell'applicazione. Questo approccio aiuta a rilevare ed eliminare le vulnerabilità causate da errori umani, incrementando il livello di sicurezza e nel contempo facendo risparmiare tempo agli sviluppatori, fornendo loro informazioni utili ed operative.

Dotarsi di soluzioni CNAPP consente alle organizzazioni di raggiungere l'obiettivo principale di creare e distribuire rapidamente le applicazioni, aiutando al contempo i difensori ad agire in modo più intelligente e veloce rispetto agli avversari.



L'immagine rappresenta una semplificazione di una moderna pipeline CI/CD con i processi che portano dalla scrittura di codice (lato sinistro) alla promozione a runtime di un componente applicativo (lato destro). Se in passato i nuovi rilasci richiedevano settimane o mesi, permettendo ai team di sicurezza di analizzare i processi, oggi il paradigma è del tutto differente; non è raro avere piattaforme applicative con molteplici rilasci al giorno e questo richiede ai team di cybersecurity un dinamismo mai implementato prima.

La sicurezza può diventare uno strumento a vantaggio anche degli sviluppatori, fornendo informazioni in ciascuna fase dello sviluppo.

I controlli possono partire dall'utenza che effettua le attività di scrittura codice, implementando meccanismi a protezione degli attacchi basati sulle identità (IDP); in questo modo ci si assicura che chi sta scrivendo codice sia il vero proprietario di quella identità digitale e non qualcuno che ne sta solo utilizzando le credenziali.

Lo stesso device usato per le attività richiede un controllo specifico (EPP) ed una raccolta di dati telemetrici (EDR) utile non solo per le finalità di prevenire compromissioni ma anche per permettere una approfondita analisi qualora questo diventi necessario.

Nel momento in cui lo sviluppatore ha scritto del codice a livello locale e lo testa su un proprio device, è possibile fornire riscontro derivante da un primo set di controlli

(IVAN) come misconfiguration, presenza di codice malevolo o deviazioni rispetto a quelli che sono gli standard di sicurezza aziendale.

Se vengono utilizzati strumenti di automazione per la gestione infrastrutturale, questi possono essere controllati (IAC) per verificare che non ci siano al loro interno componenti capaci di promuovere configurazioni a rischio.

Le immagini presenti nei registri e nei repository possono essere controllate (Image Assessment) alla ricerca di vulnerabilità e malware e per la creazione di un inventario di tutti i livelli, di sistema operativo ed applicativi, incluse nelle immagini stesse.

Se vengono utilizzati dei toolchain per l'automazione delle diverse fasi, dal test al deployment, le informazioni di analisi delle immagini possono essere utilizzate da questi tool (Toolchains Plugin Integrations) come parametri per decidere come, e se, proseguire nell'avanzamento della pipeline.

L'adozione di orchestratori quali OpenShift e Kubernetes permette il deployment automatico dei tool di sicurezza tramite Operator e Helm Chart, integrando gli strumenti di prevenzione come autentici passi di avanzamento della pipeline; questo permette di introdurre sicurezza senza aggiungere carico di lavoro agli sviluppatori.

Gli stessi orchestratori permettono di potenziare la visibilità (KPA) ed il controllo (KAC) a livello di microservizi. È possibile sapere quali microservizi sono in esecuzione e legarli alla immagine da cui derivano, avendo un quadro immediato di quali vulnerabilità si stanno esponendo a runtime ed avendo le informazioni, anche di Cyber Threat Intelligence, necessarie alla prioritizzazione degli interventi di fixing. Analogamente è possibile implementare delle politiche che permettono di prevenire attività che potrebbero esporre l'infrastruttura ad un rischio non voluto.

Per evitare che l'utilizzo di immagini non precedentemente analizzate comporti mancanza di visibilità, è fondamentale per automatizzarne l'analisi anche in fase di promozione a runtime (IAR) per poter intercettare problematiche di sicurezza anche in assenza di controlli di sicurezza precedenti.

La fase di runtime resta in ogni caso quella più critica dal momento che è in questa fase che abbiamo del codice in esecuzione ed abbiamo dei servizi potenzialmente esposti. Per questo motivo le capacità di prevenzione e la raccolta della telemetria restano fattori imprescindibili, qualsiasi sia l'ambiente in uso. La soluzione adottata deve permettere di non legarsi ad un ambiente specifico ma di seguire l'evoluzione aziendale nell'adozione di diversi ambienti cloud, pubblici, privati ed ibridi.

Una volta che l'applicazione è attiva, il controllo della applicazione stessa e di tutte le funzioni operative che la compongono rappresenta l'ultimo tassello capace di fornire

un quadro di insieme. Sapere quali moduli compongono l'architettura della applicazione, quali API vengono chiamate, quali database sono coinvolti e con quali dati e verificare il rischio di ciascun componente, permette ai team di sicurezza, di sviluppo e delle architetture di compiere scelte ragionate senza inutili complicazioni.

I cinque pilastri di un approccio di successo alla sicurezza del cloud

Le aziende hanno una richiesta sempre maggiore di scalabilità a livello applicativo e di servizi; l'incremento di bucket, microservizi, database e componenti infrastrutturali aumenta il rischio di attacco quando ci si muove in ambito cloud, sia esso pubblico o privato. Le piattaforme di sicurezza tradizionali non offrono la visibilità e l'automazione su scala necessaria per fermare gli avversari "cloud-focused" con la velocità necessaria.

Una piattaforma di sicurezza cloud moderna semplifica e unifica la sicurezza dall'on-premise al cloud per ridurre la superficie di attacco. Il consolidamento delle capacità di sicurezza in silos all'interno di un framework come CNAPP aiuta a eliminare i percorsi che gli attaccanti potrebbero seguire per sfruttare il cloud, accedere alla rete ed eseguire sofisticati attacchi moderni.

CNAPP sfrutta il consolidamento, l'automazione e l'intelligence per fornire sicurezza CI/CD, gestione e conformità della postura e protezione del runtime per ridurre i rischi dovuti all'errore umano e bloccare configurazioni errate e minacce in tempo reale. Gli strumenti risultanti forniscono agli sviluppatori di applicazioni e ai team di sicurezza le informazioni necessarie per la protezione durante l'intero ciclo di vita dell'applicazione.

Si possono identificare cinque pilastri principali per implementare una sicurezza cloud capace di rendere l'infrastruttura di sicurezza più intelligente e veloce.

1. Visibilità del 100%
2. Threat Intelligence sulle minacce perfettamente integrata
3. Strumenti consolidati ed integrati
4. Automazione su scala cloud
5. Esperienza e competenza cross tra cloud e security

Questi cinque principi fondamentali consentono ai team di sicurezza del cloud di superare gli avversari moderni e di muoversi più velocemente degli attacchi sofisticati.

Pilastri 1 e 2: visibilità e intelligence per superare in astuzia gli avversari moderni

Gli attaccanti innovano costantemente per escogitare nuovi modi per automatizzare e scalare gli attacchi. Per essere sempre un passo avanti, coloro che hanno il compito di proteggere il cloud devono comprendere le motivazioni degli avversari e anticipare le loro tattiche, tecniche e procedure (TTP). Superare in skills e velocità gli avversari comprende due dei cinque pilastri fondamentali di una soluzione CNAPP unificata:

- la copertura della visibilità end-to-end al 100% nelle implementazioni multi-cloud e ibride garantisce che gli avversari non possano nascondersi in lacune prevenibili;
- l'intelligence affidabile e in tempo reale sulle minacce e sugli avversari aiuta a comprendere gli attacchi e a riconoscere gli indicatori di compromissione (IOC) e indicatori di attacchi (IOA) per gli attacchi noti e zero-day. CNAPP dovrebbe includere la correlazione dei TTP utilizzati dagli attori cloud-focused con l'intelligence globale sulle minacce.

Pilastro 1: visibilità al 100% per evitare pericolosi punti ciechi

Le violazioni del cloud si verificano spesso a causa della mancanza di visibilità e protezione unificate e in tempo reale in ambienti ibridi e multi-cloud. Le lacune nella visibilità consentono alle minacce di insinuarsi attraverso punti ciechi tra le diverse soluzioni di monitoraggio, aumentando la superficie di attacco di un'organizzazione ed incrementando la probabilità che gli attacchi abbiano successo.

La CNAPP unificata elimina le lacune di visibilità tra gli strumenti di sicurezza e tra le pipeline CI/CD. La protezione completa azionabile tramite un'unica console consente una risposta più rapida ed intelligente. L'obiettivo finale è una visibilità completa, incorporando l'intelligence sulle minacce e l'automazione per bloccare gli attacchi.

Pilastro 2: Threat Intelligence per comprendere i moderni avversari del cloud

L'enorme incremento delle attività di sfruttamento del cloud da parte degli attaccanti e della sofisticazione degli attacchi, richiede che gli esperti di sicurezza siano in grado di comprendere il comportamento degli avversari più rapidamente che mai.

Gli avversari moderni conoscono il cloud e sanno come automatizzare gli attacchi e sfruttare ogni punto debole. La profonda conoscenza dei container, delle vulnerabilità e delle infrastrutture dei provider di servizi cloud (CSP) consente loro non solo di trovare modi per violare l'infrastruttura, ma anche di evitare il rilevamento mentre si spostano lateralmente attraverso i sistemi accedendo alle risorse più preziose e critiche dell'azienda.

A loro volta, le strategie di difesa più efficaci incorporano una profonda conoscenza di come gli avversari pensano e agiscono nelle pratiche di prevenzione, rilevamento e gestione della postura di sicurezza.

Una soluzione CNAPP dovrebbe integrare informazioni affidabili sulle minacce in tempo reale, potendo guidare un processo decisionale più intelligente e sicuro, capace di migliorare la risposta agli incidenti.

La combinazione di informazioni aggiornate sulle minacce con la conoscenza di ciò che avviene nell'ambiente consente agli strumenti di sicurezza e ai team di comprendere le motivazioni degli avversari e prevedere gli attacchi. L'integrazione di threat intelligence e adversary intelligence di livello consente agli analisti di:

- individuare i TTP moderni;
- correlare e contestualizzare il rischio;
- dare priorità agli sforzi per correggere le vulnerabilità e correggere le configurazioni errate utilizzate per eseguire attacchi cloud.

La threat intelligence deve essere perfettamente integrata in tutti gli ambienti e i controlli, in modo che il suo utilizzo e la sua applicazione avvengano automaticamente. Le soluzioni dovrebbero sfruttare l'agilità del cloud per archiviare set di dati molto grandi per l'uso futuro da parte degli analisti nella risposta agli incidenti, nella ricerca delle minacce e nell'analisi forense.

Gli indicatori di rischio integrati e comprovati, ad alta confidenza, aiutano gli analisti a rilevare e prevenire gli attacchi di runtime tramite l'implementazione di:

- indicatori di attacco (IOA) per identificare i comportamenti e le tendenze degli aggressori;
- indicatori di compromissione (IOC) per riconoscere l'inizio di un attacco;
- indicatori di configurazioni errate (IOM) per evitare che l'errore umano e i controlli configurati in modo errato lascino le porte aperte agli aggressori.

Pilastri 3 e 4: muoversi più velocemente degli attacchi sofisticati

Per accelerare il rilevamento e la risposta, individuare in modo proattivo le minacce e prevenire gli incidenti prima che si verifichino, le moderne strategie di sicurezza del cloud includono due pilastri fondamentali:

- il consolidamento degli strumenti di sicurezza semplifica le operazioni e la conformità. Una piattaforma CNAPP unificata dovrebbe combinare capacità di rilevamento e risposta con un approccio eterogeneo, sia senza agent sia basato su agent, per ottenere una visibilità completa sull'intero ecosistema cloud;

- funzionalità integrate di automazione che permettono la scalabilità e riducono le azioni manuali per rendere operativo il valore della telemetria raccolta, contestualizzare gli incidenti ed applicare l'azione di risposta corretta; l'automazione, integrata con le piattaforme di orchestrazione, permette pertanto una veloce distribuzione di applicazioni rese sicure da un controllo continuo durante l'intero ciclo di sviluppo.

Pilastro 3. Consolidamento degli strumenti per semplificare le operazioni

L'approccio tradizionale alla sicurezza del cloud si basa su strumenti eterogenei di più fornitori. Ciò costringe gli amministratori a passare dalla protezione del carico di lavoro cloud (CWP), alla gestione della postura di sicurezza del cloud (CSPM), alla gestione dei diritti dell'infrastruttura cloud (CIEM) e ad altri set di strumenti e dashboard per cercare di creare una visione olistica del rischio.

La complessità creata da un approccio a macchia di leopardo aumenta la probabilità di lacune di visibilità e ritarda il processo decisionale e di risposta. Strumenti isolati forniscono una visione frammentata che manca di un contesto sufficiente per dare priorità alle minacce.

Anche le operazioni ne risentono, poiché più strumenti generano volumi eccessivi di avvisi da analizzare ed aumenta la possibilità che vulnerabilità ed errori di configurazione passino inosservati.

Queste inefficienze aggiungono rischi e fanno lievitare i costi, rendendo più difficile mantenere la compliance e rafforzare il livello di sicurezza.

Pilastro 4: Automazione costruita su larga scala

Una soluzione CNAPP supporta le best practice CI/CD che richiedono l'integrazione e l'automazione della sicurezza durante l'intero ciclo di vita dell'applicazione cloud. Gli sforzi manuali rallentano le operazioni di sicurezza e la distribuzione delle applicazioni, aumentando al contempo il potenziale di errore umano.

Alcuni elementi autonomi di una soluzione CNAPP rilevano le minacce, ma non automatizzano le funzionalità di correzione per evitare che i problemi diventino problemi più grandi. Senza una risposta automatizzata, volumi elevati di avvisi da analizzare possono ritardare il processo decisionale tra il personale di sicurezza con risorse limitate.

Una moderna piattaforma di sicurezza cloud dovrebbe fare molto di più che comunicare agli amministratori l'esistenza di un problema, ma dovrebbe consentire loro di adottare misure per affrontare i punti deboli.

Pilastro 5: competenza ed esperienza nel cloud e nella sicurezza

Comprendere e conoscere gli elementi di uno sviluppo cloud è fondamentale per capire quale strumento implementare per metterlo in sicurezza.

Lo scopo dei team di sicurezza è duplice. Si vuole implementare un approccio shi-ft-left, dove i problemi di sicurezza vengono identificati e corretti nelle prime fasi della pipeline ma, nel contempo, si vuole mantenere un controllo nella parte destra dove, a runtime, l'applicazione eroga i propri servizi ed è dove il codice viene eseguito.

Gli attaccanti possono permettersi di concentrare tutte le loro energie sul cloud, ma il team di sicurezza oberato di lavoro raramente gode dello stesso lusso. Per estendere le capacità dei difensori aziendali troppo ridotti per tenere il passo con il rischio del cloud, le organizzazioni devono investire in una continua formazione dei propri esperti di sicurezza oppure affidarsi ad un partner per colmare le lacune nelle competenze integrando una profonda esperienza nel cloud e nella sicurezza cloud.

Alcuni dei servizi professionali di esperti a cui ci si può affidare includono:

- rilevamento e risposta gestiti (MDR) 24 ore su 24, 7 giorni su 7 in tutti gli ambienti;
- risposta agli incidenti nel cloud;
- threat hunting per individuare potenziali minacce al cloud sin dalle fasi iniziali.

Criteri per scegliere l'approccio giusto

Un solido approccio alla sicurezza in cloud deve combinare capacità di rilevamento e risposta, basandosi sia su agent che senza agent, potendo coprire endpoint tradizionali ed ambienti ibridi e multi-cloud. L'abbinamento di tecnologia e copertura basate su agent e senza agent in un'unica piattaforma unificata, consente alle organizzazioni di avere visibilità su tutto ciò che accade nei diversi ambienti e di identificare e correggere rapidamente vulnerabilità ed errori di configurazione.

L'adozione dei microservizi richiede l'utilizzo di una soluzione capace di proteggere tanto i workload tradizionali quanto, ad esempio, i container che sono alla base dell'erogazione di servizi ed applicazioni. Le soluzioni devono distinguere l'attività dei container dall'attività di un host e di un nodo e questo deve valere anche per i container effimeri. Questo approccio permette di avere i dati necessari non solo per implementare una protezione efficace ma anche per effettuare attività forensi, non indirizzabili con soluzioni tradizionali.

Le piattaforme CNAPP progettate appositamente per il cloud offrono prestazioni, agilità e scalabilità notevolmente migliorate. Le soluzioni basate sul cloud possono essere implementate con successo in ambienti con decine di migliaia di workload, nodi e container nel giro di poche ore.

L'efficienza operativa deriva da procedure sicure in tutto l'arco della pipeline di sviluppo, arrivando sino alle fasi di runtime. Una piattaforma nativa del cloud non può non includere funzioni native di scalabilità, di consentire aggiornamenti continui per affiancare la dinamicità dello sviluppo applicativo e per stare al passo con il panorama delle minacce in rapida evoluzione di oggi.

Nel complesso, il raggiungimento di questi obiettivi migliora il livello di sicurezza complessivo dell'organizzazione ed aiuta a semplificare i flussi di lavoro di sicurezza, la condivisione delle conoscenze e le attività svolte in modo collaborativo.

La decisione di adottare una strategia CNAPP completa dipende dal business case di un'organizzazione per investire nella sicurezza del cloud. Una soluzione consolidata che raggruppi più funzionalità, offre il massimo valore dell'investimento e l'efficienza operativa.

	SMARTER		FASTER		MORE EFFICIENT
Capabilities	**1. Visibility**	**2. Threat Intelligence**	**3. Tool Consolidation**	**4. Automation**	**5. Expertise**
Impact	Stop attackers from hiding in blind spots	Understand modern adversaries	Work in a single unified console	Scale protection on demand	Gain efficiency through experts
Criteria	• Full coverage for hybrid and multi-cloud deployments • Run-time visibility • Continuous coverage (vs. 24-hour snapshots) • Discovery and visibility of all cloud resources • Ability to find and fix misconfigurations • CI/CD pipe scanning • Monitoring of cloud and privileged user accounts	• Knowledge of real-world attacks and TTPs of cloud-conscious adversaries worldwide • Threat intelligence integrated into cloud security	• Combination of proven agent-based and agentless technology for every cloud in one integrated console to see/stop everything everywhere	• Automated detection and response • Automated policies with built-in IOCs, IOAs, IOMs and compliance • Ability to find misconfigurations through pre-built image scanning • Automated runtime protection and malware analysis (e.g., sandboxing)	• 24/7 MDR for cloud • Managed, analyst-led cloud threat hunting • Managed cloud incident response (IR)
Operational efficiency gains		• Eliminate silos between disparate cloud security solutions • Easily deploy coverage to unprotected hosts			

Costruire la cyber resilience per la Space Economy

[A cura di Federica Maria Rita Livelli]

Negli ultimi anni, la Space Economy ha conosciuto una notevole crescita, con aziende private e Governi che investono ingenti risorse nelle reti satellitari, nell'esplorazione spaziale e nelle infrastrutture orbitali. Tuttavia, l'espansione della commercializzazione dello spazio, comporta sempre più l'adozione di solide misure di cybersecurity per proteggere le risorse "extraterrestri" dalle minacce informatiche.

FONTE IMMAGINE : https://www.pexels.com/it-it/foto/nuvole-nuvoloso-spazio-aereo-60133/

Grazie ai progressi tecnologici e agli investimenti sempre più consistenti, la Space Economy si è trasformata in un'industria multimiliardaria che abbraccia diversi settori, come la comunicazione satellitare, l'osservazione della Terra, il turismo spaziale e l'estrazione di asteroidi. Sistemi che si sono convertiti in infrastrutture critiche, oramai parte fondamentale della nostra vita quotidiana, garantendo il funzionamento ininterrotto dei sistemi di comunicazione globale, di navigazione e, permettendo, altresì, la condivisione dei dati.

Si prevede che la Space Economy continuerà a crescere in modo esponenziale nei prossimi anni, rendendo ancora più cruciale la protezione delle nostre infrastrutture spaziali.

Secondo quanto si evince dal recente rapporto "*Quilty Space 2023-2030*" della società di ricerca e consulenza americana Quilty Space vi sono indicatori positivi per una crescita sostenuta all'interno della base industriale spaziale, a fronte del continuo

proliferare delle mega-costellazioni a banda larga in orbita terrestre bassa che costituiscono circa l'85% di tutta la domanda satellitare in Occidente.

Inoltre, il report rivela che, se tutte le missioni pianificate dalle 350 costellazioni commerciali e governative analizzate da Quilty raggiungessero l'orbita, entro il 2030 sarebbero nello spazio ben 478.000 satelliti. Tuttavia, effettuando una valutazione ponderata delle probabilità, Quilty ha stimato che solo circa 20.000 satelliti riusciranno, probabilmente, a entrare in orbita. Un numero comunque considerevole e degno di attenzione e non privo di sfide da affrontare.

Poiché l'economia globale dipende sempre di più dalle risorse spaziali, dai dispositivi e dalle reti interconnesse, aumenta la necessità di affrontare in modo proattivo l'esposizione alle nuove minacce informatiche. La crescita alimentata dall'innovazione nello spazio e i cambiamenti nelle catene del valore che si interconnettono con ecosistemi terrestri, wireless e cloud avvengono parallelamente all'aumento delle capacità degli hacker nel trovare vulnerabilità nell'infrastruttura.

Pertanto, urge un completo cambio di paradigma su come affrontare le minacce di cybersecurity nei sistemi spaziali. Le tecniche tradizionali di cybersecurity incentrate sulla difesa del perimetro, il controllo degli accessi e la responsabilità non sono più sufficienti per prevenire le violazioni informatiche, comprese le minacce interne. Il modello di cybersecurity spaziale deve, quindi, spostarsi verso un'architettura di Zero Trust, che continuerà a mettere in discussione la sicurezza, la vulnerabilità e l'affidabilità in modo continuo.

Space Economy & sfide

Entrando nel dettaglio, la crescita della Space Economy comporta numerose sfide e, precisamente:

Attacchi informatici sofisticati - Il settore spaziale è un obiettivo primario per attacchi informatici sofisticati da parte di nation-state e gruppi APT (*Advanced Persistent Threat Group* – i.e. gruppi di hacker altamente sofisticati, spesso associati a entità statali o gruppi criminali altamente organizzati), che possono comportare l'accesso non autorizzato ai dati o l'interruzione dei sistemi critici. Inoltre, è doveroso evidenziare che i sistemi spaziali sono in gran parte basati su risorse legacy sviluppate quando la cybersecurity non era un requisito prioritario. Ne consegue che, oggigiorno, la cybersecurity degli asset spaziali in orbita e a terra è diventata motivo di grande preoccupazione e le agenzie di tutto il mondo stanno adottando strategie di cybersecurity per affrontare queste sfide in modo tempestivo.

Le principali tipologie di minacce informatiche agli asset spaziali possono essere suddivise nelle seguenti macro-categorie:

- **Attacchi elettronici -** Essi mirano ai vettori spaziali attraverso cui i sistemi spaziali trasmettono e ricevono dati, provocando interferenze o falsificazioni dei segnali a radiofrequenza (RF), sottoforma di attacchi:
  - **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
  - **Spoofing:** pratica informatica che manipola o falsifica l'identità o l'origine di un determinato messaggio, pacchetto di dati o sorgente di informazioni al fine di ingannare o trarre vantaggio.
  - **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.
- **Attacchi procedurali e al personale -** Si tratta di attacchi che riguardano gli aspetti non tecnici, che possono avere un impatto significativo sulla sicurezza complessiva, quali, ad esempio, gli attacchi di social engineering.
- **Attacchi informatici -** Si tratta di attacchi che mirano ai dati e ai sistemi sottostanti utilizzati per gestire, trasmettere ed elaborare i dati e che possono comportare il monitoraggio dei modelli di traffico dei dati, l'inserimento di dati falsi o corrotti nel sistema e l'hacking delle reti di comunicazione e dei sistemi di controllo dei satelliti.

Rischi della catena di fornitura - Il settore spaziale fa affidamento su complesse catene di approvvigionamento globali, che possono creare vulnerabilità nella catena di approvvigionamento che gli aggressori possono sfruttare per ottenere ulteriore accesso ai sistemi critici.

Errore umano - Il settore spaziale coinvolge sistemi complessi e alti livelli di interazione umana. Pertanto, l'errore umano può creare rischi per la sicurezza come perdite di dati involontarie o configurazioni errate del sistema.

Visibilità limitata - La complessità e le ubicazioni remote dei sistemi spaziali rendono difficile rilevare e rispondere agli incidenti di cybersecurity e affrontare le vulnerabilità.

Space Economy & Cybersecurity: come affrontare le sfide

Partendo dal presupposto che garantire la cybersecurity e la resilienza delle risorse spaziali è fondamentale per l'economia e per la sicurezza a livello globale, è altrettanto evidente, a livello europeo, come la collaborazione tra gli Stati membri e l'industria sia quanto mai strategica per affrontare questa sfida complessa, mettendo in essere

una stretta e ben strutturata strategia collaborativa tra tutti gli stakeholder del settore spaziale. Inoltre, la cybersecurity deve essere integrata nella supply chain spaziale attraverso l'utilizzo di soluzioni di cloud sicuro, di comunicazioni critiche e di resilienza.

È necessario, quindi, implementare misure di sicurezza informatica avanzate che garantiscano la trasmissione sicura dei dati. Alcune delle misure di sicurezza informatica che possono essere utilizzate includono:

- **Protocolli di comunicazione sicuri e tecniche di crittografia -** Mantenere sicure le comunicazioni tra le stazioni terrestri e spaziali è un elemento cruciale della sicurezza informatica spaziale. L'uso di tecniche di crittografia garantirà una linea di comunicazione protetta che può essere vitale per la sicurezza di vite, dati e tecnologia.
- **Meccanismi di autenticazione e controllo degli accessi -** Garantire la corretta gestione degli accessi garantirà che solo il personale autorizzato abbia accesso alle infrastrutture critiche. In tal senso, l'utilizzo di una politica zero-trust contribuirà notevolmente a mantenere sicuro il sistema spaziale.
- **Sistemi di rilevamento e prevenzione delle intrusioni -** Le minacce informatiche devono essere identificate, isolate e mitigate dall'infrastruttura in atto. Le missioni spaziali devono utilizzare il rilevamento attivo delle intrusioni e la threat intelligence per evitare gli attacchi informatici prima che possano causare danni al sistema.
- **Strategie di crittografia e protezione dei dati -** Gli hacker mirano a esfiltrare i dati satellitari o manipolare i dati per fornire trasmissioni errate. Con la crittografia dei dati, le comunicazioni sono sicure e i dati non possono essere rubati, manipolati o danneggiati.

La spinta verso un ambiente aziendale dinamico e multi-dominio con reti definite dal software e applicazioni basate su cloud mette in discussione l'efficacia della sicurezza tradizionale, ne consegue che il settore della Space Economy dovrà adottare sempre più un approccio proattivo e difensivo, maggiormente strutturato in termini di tecnologia e di politiche di governance, poiché la crescente sofisticazione dei tradizionali attacchi saranno in grado di bypassare le tradizionali protezioni basate sul perimetro.

Inoltre, si tratterà di effettuare periodiche valutazioni avanzate del rischio e utilizzare strumenti difensivi automatizzati progettati specificamente per i sistemi spaziali in modo da aumentare la complessità e i costi per i cyber criminali e, al contempo, migliorare la resilienza del sistema spazio.

La Governance della Space Economy

L'espandersi della Space Economy rende necessaria, altresì, una governance spaziale alla base della strategia geopolitica dei vari Paesi e non solo delle più grandi nazioni spaziali.

Attualmente, l'architettura di governance esistente risulta debole, frammentaria e inadeguata al contesto attuale. Inoltre, la complessità aumenta a causa della presenza di attori diversi, volumi di dati diversi e casi d'uso diversi. Inoltre, lo scenario contingente presenta molteplici sfide e rischi derivanti dalla prevalenza degli interessi personali a breve termine dei player privati o degli Stati, a discapito della stabilità a lungo termine e degli interessi comuni globali. Pertanto, diventa di estrema importanza costruire un quadro di governance che promuova una distribuzione più equa delle risorse tra i Paesi sviluppati e quelli in via di sviluppo.

Space Economy, Cybersecurity e contesto normativo

Già nel 2022, il World Economic Forum aveva identificato, tra le principali minacce globali, le dipendenze digitali, le vulnerabilità informatiche, l'affollamento e la competizione nello spazio. Tuttavia, è ancora in fase di definizione un quadro di leggi e norme internazionali che tengano conto delle minacce informatiche nello spazio e siano in grado di garantire un ambiente spaziale sicuro, protetto e sostenibile per tutti.

In quest'ottica, a livello europeo, vanno interpretate le recenti direttive e i recenti regolamenti, quali: Cyber Resilience Act, Nuovo Regolamento Macchine e NIS2 e AI Act (in fase di definizione). Si delinea una galassia normativa che adotta un approccio risk-based e resilience-based che implica necessariamente - da parte dei vari attori della Space Economy - l'implementazione dei principi di risk management, business continuity e cybersecurity. In particolare, la direttiva NIS2 riconosce il settore spaziale come un'entità essenziale, soggetta ai suoi requisiti di cybersecurity più rigorosi. Ma vediamo in dettaglio cosa comportano.

Focus su NIS2 e Space economy

La NIS2 pone un accento significativo sull'importanza della continuità aziendale, soprattutto a fronte di gravi incidenti informatici. Le aziende, gli enti governativi e i fornitori di infrastrutture critiche spaziali dovranno sviluppare e mantenere piani solidi per garantire il funzionamento ininterrotto dei loro servizi. Ciò include disposizioni in termini di:

- **Politica sulla sicurezza delle informazioni -** Un aspetto cruciale della sicurezza informatica è la valutazione del rischio. La direttiva NIS2 richiede alle aziende di valutare l'impatto potenziale di un attacco sulle loro risorse più vitali e di prestare

attenzione alle vulnerabilità della rete o agli incidenti segnalati da altri attori del settore. Inoltre, devono adottare un approccio proattivo nella gestione del rischio, implementando politiche solide di sicurezza delle informazioni per condurre un'analisi sistematica e approfondita dei rischi.

- **Continuità aziendale e gestione delle crisi -** La direttiva NIS2 si propone di garantire che le aziende siano in grado di mantenere la continuità delle proprie attività in caso di attacco informatico. Le organizzazioni devono avere un piano ben definito su come reagire a un attacco e su come riprendersi il più velocemente possibile, minimizzando le interruzioni. Questo piano deve essere verificabile e comprendere strategie per mitigare gli effetti dell'attacco, ripristinare i servizi e riprendere le operazioni normali nel minor tempo possibile.
- **Ripristino dei sistemi -** La direttiva NIS2 richiede alle organizzazioni di avere piani completi di ripristino dei sistemi. Questo implica lo sviluppo di strategie per recuperare rapidamente dagli incidenti informatici e per ripristinare le normali operazioni. L'obiettivo principale è ridurre al minimo i tempi di inattività e le interruzioni, garantendo una pronta risposta agli attacchi informatici e una rapida ripresa delle attività.
- **Procedure di emergenza -** Secondo la direttiva NIS2, le organizzazioni devono definire e implementare procedure di emergenza che vengono attivate in caso di incidente informatico. Queste procedure devono essere documentate in modo accurato, testate regolarmente e includere un chiaro percorso di escalation per il processo decisionale. L'obiettivo è garantire una risposta efficace e tempestiva agli incidenti informatici, consentendo una gestione adeguata dell'emergenza e una rapida presa di decisioni per mitigare gli effetti negativi e ripristinare le normali operazioni.
- **Squadre di risposta alle crisi -** Uno degli aspetti critici di NIS2 è la formazione di squadre di risposta alle crisi. Ovvero, team composti da esperti in grado di valutare e mitigare rapidamente le minacce informatiche. Questi specialisti svolgono un ruolo fondamentale nel coordinare la risposta dell'organizzazione a un incidente informatico.
- **Prevenzione, rilevamento e risposta agli incidenti -** Secondo la direttiva NIS2, le organizzazioni devono avere piani di backup e di ripristino, condurre esercitazioni e informare tutte le parti interessate. Dopo aver identificato le vulnerabilità più significative, le organizzazioni devono implementare procedure chiare per prevenire gli attacchi e definire metodi per rilevare potenziali incidenti. Questo si traduce in un piano di risposta agli incidenti che include una catena di comando trasparente per l'implementazione delle azioni necessarie. L'obiettivo è garantire una gestione efficace degli incidenti informatici, con procedure ben definite per proteggere le risorse e ripristinare le operazioni nel minor tempo possibile.

- **Divulgazione delle vulnerabilità -** NIS 2 richiederà una divulgazione e una gestione delle vulnerabilità più trasparenti. Le organizzazioni dovranno adoperarsi a fornire modalità affinché il pubblico possa segnalare eventuali vulnerabilità e garantire che la funzione competente agisca in base a tali informazioni. Se un'organizzazione identifica una vulnerabilità all'interno della propria rete, la nuova direttiva impone loro di divulgarla. La divulgazione di tali vulnerabilità sosterrà la lotta contro la criminalità informatica e garantirà che non vengano sfruttate altrove.
- **Sicurezza della catena di fornitura -** La sicurezza della catena di fornitura è da tempo sotto esame a livello globale. NIS 2 richiede alle organizzazioni di considerare le vulnerabilità di ciascuno dei propri fornitori e prestatori di servizi e verificarne le pratiche di cybersecurity. Ciò richiederà ai fornitori di sviluppare piani di audit per la conformità, oltre a migliorare il supporto alla sicurezza durante l'intero ciclo di vita di qualsiasi sistema spaziale, garantendo di essere in grado di affrontare le minacce informatiche in modo efficace e di soddisfare le normative di cybersecurity in continua evoluzione.

NIS 2 impone, inoltre, approcci aggiornati in termini di:

- **Segnalazione di incidenti -** Secondo la direttiva NIS2 aggiornata, le aziende sono tenute a presentare una serie di relazioni in caso di incidenti significativi. Devono fornire una relazione iniziale entro 24 ore dal momento in cui vengono a conoscenza dell'incidente, una notifica completa entro 72 ore e una relazione finale entro un mese alle autorità competenti, al Computer Security Incident Response Team (CSIRT) e, in alcuni casi, ai loro clienti.
  È importante sottolineare che, secondo la NIS2, un incidente è considerato "significativo" se ha causato o è in grado di causare gravi interruzioni operative del servizio o perdite finanziarie, o se ha avuto un impatto significativo su altre aziende o utenti.
- **Collaborazione -** La prima direttiva NIS non considerava i diversi modi in cui operavano i singoli Paesi. Pertanto, NIS 2 si pone come scopo:
  - Maggiore condivisione dei dati tra le autorità.
  - Richiesta alle autorità di partecipare alla risposta agli incidenti a livello UE piuttosto che a livello nazionale.
  - Istituzione di meccanismi di cooperazione tra le autorità nazionali di cybersecurity e introduzione di una rete europea per le crisi informatiche (EU-CyCLONe) in modo da garantire una gestione coordinata degli incidenti e delle crisi di cybersecurity nel settore della Space Economy.

Conclusione

La crescita alimentata dall'innovazione nello spazio e i cambiamenti nelle catene del valore - che si interconnettono con ecosistemi terrestri, wireless e cloud - avvengono parallelamente all'aumento delle capacità degli hacker nel trovare vulnerabilità nell'infrastruttura spaziale. Pertanto, urge un completo cambio di paradigma su come affrontare le minacce di cybersecurity dirette al settore della Space Economy.

Le tecniche tradizionali di cybersecurity incentrate sulla difesa del perimetro, il controllo degli accessi e la responsabilità non sono più sufficienti per prevenire le violazioni informatiche, comprese le minacce interne. Il modello di cybersecurity spaziale deve spostarsi verso un'architettura che continuerà a mettere in discussione la sicurezza, la vulnerabilità e l'affidabilità in modo continuo.

La collaborazione tra le parti interessate, l'uso di tecnologie innovative e un approccio proattivo sono fondamentali per garantire la sicurezza e la protezione delle risorse spaziali. Investendo nella cybersecurity, non solo proteggiamo i nostri investimenti nello spazio, ma gettiamo anche le basi per un futuro sicuro e prospero nell'ultima frontiera.

Di fatto, si tratta di monitorare gli sviluppi in materia di sicurezza spaziale e il loro legame con la cybersecurity, lavorando insieme per trovare modi efficaci per migliorare l'utilizzo pacifico dello spazio attraverso la governance, le leggi e le norme applicative.

È importante ricordare, altresì, che la cybersecurity coinvolge non solo la tecnologia, ma anche le persone e i processi. Pertanto, è fondamentale promuovere una forte cultura della cybersecurity a livello nazionale e internazionale, soprattutto per affrontare le sfide che coinvolgono i domini cyber e spaziale attraverso la sensibilizzazione e la formazione dei decisori e delle persone coinvolte nell'utilizzo e nella gestione dei sistemi spaziali.

Inoltre, la collaborazione tra i Paesi e le organizzazioni sovranazionali risulterà quanto mai strategica per affrontare le sfide congiunte della Space Economy. Ciò implicherà la condivisione delle migliori pratiche, lo scambio di informazioni sulle minacce e la cooperazione nella definizione di standard e normative comuni, al fine di garantire una cybersecurity efficace e coerente.

Fonti

- Articolo Il sole 24 ore – *Quasi 7000 satelliti orbitano intorno alla terra: chi li controlla*; https://www.infodata.ilsole24ore.com/2023/10/21/quasi-7-000-satelliti-orbitano-attorno-alla-terra-chi-li-controlla/?refresh_ce=1)
- Articolo - *Industry Report: demand for satellites is rising but not skyrocketing*; https://spacenews.com/industry-report-demand-for-satellites-is-rising-but-not-skyrocketing/
- European Commission, European Union Space Strategy for Security and Defence (JOIN/2023/9), 10 March 2023; https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52023JC0009
- European Commission, Space Strategy for Europe (COM/2016/705), 26 October 2016; https://eurlex.europa.eu/legal-content/en/TXT/?uri=celex:52016DC0705
- Direttiva NIS2; https://digital-strategy.ec.europa.eu/it/policies/nis2-directive

CSIRT Network: Incident Response per una Crisis Management di successo in un Contesto Internazionale

[A cura di Francesco De Feo, Serena Angela Gracco, Jari Iannucci e Vincenzo Iucci, NTT Data]

Nel contesto attuale, una singola e-mail di phishing o un solo account possono innescare una catena di eventi a valanga di indisponibilità che si portano ad una crisi permanente e duratura.

Sebbene le minacce di questo tipo siano già impegnative a livello nazionale, diventano ancor più complesse e impegnative in un contesto imprenditoriale internazionale. Affrontare con successo tali sfide richiede un impegno significativo.

Come gestire un tale scenario affinché una azienda internazionale possa continuare ad avere un futuro imprenditoriale?

Una risposta efficace è rappresentata dall'attuazione di un CSIRT Network con una prospettiva internazionale.

Affinché tale Network risulti efficace, è essenziale affrontare non solo gli aspetti tecnici di risposta e contenimento, ma anche quelli organizzativi, di comunicazione, legali e di caring dei clienti.

Il CSIRT Network non solo si pone come una difesa contro le minacce cibernetiche, ma costituisce anche la base per un autentico partenariato pubblico-privato. Solo attraverso un approccio integrato e cooperativo è possibile affrontare con successo le sfide sempre crescenti della sicurezza informatica su scala internazionale.

Scopo del Focus on

L'articolo propone un approccio efficace per la gestione di incidenti critici attraverso l'implementazione di un Network CSIRT in un contesto internazionale. L'obiettivo primario è illustrare un approccio completo finalizzato ad affrontare le complesse minacce cibernetiche che possono causare impatti devastanti su aziende operanti a livello globale.

L'analisi si focalizza sulle sfide specifiche che un'azienda internazionale deve affrontare nel campo della sicurezza informatica, considerando la complessità delle minacce e la diversità delle giurisdizioni. Si adotta un quadro completo che integra aspetti tecnici, organizzativi, legali e comunicativi, prendendo in considerazione le diversità linguistiche, culturali e giuridiche presenti a livello internazionale.

L'approccio proposto supera le barriere geografiche e culturali, consentendo di affrontare con successo le sfide sempre crescenti della sicurezza informatica a livello internazionale. La collaborazione internazionale emerge come elemento cruciale, poiché le minacce cibernetiche non conoscono confini geografici. L'obiettivo principale è quello di ridurre l'area esposta agli attacchi, assicurare una capacità operativa sufficiente in caso di incidente e ripristinare rapidamente ed efficacemente le normali condizioni operative. La necessità di sviluppare un programma di resilienza cibernetica diventa essenziale in un contesto in cui gli incidenti globali sono in costante aumento.

Normative locali

La conoscenza delle normative e i rapporti con le agenzie emergono come elementi fondamentali nella cybersecurity. Le normative stabiliscono standard indispensabili per garantire la sicurezza e proteggere i dati sensibili, come il GDPR in Europa. La conformità normativa è essenziale per evitare sanzioni legali e finanziarie.

La collaborazione con agenzie governative è fondamentale per affrontare minacce complesse, facilitando la comunicazione e la condivisione di informazioni. Il coordinamento globale e il supporto locale sono indispensabili, con il cyberspazio richiedendo una responsabilità condivisa a livello nazionale e globale.

Dall'analisi della Data Governance Act dell'UE, emergono tre attori principali: il detentore dei dati, l'intermediario dei dati e l'utente dei dati. La protezione dei dati è vitale, specialmente per la conformità al GDPR, con sfide nel conciliare ruoli e requisiti.

L'ingegneria della protezione dei dati è fondamentale per consentire la coesistenza efficace tra condivisione e protezione dei dati personali. La responsabilità e accountability del "controller" sono sottolineate, delineando blocchi principali per raggiungere l'accountability, cioè la chiara responsabilizzazione delle azioni compiute.

Gli intermediari dei dati svolgono un ruolo determinante nello scambio efficiente di dati, ma i loro ruoli e obblighi devono ancora essere definiti in pratica, con la necessità di accordi su misure tecniche e organizzative. In sintesi, la complessità della data sovereignty nel contesto globale richiede un costante adattamento alle normative in evoluzione e un approccio informato per garantire la conformità e mantenere la fiducia dei clienti e partner.

Analisi dei Major Incident

Un "major incident" in cybersecurity rappresenta un evento critico che minaccia gravemente la sicurezza informatica di un'organizzazione, derivante da attacchi sofisticati, violazioni di dati sensibili o compromissione di sistemi vitali.

La gestione di tali incidenti richiede una risposta tempestiva e coordinata per limitare danni, identificare l'estensione dell'attacco e ripristinare la sicurezza del sistema. Coinvolge team specializzati di sicurezza informatica, risposta agli incidenti e comunicazione per mitigare gli impatti negativi e ripristinare la fiducia delle parti interessate.

Le principali minacce comprendono la compromissione di dati sensibili, l'interruzione dei servizi critici, danni reputazionali, perdite finanziarie, riduzione della produttività, violazioni della conformità normativa, attacchi ransomware, impatti sulle relazioni commerciali, aumento dei costi di sicurezza e la perdita di fiducia da parte di clienti, dipendenti e partner. Affrontare efficacemente tali situazioni richiede prontezza, pianificazione e investimenti in misure di sicurezza supplementari per prevenire futuri attacchi.

Dati statistici

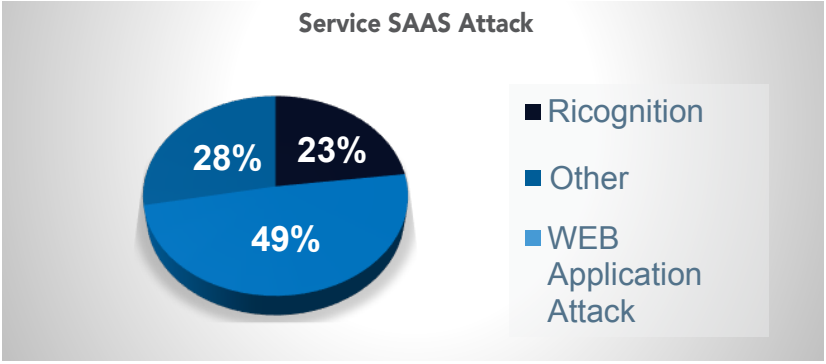
Top 5 settori più colpiti

I settori delle infrastrutture critiche e della catena di approvvigionamento sono rimasti obiettivi di alto valore. Poiché Tecnologia, Manifatturiero e Trasporto/Distribuzione sono fortemente integrati in questi aspetti cruciali della vita quotidiana, tali industrie sono rimaste nei nostri primi 5 settori più colpiti.

Il settore pubblico ha registrato il più grande aumento nell'ultimo anno, passando dalla posizione sei nel 2021 alla quattro nel 2022, un cambiamento attribuibile al clima geopolitico in evoluzione. Come l'anno scorso, l'Istruzione è rimasta nei primi 5 settori più colpiti, principalmente a causa degli attacchi a Microsoft Office e del criptomining derivante dai dispositivi degli studenti e dalle reti più aperte in molti campus.

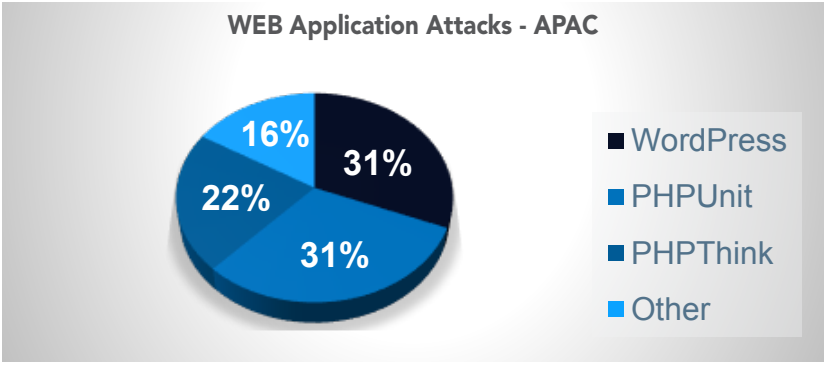
Attacchi al cloud e ai servizi SaaS

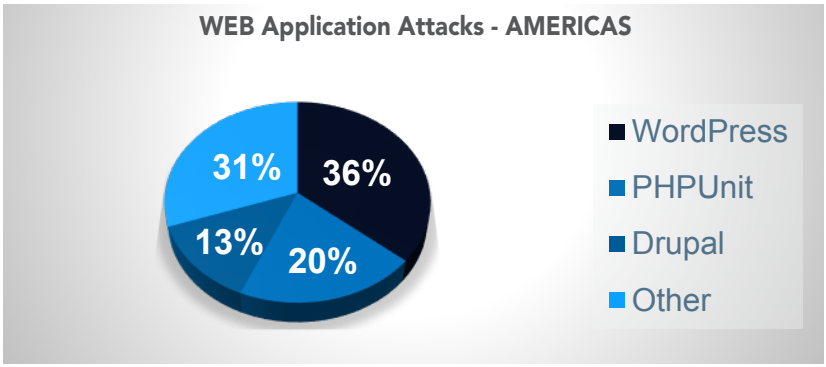
Come previsto, gli attacchi al cloud e ai servizi SaaS hanno continuato ad aumentare, come evidenziato dai dati del Global Threat Intelligence Center (GTIC). Minacce alle applicazioni basate su web e desktop costituivano il 70% degli attacchi. I software di Content Management System (CMS) come WordPress, i prodotti Apache e le utilità come Log4J e i prodotti Atlassian come Confluence rappresentavano circa l'80% degli obiettivi ospitati sul web. Questa tendenza è stata ulteriormente evidenziata dalle vulnerabilità critiche in prodotti come JIRA, Confluence e Bitbucket, che sono state corrette durante l'anno ma potevano portare al takeover dell'account.

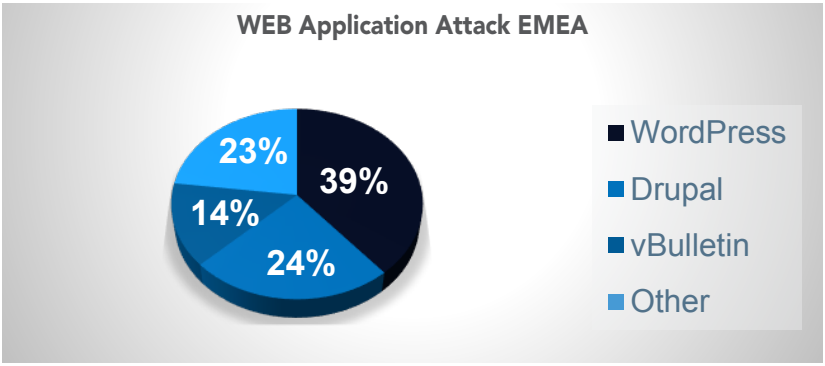


Attacchi alle applicazioni web

A livello globale, gli attacchi contro software CMS, plugin e applicazioni web PHP sono distribuiti uniformemente. WordPress è il CMS più attaccato nelle Americhe, nell'APAC e nell'EMEA, nonostante la maggior parte degli host che lo utilizzano si trovi negli Stati Uniti. Gli attacchi su molte applicazioni sono basati su exploit integrati in malware e botnet, diversamente dalle campagne mirate. Ad esempio, un trojan Linux in linguaggio Go ha preso di mira WordPress nel 2022. Questo targeting è riflesso nell'aumento del volume di attacchi osservato dal GTIC, che non è concentrato in una singola regione. Inoltre, sono stati registrati aumenti negli attacchi contro Realtek, con vulnerabilità integrate in botnet come Mirai, Mozi e, nel 2022, RedGoBot.



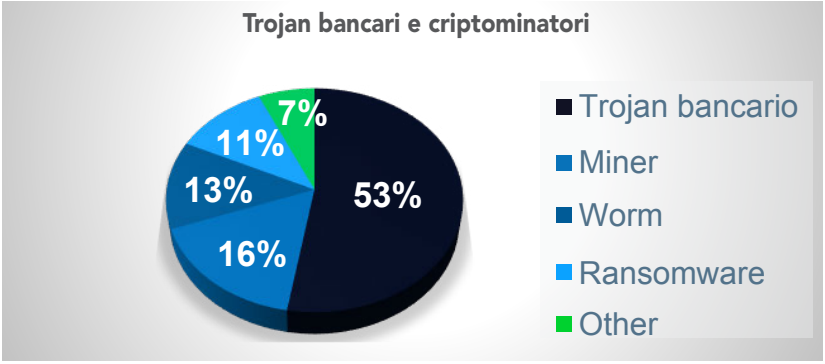




I chipset Realtek, presenti in numerosi dispositivi IoT, sono stati maggiormente mirati nelle Americhe, con una prevalenza nel settore della Tecnologia al 57%.

Trojan bancari e criptominatori

I trojan bancari hanno registrato un lieve calo rispetto all'anno scorso, ma rimangono comunque in testa. I criptominatori sono risaliti dopo una pausa nel 2021, nonostante la perdita di valore di molte valute. Queste fluttuazioni sono relativamente comuni poiché partner industriali, fornitori di hosting e forze dell'ordine cercano di disturbare e smantellare attori e infrastrutture malware, oltre alle risorgenze osservate in malware precedentemente disturbati, come Emotet. Il malware sta evolvendo più rapidamente, con alcune varianti che cambiano più dei loro Tactics, Techniques, and Procedures (TTPs); ad esempio, Ursnif ha abbandonato la capacità di furto finanziario con una nuova variante.



Vulnerabilità ad alto impatto e più bersagliate

Il GTIC monitora attacchi mirati a vulnerabilità ad alto impatto, con il 75% con gravità critica o alta. Si dedica maggior attenzione a codice dannoso verso CVE con bassa complessità e alto impatto. Le vulnerabilità più colpite sono notoriamente conosciute. Nel 2023, l'Africa ha visto un aumento significativo di attacchi informatici, inclusi un attacco a un ISP in Nigeria, una campagna di phishing contro banche centrali e attacchi ransomware. La crisi economica globale ha colpito l'Africa, aumentando i rischi di attacchi informatici.

In Europa, la crisi ucraina ha influenzato i prezzi del petrolio e del gas, portando a nuove norme sulla gestione della catena di approvvigionamento. Il lavoro cloud e ibrido è diventato permanente, con aumenti di attacchi informatici durante la pandemia sia in Europa che in Africa. In Africa, gli attacchi informatici sono cresciuti del 300% dal 2020, suggerendo crisi persistenti nel 2024.

I CISO dovranno adottare rapidamente nuove contromisure, presidiare la sicurezza fondamentale e comprendere le nuove tecnologie. La Generative AI e la digital transformation rimarranno rilevanti.

Prodotto	CVE	Percentuale	CVSS
Apache Log4J	CVE-2021-44228	26.25%	10
Realtek SDK	CVE-2021-35394	5.02%	9.8
Spring Cloud	CVE-2022-22963	2.93%	9.8

Supporto alla Gestione degli Incidenti Cyber

Caratteristiche della Gestione degli Incidenti

La gestione degli incidenti gioca un ruolo cruciale nella difesa aziendale, concentrandosi su identificazione, risposta e mitigazione di eventi indesiderati. Questo processo è fondamentale per affrontare minacce che potrebbero mettere a rischio le operazioni e la sicurezza delle informazioni. Esso inizia con una preparazione accurata, creando piani dettagliati e assegnando ruoli e responsabilità.

Rilevare tempestivamente gli incidenti è vitale, usando sistemi di monitoraggio avanzati per individuare comportamenti sospetti. Una risposta rapida è essenziale per limitare i danni e tornare alla normalità, con un team addestrato a guidare l'azione. Segue un'indagine approfondita per comprendere cause e impatti, alimentando un ciclo di apprendimento costante.

La comunicazione durante tutto il processo di gestione di un incident gioca un ruolo chiave, richiedendo trasparenza con dipendenti, clienti e autorità regolatorie. La gestione degli incidenti deve rispettare normative e leggi sulla protezione dei dati. Questo processo dinamico richiede un equilibrio tra preparazione, risposta, analisi e miglioramento continuo.

Skills necessarie e metodologie di indagine standardizzate

Le minacce alla sicurezza informatica costituiscono un problema crescente per tutte le organizzazioni con dati da proteggere e non solo, creando una forte domanda di professionisti altamente qualificati. Le competenze necessarie per affrontare sfide sempre più complesse possono essere divise in due categorie principali: competenze tecniche e competenze trasversali.

Il primo gruppo, quello delle competenze tecniche, richiede una comprensione funzionale dei sistemi operativi, una solida conoscenza delle reti informatiche e del cloud computing, la capacità di progettare e valutare l'architettura di rete, competenza in linguaggi di programmazione come Java, Python e C++, familiarità con piattaforme di database come MySQL, e comprensione dei protocolli per rilevare e prevenire violazioni del firewall. Inoltre, è essenziale padroneggiare i principi di base degli antivirus, delle VPN e dei firewall, nonché condurre verifiche di sicurezza per preparare difese efficaci contro gli attacchi informatici.

Il secondo gruppo, quello delle competenze trasversali, è altrettanto critico. Capacità come la leadership sono fondamentali, e la flessibilità e l'adattabilità sono necessarie per prosperare professionalmente. La natura mutevole della sicurezza informatica richiede un continuo sviluppo di competenze trasversali per affrontare le sfide in modo efficace.

Per quanto riguarda la gestione degli incidenti, la standardizzazione del processo emerge come pilastro fondamentale, riducendo significativamente il tempo necessario per risolverli. Questo approccio sistematico e strutturato facilita la cattura e l'analisi accurata dei dati rilevanti, semplificando la comprensione degli eventi e consentendo risposte tempestive e mirate. L'implementazione di metodologie standardizzate promuove la coerenza nelle azioni intraprese, favorendo la collaborazione e la condivisione efficace delle informazioni.

In ottica proattiva, l'uso di metodologie standardizzate migliora la resilienza organizzativa, limitando gli impatti negativi degli incidenti e rafforzando la capacità di fronteggiare futuri eventi. La standardizzazione non solo crea un framework robusto ma contribuisce anche a un apprendimento continuo e all'evoluzione costante delle strategie di sicurezza informatica. La combinazione di competenze tecniche e trasversali è essenziale per affrontare le sfide in rapida evoluzione del campo della sicurezza informatica.

IoC Exchange, Deception, Threat Intelligence Feeds

L'integrazione sinergica dell'Exchange di Indicatori di Compromissione (IoC), delle tecniche di Deception e dei feed di Threat Intelligence emerge come un approccio strategico essenziale nella progettazione di un sistema di sicurezza informatica robusto e proattivo. Questa combinazione sinergica di risorse avanzate agisce come un baluardo preventivo, mirato a prevenire incidenti e a rafforzare le difese dell'ambiente digitale.

L'utilizzo dell'IoC Exchange permette una rapida condivisione di informazioni sugli indicatori di compromissione tra diversi componenti del sistema di sicurezza. Ciò facilita un'applicazione tempestiva di contromisure, basate su dati in tempo reale, che contribuiscono a prevenire la diffusione di potenziali minacce. Inoltre, la centralizzazione e la standardizzazione degli IoC favoriscono un monitoraggio proattivo e una risposta immediata, riducendo il rischio di exploit e intrusioni.

Inoltre, la presenza di una piattaforma proprietaria di Threat Intelligence, centralizzata e basata sui vari feeds dei diversi team, ci consente di adottare un approccio proattivo anche durante l'analisi di diversi attacchi, assicurando così una risposta più rapida all'incidente.

Le tecniche di Deception, tra cui le honeypots, aggiungono un ulteriore strato di difesa, creando un ambiente simulato che inganna gli attaccanti e li indirizza lontano dai veri asset critici. L'utilizzo delle honeypots, in particolare, offre una prospettiva unica, consentendo di studiare da vicino gli attaccanti e le loro tattiche senza compromet-

tere la sicurezza effettiva dell'organizzazione. Questa forma di "trappola" cibernetica non solo distoglie l'attenzione degli aggressori, ma fornisce anche un'opportunità unica per analizzare le tattiche, le tecniche e le procedure (TTP) degli attaccanti, contribuendo così a migliorare la preparazione dell'organizzazione contro futuri tentativi.

L'integrazione di feed di Threat Intelligence completa questo quadro difensivo, fornendo informazioni aggiornate sulle ultime minacce e tendenze del panorama cibernetico. La comprensione approfondita di queste informazioni consente di adattare le strategie di sicurezza in tempo reale, anticipando e mitigando potenziali rischi.

L'interconnessione efficace di IoC Exchange, tecniche di Deception e feed di Threat Intelligence non solo eleva la resilienza dell'organizzazione, ma costituisce una barriera proattiva contro le sempre evolventi minacce informatiche, promuovendo una difesa informatica agile e robusta

Follow-the-sun e know-how distribuito sulle tecnologie

L'adozione di un modello "Follow-the-Sun" rappresenta una strategia chiave per garantire una copertura ininterrotta e globale nelle attività operative. Questo approccio si traduce in un flusso di lavoro senza interruzioni, poiché le responsabilità vengono trasferite tra i team in diverse fusi orari, assicurando una sorveglianza costante e una prontezza operativa 24/7. La sinergia di team distribuiti geograficamente non solo consente di estendere la copertura temporale, ma anche di sfruttare al massimo le competenze specifiche di ciascun team, creando un ambiente operativo dinamico e altamente responsivo.

Parallelamente, la distribuzione del know-how su diverse tecnologie emerge come un elemento cruciale nella costruzione di una risposta agli incidenti altamente specializzata e verticalizzata. Questa diversificazione delle competenze non solo accresce la profondità della conoscenza, ma facilita anche l'adattamento alle mutevoli minacce digitali e alle varie tecnologie coinvolte. La specializzazione tecnologica si rivela fondamentale per affrontare in modo efficace incidenti specifici legati a determinate piattaforme o sistemi, garantendo un livello di competenza ottimale nella gestione degli eventi critici.

In sintesi, l'implementazione del modello "Follow-the-Sun" e la diffusione strategica del know-how su diverse tecnologie si combinano sinergicamente per creare un approccio operativo robusto, in grado di affrontare le sfide di sicurezza informatica in modo continuativo e altamente specializzato. La copertura continua e la verticalità nella risposta agli incidenti diventano così elementi fondamentali per garantire un ambiente digitale sicuro e resilient.

Approccio Zero Trust e fasi di gestione di un Incident

L'approccio Zero Trust rappresenta una filosofia di sicurezza informatica che sfida il tradizionale modello di fiducia implicita all'interno di una rete aziendale. La Pubblicazione Speciale NIST 800-207 ha delineato un insieme completo di principi zero trust e ha fatto riferimento alle architetture zero trust (ZTA) per trasformare quei concetti in realtà. Una chiave di volta nel paradigma delle ZTA è il cambiamento di focalizzazione dai controlli di sicurezza basati su segmentazione e isolamento utilizzando parametri di rete (ad esempio, indirizzi Internet Protocol (IP), subnet, perimetro) alle identità.

In un contesto Zero Trust, ogni utente, dispositivo o sistema è trattato come potenzialmente non fidato, richiedendo autenticazione continua e rigorosi controlli di accesso. Questo approccio mira a mitigare i rischi di sicurezza, considerando che le minacce possono provenire sia dall'esterno che dall'interno. In termini di gestione degli incidenti, il processo può essere suddiviso in diverse fasi chiave. La prima fase coinvolge la rilevazione tempestiva di un potenziale incidente attraverso strumenti avanzati di monitoraggio e analisi dei comportamenti anomali. Successivamente, si passa alla fase di analisi approfondita, comprendente la determinazione delle cause, l'estensione dell'incidente e l'identificazione degli asset colpiti. La risposta immediata è la terza fase, che prevede la mitigazione degli effetti e il contenimento dell'incidente. Infine, la fase di recupero coinvolge il ripristino delle normali operazioni e l'apprendimento dalle lezioni apprese per migliorare la resistenza futura. L'implementazione di un approccio Zero Trust contribuisce a rafforzare la sicurezza complessiva, mentre una gestione degli incidenti strutturata è essenziale per rispondere in modo efficace e tempestivo alle minacce emergenti.

Esperienze e Best Practice: caso internazionale

Nell'Incidente riportato di seguito, si è verificato un sfortunato attacco informatico quando un cliente il cui nome rimane confidenziale, è caduto vittima di un attacco informatico. Ecco un riassunto degli eventi chiave e del ruolo cruciale svolto nella gestione della crisi.

Panoramica dell'Attacco

Il cliente ha optato per un contratto di risposta agli incidenti (IR), promettendo assistenza entro un accordo di livello di servizio (SLA) di 4 ore. L'attacco è iniziato con uno scambio di e-mail apparentemente normale tra il cliente e i suoi partner. L'attaccante ha sfruttato questa comunicazione, inserendo un file dannoso durante una risposta via e-mail. L'infezione si è diffusa quando un utente della azienda coinvolta, fidandosi del mittente conosciuto, ha aperto il file. L'attaccante è riuscito con successo a infiltrarsi nel sistema, portando alla fuoriuscita di dati, a trasferimenti di dati ad alto volume non notati e alla successiva crittografia di tutti i sistemi IT su 385 siti.

Problemi Pre-Crittografia

Nonostante avesse processi e team di sicurezza informatica, il cliente ha affrontato sfide. Il Centro Operativo di Sicurezza (SOC) non era adeguatamente formato, non riuscendo a rilevare, prioritizzare ed analizzare la minaccia in modo professionale. Il SOC ha ignorato gli avvisi e, anche quando l'attacco è stato identificato, non sono stati avviati casi d'uso o procedure efficaci. Il cliente è entrato in modalità panico, suscitando l'attenzione totale della direzione solo dopo l'attacco.

Risposta e interventi

Una transizione rapida dalla modalità panico alla risoluzione strutturata ha coinvolto un'analisi dettagliata, l'arresto di attacchi aggiuntivi e l'avvio di compiti di recupero. Il supporto on-site è stato fornito a livello globale, superando le aspettative del cliente. La crisi ha evidenziato una mancanza di preparazione nei piani di continuità aziendale della vittima, generalmente orientati a guasti in sistemi isolati piuttosto che a uno spegnimento completo dell'IT.

Principali interventi:

- analisi strutturata e pianificazione del recupero;
- prevenzione di attacchi aggiuntivi attraverso analisi approfondite;
- attivazione di sistemi di comunicazione di emergenza e migrazione rapida verso servizi cloud;
- implementazione di automazione della sicurezza (SOAR) per la rapida distribuzione di strumenti;
- analisi dettagliata dei backup infetti e supporto durante il ripristino;
- implementazione di ulteriori misure di sicurezza informatica in IT e OT;
- monitoraggio continuo attraverso servizi di sicurezza gestiti e UMDR.

L'incidente sottolinea le lezioni cruciali per le organizzazioni:

- aspettarsi l'imprevisto; gli incidenti possono essere peggiori del previsto;
- essere proattivi e addestrare per vari scenari di sicurezza informatica;
- formare il personale di sicurezza informatica e IT per rispondere in modo efficace;
- sfruttare tecnologie efficienti ed abbracciare l'automazione della sicurezza informatica;
- collaborare con partner esperti per un supporto completo in una crisi informatica.

In conclusione, l'Incidente serve come un forte richiamo sulle minacce informatiche in evoluzione e sull'importanza di misure robuste di sicurezza informatica, preparazione e collaborazione con partner esperti.

Conclusioni

In conclusione, il presente studio ha delineato in modo approfondito l'importanza della collaborazione internazionale nel contesto della gestione degli incidenti cyber, sottolineando il ruolo cruciale dei CSIRT Network nell'affrontare le minacce emergenti alla sicurezza informatica. La crescente complessità delle minacce digitali richiede un approccio olistico e collaborativo, che tenga conto delle diversità normative e culturali esistenti nei vari contesti globali. Come prossimo passo nella gestione degli incidenti cyber su scala internazionale, è essenziale sviluppare un quadro normativo condiviso che faciliti la cooperazione tra le nazioni, rispettando al contempo le specificità locali. Inoltre, l'implementazione di tecnologie avanzate, come l'intelligenza artificiale e l'apprendimento automatico, può rivestire un ruolo chiave nel migliorare la capacità di rilevamento e risposta, contribuendo così a un'efficace mitigazione degli incidenti informatici. Allo stesso tempo, è fondamentale investire nelle competenze e nella formazione del personale, al fine di garantire una risposta rapida ed efficiente alle minacce sempre più sofisticate. In definitiva, solo attraverso un impegno collettivo, con il coinvolgimento attivo di tutte le parti interessate, sarà possibile costruire un futuro resiliente e sicuro nella gestione degli incidenti cyber su scala internazionale.

Riferimenti

- https://inno3.it/2023/12/04/aradori-ntt-data-lavorare-alla-cyber-resiliency/
- https://us.nttdata.com/en/-/media/NTTDataAmerica/Files/gated-asset/2023-NTTSH-GTIR-Cybersecurity-Report.pdf
- https://dam-americas.nttdata.com/api/public/content/672544-2021-Global-Threat-Intelligence-Report-full-report.pdf
- https://dam-americas.nttdata.com/api/public/content/672545-2020-Global-Threat-Intelligence-Report-Full-Technical-Report.pdf
- https://csrc.nist.gov/pubs/sp/800/207/final
- https://csrc.nist.gov/pubs/sp/800/207/a/final
- https://cyberdefensematrix.com/
- https://www.okta.com/state-of-zero-trust/#:~:text=Our%20report%20finds%20growing%20adoption,within%20the%20next%2018%20months.
- https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf
- https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- https://www.cybertrends.it/evoluzione-degli-attacchi-informatici-in-africa-ed-europa-nel-2023/
- https://www.orangecyberdefense.com/global/security-navigator?utm_source=linkedin&utm_medium=social&utm_campaign=sn2024
- https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces

Intelligenza Artificiale e Automazione: le chiavi per rivoluzionare il SOC

[A cura di Umberto Pirovano, PaloAlto Networks]

Nell'attuale contesto di rivoluzione tecnologica anche i "cattivi" possono aggiungere al loro arsenale nuove tecnologie quali ML, AI, e automazione per velocizzare e rendere "smart" ogni fase dei loro attacchi. In questa situazione i Security Operation Centers (SOC) costruiti attorno a tecnologie legacy - quali i Security Information and Event Management (SIEM) - non riescono a fornire una soluzione flessibile e scalabile che possa sostenere i processi di trasformazione digitale, le iniziative di cloud transformation e le moderne campagne di attacco.

L'espansione della superficie di attacco delle aziende ha portato con sé un aumento dei dati di security senza precedenti. Tuttavia la rete, gli endpoint, l'identità e i dati cloud rimangono in sistemi separati: la telemetria dell'endpoint è raccolta in un sistema di rilevamento e risposta (EDR), i dati cloud si trovano dispersi tra svariati strumenti di sicurezza cloud e non sono correlati tra loro, con la conseguenza che gli analisti SOC spesso devono analizzare manualmente i dati per dare inizio alla fase di triage e di conseguenza valutare quale azione intraprendere .

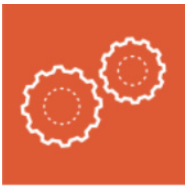
L'elevato numero di alert genera inevitabilmente un sovraccarico di lavoro sugli analisti, pertanto alcune minacce non vengono affrontate e i tempi di reazione rimangono discordanti dai tempi medi di exfiltration di dati da parte degli attaccanti. Gli analisti di sicurezza faticano a integrare nuovi flussi di dati provenienti dall'adozione di nuove tecnologie di cyber protection e a integrarli nei progressi di gestione degli eventi. I risultati sono prevedibili: alert fatigue, indagini lente e aggressori che si celano in rete per mesi.

L'evoluzione moderna ed efficace del SOC passa attraverso l'automazione, facendo leva su intelligenza artificiale e machine learning quali fondamenti tecnologici e permettendo la focalizzazione degli analisti sugli incidenti ad alto rischio. Oggigiorno condurre un veicolo a guida autonoma non richiede più il controllo diretto e costante da parte del conducente; allo stesso modo un SOC guidato dall'automazione gestisce la maggior parte degli alert ripetitivi e a basso rischio, esegue task e mitigazioni. Ciò consente agli analisti di lavorare su incidenti urgenti e ad alto impatto, mentre la piattaforma sottostante guida automaticamente il SOC verso risultati sicuri, imparando da ciascuno degli eventi valutati e arrivando a fornire informazioni e raccomandazioni efficaci al responsabile del SOC.

Ecco la nostra visione del SOC moderno: l'automazione tramite uso massivo di AI e ML è in grado di abbattere drasticamente i tempi medi di detection e remediation e, se utilizzato in un disegno di architettura cyber correttamente strutturata, consente il passaggio da un approccio detect/remediate ad uno predict/protect.

La rivoluzione di un SOC in chiave moderna richieda 6 elementi fondamentali:

1. Processi



I passi necessari affinche' un SOC possa identificare, investigare e mitigare un sospetto incidente di sicurezza.

2. Collaborazione

Tra individui, team e organizzazioni coinvolte a supporto dei SOC e delle attività di risposta agli incidenti.

3. People

Miglioramento continuo di capacità e conoscenza con l'adozione di piani di crescita professionale

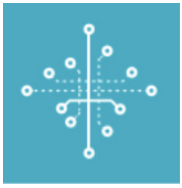
4. Business

Gli obiettivi di business di tutti gli stakeholders aziendali devono essere condivisi e integrati negli obiettivi di un SOC.

5. Visibilità

Consapevolezza real time delle attività del SOC generate da tentativi di attacco e campagne.

6. Tecnologie



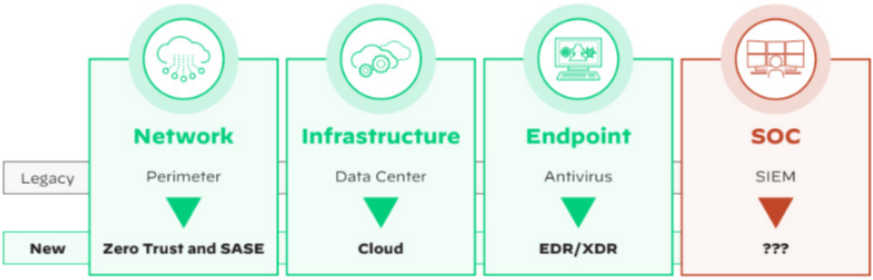
La combinazione di buoni dati e buoni modelli di AI/ML devono consentire tempi di risposta agli incidenti sempre più prossimi al real-time.

Uno sguardo al passato

Negli ultimi anni le esigenze dei SOC sono cambiate, ma il design dei SIEM utilizzati non si è evoluto di conseguenza. I sistemi di security information and event management (SIEM) hanno costituito il cuore tecnologico delle security operations per anni non riuscendo tuttavia a eliminare la deriva dell'overhead manuale e fornendo solo piccoli miglioramenti incrementali in confronto all'esplosione dei dati da analizzare. Le altre tecnologie che compongono l'architettura di cybersecurity si sono evolute:

- l'endpoint protection è passata dai sistemi legacy di antivirus all'endpoint detection and response (EDR) e poi all'extended detection and response (XDR);
- la network security si è evoluta da un concetto di protezione perimetrale verso un approccio globale di tipo Zero Trust e SASE;
- parte dei runtime si sono spostati dai datacenter on-prem al cloud, creando dispersione di applicazioni e dati come mai in precedenza.

Nonostante queste trasformazioni, i SIEM operano esattamente come operavano 20 anni fa.



Diversi sono i motivi che spiegano l'inerzia tecnologica nei SIEM:

- **utilizzo di tecnologie legacy:** molti SIEM sono stati sviluppati più di 10 anni fa e sono spesso basati su architetture obsolete che ne limitano la possibilità di adattamento alle nuove sfide;
- **complessità:** l'implementazione e la gestione dei SIEM sono spesso complesse e va considerata la necessità di tuning continuo per evitare falsi positivi o falsi negativi;
- **mancanza di innovazione:** il mercato dei SIEM è complesso e maturo che offre pochi incentivi ai vendor che vogliano innovare radicalmente le soluzioni;
- **difficoltà con le integrazioni:** è necessario che i SIEM si integrino con differenti tecnologie quali sistemi EDR, IDS, network traffic analysis (NTA). Cambiare le

tecnologie sulle quali i SIEM sono costruiti potrebbe causare problemi con le integrazioni interrompendo le security operations;
- **necessità di personalizzazione:** molte organizzazioni hanno pesantemente "customizzato" i propri SIEM per adattarli alle proprie esigenze. Cambiamenti radicali nelle architetture dei SIEM potrebbero richiedere pesanti riconfigurazioni da parte dei clienti;
- **aderenza alle normative:** molte organizzazioni utilizzano i SIEM per assicurare la compliance alle normative di sicurezza. Qualunque cambiamento può avere un impatto su questa necessità.

Il risultato è che, a fronte di un crescita esponenziale di dati da processare, la capacità di gestione razionale dei log rimane limitata, ribaltando l'incapacità di scalare su processi manuali a carico degli analisti.

Tuttavia questa rappresenta solo la punta di un iceberg di limitazioni che sono divenute via via più evidenti:
- mancanza di visibilità e contesto: i dati e gli alert arrivano da piattaforme di cybersecurity che coprono sempre più ambiti, dai sistemi di securizzazione del codice applicativo fino agli endpoints, dai sistemi anti-frode, ai sistemi di attack surface management
- Come conseguenze del punto precedente, aumentano la complessità nell' analisi e nelle investigazioni;
- la cosiddetta alert-fatigue, ovvero l'elevato "rumore" causato da alert che non si possono processare, soprattutto alert a bassa affidabilità che possono contenere informazioni utili;
- mancanza di automazione e orchestrazione, che costringe a task manuali e ripetitivi ed espone a errori umani, non garantendo l'esecuzione di playbook uniformi per famiglie di incidenti. Questo si ripercuote su tempi e SLA nei SOC
- difficoltà di raccogliere, processare e rendere operativi dati di threat intelligence.

La trasformazione del SOC Manuale

Il modello del "SOC manuale" - che fosse implementato on-prem o in cloud - si strutturava attorno alla figura dell'analista umano. Gli analisti sono quotidianamente coinvolti nella gestione di centinaia di alert ed eseguono triage manuali per la contestualizzazione dei dati, dedicando gran parte del loro tempo a falsi positivi e processi manuali.

Non appena il volume dei dati è aumentato, così come la loro complessità di integrazione (poiché provenienti da diversi sistemi) l'approccio umano-centrico si è rivelato

un anello debole. La capacità del SOC di operare correttamente ha subito un rapido decadimento, con un significativo impatto sulla gestione degli incidenti e sulla sua stessa vita.

L'evoluzione delle architetture di cybersecurity verso il concetto di "*piattaformizzazione*" e la modernizzazione del SOC non sono tra loro alternative, bensì entrambi elementi indispensabili per evolvere da un approccio cyber del tipo detect/response ad uno predict/prevent.

Secondo Leonardo da Vinci: "La semplicità è la suprema sofisticazione".

A seguito di acquisizioni, fusioni e della mancanza di standardizzazione per prodotti di sicurezza simili, molte organizzazioni si ritrovano con stack di sicurezza appesantiti da un numero elevato di strumenti. Si potrebbe dire che avere troppi strumenti comporta troppi problemi.

Avendo risorse tanto in ambienti cloud quanto on-premise, i team IT di sicurezza sono in difficoltà ad avere completa visibilità della loro superficie di attacco. Come si può sperare di conoscere la propria superficie di attacco se, ad esempio, non si ha un quadro chiaro dei fornitori di servizi cloud in uso e dei servizi che erogano (applicazioni e dati) e con quali flussi?

La diffusione incontrollata degli strumenti cyber può iniziare proprio con la distribuzione di una soluzione mirata per risolvere un problema specifico.

Tale approccio frammentario, combinato alla gestione di numerosi agenti, può (ironicamente) causare una maggiore vulnerabilita', con lacune causate da problemi derivanti dalla mancanza di interoperabilità e da una configurazione impropria.

Uno dei primi passi che un'organizzazione può intraprendere per ridurre l'impatto sulla sicurezza della proliferazione degli strumenti è l'audit di sistemi ed entità protette.

Identificare con precisione cosa viene protetto, quali eventi vengono impediti e il livello di criticità di applicazioni, dati e utenti, può dare priorità alla protezione delle risorse di alto valore e ad alto rischio.
L'adozione di una piattaforma cyber incentrata su condivisione di dati, orchestrazione e automazione nativa è quindi un passo cruciale verso il concetto di un SOC autonomo.

Il secondo elemento che richiede una innovazione radicale è quello dall'automazione e dell'orchestrazione.

L'analisi di un potenziale evento richiede diversi passaggi: innanzitutto la revisione dei log disponibili, poi la comparazione con dati di threat intelligence, necessaria per verificare eventuali indicatori noti di attività malevole.

Altro passaggio imprescindibile è la ricerca di dati mancanti per verificare eventuali altri passaggi nei cicli degli attacchi, la verifica intra e inter teams per evitare duplicazione di azioni e infine la necessaria valutazioni finale, ossia se l'alert in oggetto deve essere portato a un livello superiore o scartato o immediatamente rimediato e chiuso.

A posteriori - o anche durante il processo - resta la necessità di documentare eventuali azioni manuali applicate su vari sistemi.

Il numero degli alert a cui i SOC sono sottoposti cresce a ritmo elevatissimo e ben presto si raggiunge il punto in cui agli analisti è richiesto di concentrarsi solo sugli alert che vengono considerati ad alta priorità - a torto o a ragione- scartando gli altri in modalità silente .

Spesso in fase di triage ci si trova nella condizione di non avere abbastanza dati di contesto per determinare il reale valore di rischio. Questo comporta l'innesco dell'intero processo di validazione anche in caso di alert che in realtà non richiederebbero elevati livelli di attenzione, rendendo il SOC "manuale" ulteriormente inefficiente. Ovviamente a scapito del mean time before detect (MTBD) e del mean time before remediate (MTBR).

Il cuore della limitazione è l'impossibilità di processare tutti i dati a disposizione per la difesa: negli anni i vendor di cybersecurity con una visione estesa fino alla trasformazione dei SOC, hanno incrementato la generazione di dati telemetrici da end point, cloud, reti, consentendo l'estrazione di informazioni prima non disponibili, aumentando al contempo considerevolmente i volumi (anche di diversi fattori).

Se i SIEM sono stati pensati per facilitare la gestione di alert e log "human-centric"i sistemi di security orchestration automation e response (SOAR) si sono rivelati degli ottimi strumenti per introdurre un importante livello di automazione nelle principali fasi della gestione di un incident.

Inoltre, tramite integrazioni tecnologiche, un buon SOAR può orchestrare e automatizzare i flussi di lavoro velocizzando le fasi di triage, qualificazione delle minacce, risposta agli incidenti, arricchimento dei dati mediante threat intelligence, verifica delle compliance.

Non meno importante per il SOAR è la funzione di facilitare la collaborazione tra differenti stakeholders durante un incidente, l'omogeneità della gestione per tipo di incidente mediante playbooks, la reportistica e documentazione sugli incidenti trattati.

SOAR ha rappresentato un primo passo per l'introduzione di tecnologie predittive (artificial intelligence/machine learning) per automatizzare quanto più possibile i processi di un SOC: quello che non ha fatto è cambiare il punto di vista. Si è mantenuto il concetto di gestione alert/incidents human-centric lavorando all'efficientamento dei processi così creati.

Un SOC moderno deve secondo noi essere costruito con una nuova architettura compatibile coi requisiti degli ambienti IT/OT attuali e futuri.

Questa architettura deve essere flessibile, scalabile, affidabile e integrabile con un ampio spettro di tecnologie e tool di security.

In generale il design deve considerare:

- integrazione dati, analisi e triage automatici;
- workflows uniformati per massimizzare la produttività;
- intelligenza integrata per bloccare attacchi con intervento minimo da parte degli analisti.

A differenza di quanto avveniva in precedenza, il SOC moderno si basa su data science su basi dati massive, più che sul giudizio degli esseri umani e su regole definite per identificare le minacce note. Questo approccio consente di invertire il punto vista, ottimizzando i processi per sfruttare la potenzialità delle macchine: usando una analogia possiamo paragonare un SOAR ai sistemi di assistenza alla guida introdotti per aiutare l'uomo (gestione del salto corsia, rilevamento ostacoli, ABS etc.). In questo caso la nuova piattaforma per il SOC moderno rappresenta un sistema di guida autonoma, dove il compito è gestito dalle macchine con la supervisione dell'uomo.

Questo rappresenta a nostro avviso il punto di partenza per una piattaforma di cyber-security del futuro, capace di fornire un livello di protezione drammaticamente superiore con near realtime detection e response fino ad arrivare ad un approccio realmente detect and prevent.

Una piattaforma SOC simile deve includere funzioni "classiche" *best in class* quali EDR, XDR, SOAR, ASM, UEBA, TIP e SIEM in grado di identificare e bloccare attacchi mai visti prima dall'end-point fino al cloud. Il modo in cui queste funzioni sono integrate è fondamentale: agli analisti serve un'unica interfaccia, sia orientata ai task e ai processi guidata dall'automazione.

È essenziale rompere il modello incrementale di headcount e complessità all'eventuale aggiunta di nuove tecnologie di protezione, e questo è possibile solo cambiando il modo in cui la tecnologia supporta le SecOps.

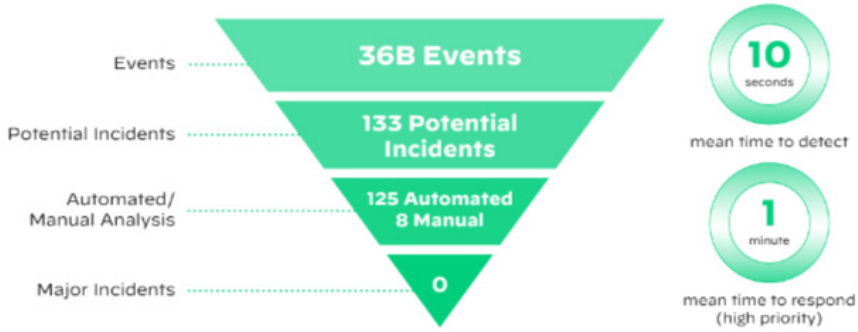
Gli advanced analytics e l'AI sono in grado di ridurre il tempo che i team impiegano nella gestione di dati e alert. I data model allenati da basi dati massive costituite di log e alert su dati appositamente estratti per essere manipolati da AI e ML e provenienti da cloud, rete, endpoint, consentono di processare automaticamente ogni singolo alert e solo dopo arrivare all'aggregazione in incidenti arricchiti di contesto e preparati per l'analisi e il triage automatizzati, limitando al massimo l'intervento degli analisti.

L'automazione e i playbook inline applicano i risultati degli analytics per l'esecuzione intelligente degli incidenti.

Quello che ML (sottoinsieme di AI) deve fare in una piattaforma tecnologica unica per il SOC è:

- **analisi di comportamento:** gli algoritmi AI e ML analizzano i comportamenti di end-point, rete e cloud, identificando anomalie anche a bassa priorità che possono indicare la presenza di una minaccia;
- **Threat Intelligence:** la piattaforma impiega algoritmi ML per analizzare volumi massivi di dati di threat intelligence per identificare patterns e trend che possono indicare la presenza di una minaccia sin dalle prime fasi;
- **risposta automatica:** le automazioni devono essere guidate da AI per poter continuare a rispondere alle minacce in real-time con l'evoluzione delle minacce stesse;
- **analisi predittiva:** algoritmi ML devono essere impiegati per analizzare dati storici in modo da poter predire rischi potenziali e aiutare nella protezione contro attacchi futuri;
- **apprendimento continuo:** dai nuovi dati per correggere e migliorare continuamente i modelli, migliorando accuratezza ed efficacia della piattaforma.

L'esempio di quello che si può ottenere da un simile approccio è rappresentato dai dati reali di un singolo giorno nel nostro SOC, che da 3 anni è stato trasformato secondo questa filosofia: il tempo medio di detect è ridotto a 10 secondi, mentre quello di risposta è nell'ordine del minuto.



La Sicurezza dei sistemi di acquisizione e stampa

[A cura di Sara Bonini, Luca Lazzari e Massimo Prato, ASSOIT]

I sistemi di stampa e digitalizzazione sono ormai oggi dei dispositivi IoT, connessi alle reti aziendali e ai servizi IT, con la possibilità di memorizzare elevate quantità di dati. Sono accessibili da dispositivi mobili e dal cloud e possono rappresentare, come altri strumenti, se non correttamente protetti, un punto di ingresso per attacchi, o essi stessi un obiettivo, da parte di cyber criminali.

Nonostante il fatto che le stampanti e i dispositivi di nuova generazione siano composti da diversi elementi quali firmware, processori, sistemi di memorizzazione, con capacità di connessione ed elaborazione elevate esattamente come un moderno computer, ancora oggi tali apparati sono percepiti come comuni "periferiche", come un mouse o una tastiera.

"Dispositivi di acquisizione e stampa" sono oggi il termine che rappresenta in modo più corretto la realtà attuale in un'ottica di sistemi di elaborazione complessi, per non considerarli più alla stregua di comuni "elettrodomestici".

La tecnologia che risiede all'interno di questi dispositivi è elevatissima, con funzionalità veramente evolute rispetto all'equivalente oggetto di pochi anni fa. Per fare un esempio, la connessione tra i notebook o i PC e i dispositivi di acquisizione e stampa è bidirezionale; pertanto, può essere sfruttata per diffondere malware o compiere azioni malevole. Per questo motivo, tali apparati sono diventati oggetto di attenzione dei cyber criminali, consapevoli che agli occhi della maggior parte dei responsabili IT e della sicurezza delle aziende, le stampanti non sembrano rappresentare un punto di attenzione.

Gli attacchi possono essere i più disparati e con obiettivi diversi: "hacktivism" o "cybercrime" con scopi di spionaggio, sabotaggio e furto di dati.

Oltre alle finalità, anche le conseguenze di un attacco ai dispositivi di acquisizione e stampa sono le più diverse: rendere indisponibili tali apparati, rubare informazioni contenute al loro interno, violare altri sistemi aziendali, eseguire campagne di attivismo (ad esempio obbligando gli apparati a stampare volantini propagandistici).

Le tecniche per accedere a questi dispositivi sono poi quelle tradizionali: attacchi diretti a tali apparati, come nei casi rappresentati precedentemente, oppure

indirettamente usando altri canali di ingresso dell'organizzazione, come un messaggio contenente un allegato o un link arrivato via e-mail o trovato nel feed del proprio profilo social.

Le vulnerabilità più comuni, utilizzate per condurre con successo tali attacchi sono sicuramente legate all'obsolescenza o all'assenza di pratiche di aggiornamento continuo, unitamente al fatto che, anche laddove non raggiungibili dalla rete internet, questi dispositivi possono essere violati anche mediante l'inserimento di dispositivi di memoria USB o tramite la connessione attraverso la rete interna da parte di sistemi posti sotto il controllo di un attaccante.

I dispositivi di acquisizione e stampa possono davvero essere utilizzati per causare gravi impatti alle aziende e pubbliche amministrazioni?

Andando indietro nel tempo, il c.d. "Bangladesh Bank cyber heist" del 2016, forse il più grande attacco informatico mai registrato verso il mondo bancario (ovvero verso i circuiti bancari e gli istituti coinvolti, diversamente da come solitamente accade, verso i correntisti) ha visto protagonista, in una delle fasi cruciali dell'incidente, una stampante.

Quell'evento dimostrò, in questo particolare ambito, come la percezione sui dispositivi di stampa fosse ancora quella della "periferica", dando per scontato che ciò che esce in formato cartaceo da questi dispositivi, siano le informazioni provenienti dai computer connessi. Durante l'attacco, in realtà, agendo proprio sui dispositivi di stampa, gli hacker hanno fatto in modo che tutta una serie di operazioni bancarie non finissero sui registri cartacei, su cui si basava in buona parte il processo di controllo attuato dagli Istituti.

Più di recente, a maggio 2023, è uscita la notizia di una campagna hacker cosiddetta "state sponsored", ossia un team di hacker sostenuto da una intelligence di un governo.

Nello specifico stiamo parlando di un governo mediorientale che avrebbe finanziato un team di hacker per individuare delle vulnerabilità all'interno dei dispositivi di stampa e svolgere poi, sfruttando queste vulnerabilità, degli attacchi contro infrastrutture critiche di alcuni Paesi nemici.

Questi eventi sono la dimostrazione che ciò che era solo teorizzato pochissimi anni fa ed era oggetto di situazioni veramente molto rare, ormai è diventata quasi una consuetudine e quindi un grosso punto d'attenzione.

Quanto è elevato il rischio potenziale?

Per rispondere alla domanda su quanto possa essere elevato il rischio di subire un attacco come quelli sopra rappresentati, è possibile richiamare un fatto non recentissimo, tuttavia purtroppo ancora attuale. Parliamo dell'attacco di tipo "printjack": un'azione che solitamente consiste nell'invio su larga scala di job di stampa ripetuti a più stampanti non protette o mal configurate fino a quando queste non esauriscono la carta e il toner.

Condotto dalla rivista statunitense Cybernews nel 2020, gli esperti di sicurezza informatica di Cybernews hanno preso il controllo di quasi 28.000 stampanti non protette in tutto il mondo e le hanno costrette a stampare una guida per aumentare la consapevolezza sui problemi di sicurezza dei sistemi di stampa.

Gli esperti di Cybernews sono riusciti a violare esattamente 27.944 stampanti sui 50.000 dispositivi presi di mira usando dati OSINT da motori come Shodan e Censys, con una percentuale di successo del 56%. Tenendo conto di questa percentuale, si può presumere che su 800.000 stampanti connesse a Internet nel 2020 in tutto il mondo, almeno 447.000 non erano protette.

Andando alla ricerca di dati più recenti, è possibile citare il rapporto "Print Security Landscape 2023" di Quocirca, un'azienda globale di analisi e ricerche di mercato specializzata nell'analisi della convergenza delle tecnologie di stampa e digitali.

La prima informazione significativa che riporta tale report è che il 61% degli intervistati ha subito nel 2023 una perdita di dati legata a sistemi di stampa non sicuri. In particolare, il 39% degli intervistati ritiene che sia sempre più difficile far fronte alle richieste di sicurezza della stampa. Il costo medio della perdita dei dati è salito a oltre 800 mila euro rispetto ai 737 mila euro nel 2022.

Un dato confortante è rappresentato dal 79% che prevede di aumentare la spesa per la sicurezza dei sistemi di stampa nel 2024.

Lo stesso report rivela che i Chief Information Officer e i Chief Information Security Officer hanno opinioni divergenti sul livello di sfida e rischio associato al mantenimento della sicurezza dei dispositivi di acquisizione e stampa: i CISO sono più ottimisti, per cui solo il 28% sostiene che è diventato più difficile affrontare le sfide della sicurezza di questi apparati, rispetto al 50% dei CIO.

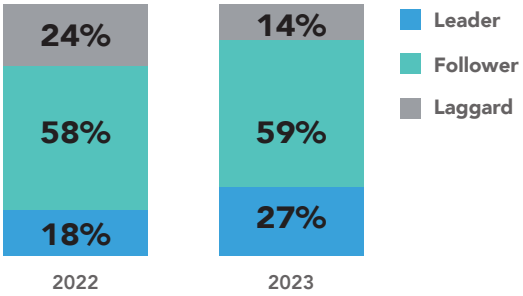
Allo stesso modo, solo il 45% dei CISO è preoccupato per il rischio relativo a stampanti non sicure, rispetto al 72% dei CIO.

Questi dati indicano che i due principali influencer sulla sicurezza e protezione dei dati in azienda non sono allineati nella loro percezione del rischio associato all'infrastruttura di stampa.

Quasi la metà (47%) del cluster dei responsabili più attenti (Leaders) alla sicurezza di stampa ha riportato una o più perdite di dati dovute a sistemi non sicuri, ma questa percentuale sale al 65% tra il panel che rappresenta le figure professionali attente al tema (Followers) e al 68% del segmento che rappresenta le figure meno attente e restie a prendere decisioni (Laggards).

La maturità della print security sta migliorando

Print Maturity Index di Quocirca basato sul numero di misure di sicurezza implementate



Fonte: Quocirca

Sensibilizzare e formare

Uno degli elementi di maggiore importanza, che può rappresentare una risposta concreta e rapida da introdurre fin da subito per la sicurezza IT, è quello di cambiare la percezione rispetto a questi dispositivi da parte di tutti gli utilizzatori e sviluppare pratiche di configurazione sicura, sfruttando gli strumenti di difesa di ultima generazione introdotti dai principali produttori di dispositivi di acquisizione e stampa.

Abbiamo provato, qui di seguito, a fornire una breve linea guida che tutte le organizzazioni, anche le più piccole, possono seguire per far fronte alle sfide per la sicurezza nella protezione del proprio sistema informativo "integrato" con dispositivi di acquisizione e stampa.

BUONE PRATICHE D'USO

ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

Aggiornamento dei dispositivi

È utile prendere in considerazione l'aggiornamento del proprio parco stampanti. Molte nuove stampanti dispongono di funzionalità di sicurezza integrate che semplificano la protezione della rete e la protezione da un attacco informatico.

Mantenere aggiornato il software dei dispositivi

Le stampanti hanno spesso un firmware che le aiuta a funzionare, potrebbero anche avere un software antivirus o anti-malware integrato. È bene consultare il manuale del proprio dispositivo per conoscere le diverse caratteristiche e la sua manutenzione. È inoltre importante installare eventuali patch di sicurezza o aggiornamenti, poiché il software obsoleto è spesso una delle cause principali che porta alla violazione dei dati.

Creare policy aziendali per proteggere i dati contenuti negli hard disk e sui documenti lasciati nei vassoi delle stampanti

Creare una serie di regole pratiche e norme di condotta sono la base per ottenere una linea di difesa verso gli attacchi. Una serie di policy adeguate può aiutare a proteggere sistemi e utenti, anche coloro che lavorano in remoto.

Mettere in atto un processo di autenticazione

Una buona pratica è quella di verificare che le stampanti dispongano di misure di sicurezza come pass code univoci per trattenere le stampe fino a quando un utente non è fisicamente presente per ritirarli. Questo processo permette di verificare i dati inviati, per questo le stampanti potrebbero subire altre vulnerabilità che potrebbero rivelarsi sfruttabili, anche da remoto I sistemi di stampa e digitalizzazione sono dotati di funzionalità che garantiscono la protezione delle informazioni, come l'autenticazione e l'autorizzazione per verificare l'identità degli utenti prima che venga rilasciata qualsiasi stampa. I metodi di convalida possono essere diversi: lettori badge, codici PIN o sistemi di autenticazione biometrica.

Utilizzare i software di monitoraggio

Il software di monitoraggio dei dispositivi di stampa permette di avere sotto controllo tutte le attività di stampa della propria organizzazione. Questi cruscotti sono inoltre in grado di individuare attività sospette e consentire una reazione tempestiva agli attacchi.
Gli utenti dei servizi di stampa gestiti (MPS) possono anche ottenere regolari report di conformità, che dovrebbero includere il monitoraggio e la segnalazione delle violazioni dei dati.

BUONE PRATICHE D'USO

ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

Posizionare i dispositivi di stampa e digitalizzazione su una rete separata e dedicata all'interno dello spazio di lavoro

Posizionare le stampanti su una rete separata non eliminerà la minaccia di malintenzionati che accedono alla rete aziendale da questi dispositivi, ma impedirà loro di utilizzarli come potenziali punto di ingresso nella rete aziendale.

Formare e rendere consapevoli gli utenti su minacce e attacchi

Questa pratica consente di rendere informati gli utenti sui rischi legati ai dispositivi di stampa. Sensibilizzare gli utenti dotandoli di regole di comportamento è il primo passo verso una maggiore sicurezza. Una survey contenuta nel Rapporto Clusit 2023 sulla Sicurezza ICT in Italia, ha evidenziato che le policy e le procedure di sicurezza pubblicate sono conosciute da dipendenti e collaboratori solo in un terzo (33%) delle aziende.

Sanificazione dei dati al momento della sostituzione dei dispositivi

È importante accertarsi che il dispositivo sia sottoposto ad un procedimento di sanificazione certificata dei dati che include la distruzione degli hard disk, o la loro formattazione in modalità sicura a basso livello, e la cancellazione di tutti i dati presenti nelle rubriche interne al dispositivo, come per esempio rubrica e-mail, rubrica telefonica-fax, al momento della sua sostituzione. Questa pratica consente di distruggere in modo definitivo tutti i dati contenuti in questi dispositivi e la certificazione, dichiarazione emessa dal fornitore che effettua il servizio, tutela l'azienda o il privato che ha utilizzato il dispositivo fino a quel momento.

Servizi professionali di Print Security Risk Assessment

Come già detto, spesso il perimetro dei dispositivi di stampa non viene tenuto nella giusta considerazione da parte del personale IT, che tende a valutare come sicuro un ambiente nel quale invece i potenziali bug di sicurezza sono presenti. È raccomandato valutare col proprio fornitore di dispositivi di stampa la possibilità di usufruire di un servizio professionale di Security Risk Assessment per i dispositivi di stampa grazie al quale verranno analizzate in profondità tutte le potenziali aree di rischio: hardware, firmware, network, processi e procedure, asset management, configurazioni iniziali e manutenzione delle stesse, patching, governance.

Buone pratiche a casa

Avere una stampante non protetta collegata alla rete domestica o aziendale è come lasciare una porta aperta nella propria stanza o in ufficio. Quindi, è bene assicurarsi di rivedere e disabilitare tutto ciò che comporta la stampa su Internet. Ciò include la configurazione delle impostazioni di rete in modo che la stampante risponda solo ai comandi provenienti dal router di rete. Inoltre, non dimenticare di scollegare la stampante quando non è in uso: se non c'è connessione, i malintenzionati non possono compromettere la rete.

Quello che le aziende e le pubbliche amministrazioni, in conclusione, devono tenere ben presente nella scelta dei dispositivi di acquisizione e stampa, è verificare che questi rendano disponibili nativamente le funzionalità necessarie per implementare le buone pratiche sopra elencate:

- meccanismi per la protezione dell'accesso alle informazioni, come l'autenticazione e l'autorizzazione per verificare l'identità degli utenti prima che venga rilasciata qualsiasi stampa (i metodi di convalida possono essere diversi: lettori badge, codici PIN o sistemi di autenticazione biometrica);
- protezioni e certificazioni a livello hardware e software, applicazioni, sistema operativo, firmware, bios e disco fisso; questo per assicurare che i processi di gestione dei documenti e delle stampe siano conformi alle più stringenti normative;
- cifratura dei dati secondo algoritmi standard e certificati, per assicurare che le informazioni, se rubate, siano rese illeggibili e inutilizzabili;
- presenza di un supporto attivo e regolare che renda disponibili aggiornamenti per la sicurezza e meccanismi atti a proteggere i dispositivi da tentativi di installazione di applicazioni o software malevoli;
- in particolare, in ambito enterprise, strumenti di supporto e salvaguardia su tutto il processo legato al ciclo di vita dei documenti, anche in fase di digitalizzazione e di gestione documentale, mediante cruscotti in grado di rilevare e allertare i responsabili della sicurezza relativamente ad accessi non autorizzati, per consentire un intervento proattivo e tempestivo.

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.

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/
LinkedIn: ASSOIT
Twitter: ASSOIT2
YouTube: ASSOIT

Attraverso il tunnel del cambiamento: l'evoluzione della connessione sicura da VPN a ZTNA

[A cura di Alessandro Ercoli, Andrea Negroni e Davide Costanigro, HPE Aruba Networking]

Il viaggio dall'edge al cloud continua!

Abbiamo passato diverse tappe da quando è iniziata la trasformazione digitale delle aziende pubbliche e private e di riflesso, come è cambiato il ruolo delle infrastrutture di rete.

Progressivamente si stanno unendo i punti cardine, delineando un nuovo disegno, un disegno di un'architettura, che seppur complessa, si rivela semplice, sicura, flessibile, scalabile grazie anche al supporto dell'Intelligenza Artificiale.

Anni fa si consideravano le infrastrutture di rete una semplice commodity, monolitiche e complesse da gestire e spesso, separate dalle tematiche di sicurezza e dalle potenziali esposizioni al rischio.

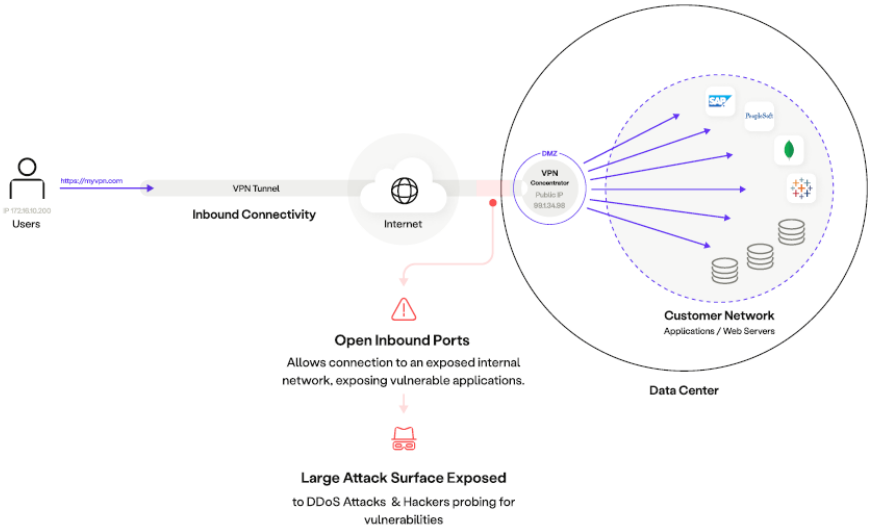
Oggi sfruttiamo al meglio i dati e gli analytics che raccogliamo all'edge, per garantire la miglior esperienza utente possibile, sfruttando la potenza dell'AI e mantenendo un alto standard di sicurezza attraverso l'adozione di modelli Zero Trust.

Il rapido sviluppo del panorama digitale, guidato principalmente dall'adozione del cloud, dallo smart-working e la diffusione di dispositivi mobili, ha messo in evidenza i limiti dei modelli IT centralizzati, tra i quali, quello legato all'accesso remoto tramite reti private virtuali (VPN).

Queste limitazioni sono molteplici, come ad esempio: complessità gestionale e relativa ricaduta sui costi operativi, estensione della superficie d'attacco, problemi di latenza nelle connessioni e mediocre esperienza d'uso e costi di mantenimento dell'infrastruttura. A fronte di questi limiti, il mercato è sempre più attento a valutare nuovi modelli come il Zero Trust Network Access (ZTNA).

I limiti degli accessi remoti tramite VPN

Come già anticipato, i modelli tradizionali di accesso remoto tramite VPN hanno svolto un compito importante negli ultimi 20 anni, in particolare durante la pandemia dove la necessità di garantire un accesso sicuro ai servizi, ed agli asset aziendali, è stato fondamentale.



Come riassunto in precedenza, rimangono tuttavia una serie di limiti di questi servizi di accesso remoto VPN che comprendono diversi aspetti chiave quali:

- *Complessità:*
  - operativa: la gestione e la risoluzione dei problemi delle VPN, comporta spesso una complessità intrinseca che richiede competenze specializzate e soprattutto tempo. Le complessità coinvolte nella configurazione, nel monitoraggio e nella risoluzione dei problemi possono portare a sfide operative per l'IT, rendendo più difficoltosa la gestione del servizio o peggio ancora, esporre involontariamente a delle vulnerabilità. Un esempio su tutti, la gestione delle vulnerabilità di sicurezza (CVE) e relativi tempi di inattività dovuti all'applicazione di patch ed aggiornamenti. L'applicazione tardiva o incompleta delle patch di sicurezza può esporre l'infrastruttura VPN a potenziali exploit, aumentando il rischio di accesso non autorizzato, violazioni dei dati e altri incidenti di sicurezza.
  - infrastrutturale: la manutenzione e la scalabilità dell'infrastruttura VPN possono essere un'impresa costosa, soprattutto quando si ha a che fare con forza lavoro geograficamente distribuita. Le spese associate all'hardware, alle architetture in alta affidabilità, al software e alla manutenzione continua, incidono all'onere finanziario e rendono il servizio complesso da adattare a nuove esigenze e necessità aziendali (scenari di M&A, strategie multi-cloud, etc.).

- ***Sicurezza:*** come evidenziato precedentemente, una soluzione complessa da implementare, gestire e monitorare può potenzialmente introdurre delle vulnerabilità aumentando il rischio per la sicurezza informatica. Il modello di accesso remoto tramite VPN, per come è strutturato e spesso configurato, introduce ulteriori elementi di esposizione. Come sappiamo, l'utente remoto stabilisce una connessione VPN verso un concentratore (o server VPN) che risiede all'interno della rete aziendale (idealmente in una zona demilitarizzata DMZ) che deve però esporre il servizio di accesso remoto su Internet e quindi, esporsi potenzialmente ad attacchi quali DDoS, accesso non autorizzato, etc. Altro elemento estremamente importante, è legato al tipo di accesso che viene assegnato all'utente remoto una volta connesso. Stabilito il tunnel VPN, spesso all'utente può essere concessa la visibilità di una subnet aziendale come se fosse fisicamente presente all'interno della rete locale per avere accesso alle risorse aziendali. È evidente che senza una adeguata (e spesso complessa) segregazione e segmentazione di rete, il rischio di esporre una notevole superficie di attacco ad un attaccante è molto significativo.
- ***Esperienza d'uso:*** spesso l'esperienza utente non è ottimale per via della intrinseca natura centralizzata del servizio, dove il concentratore VPN può rivelarsi un collo di bottiglia costringendo anche alle comunicazioni utente-internet di passare per il data center aziendale, introducendo latenza che puo' incidere negativamente su applicazioni real-time come, ad esempio, i servizi SaaS di videocomunicazione. Si cerca di indirizzare questo problema con lo "slpit-tunneling VPN" in modo che l'utente possa instradare il traffico verso internet in modo diretto, senza passare per il tunnel VPN e bypassando quindi i controlli centralizzati per la navigazione. Questo è un compromesso, chiaramente non ottimale, che può andare a scapito sia della sicurezza dell'utente e di conseguenza della sua azienda.
- ***Flessibilità e scalabilità:*** i limiti di flessibilità e scalabilità di una tradizionale soluzione di accesso remoto, possono incidere significativamente sulla capacità di un'azienda di adattarsi a nuove esigenze o nuovi modelli IT in modo rapido. Essendo questo servizio totalmente dipendente dall'infrastruttura tecnologica sottostante, è evidente che ogni necessità di cambiamento del servizio VPN richiede talvolta un aggiornamento dell'hardware, del suo dimensionamento, dell'architettura di riferimento, con conseguente impatto su costi e tempi.

Il Zero Trust Network Access (ZTNA)

Il modello Zero Trust Network Access (ZTNA) si sta affermando sempre di più come una soluzione innovativa per superare i limiti delle vecchie reti private virtuali (VPN).

Caratteristica principale e distintiva di questo nuovo approccio risiede proprio nel concetto di Zero Trust ovvero, stabilire che nessuna entità, sia essa un utente,

dispositivo o workload, può essere automaticamente considerato affidabile, anche se residente all'interno del perimetro aziendale.

Le caratteristiche principali di una soluzione ZTNA includono quindi controlli granulari degli accessi, che consentono livelli di autorizzazione precisi, un'autorizzazione dinamica che si adatta alle mutevoli condizioni del contesto, ed un monitoraggio continuo della sicurezza per identificare e rispondere in modo proattivo a potenziali minacce. Non ultimo, il modello ZTNA tipicamente viene erogato sotto forma di servizio SaaS andando a migliorare tutta una serie di aspetti relativi all'esperienza utente, alla sicurezza, alla flessibilità/scalabilità ed alla gestione operativa e di riflesso a contenere i costi.

Concludendo, il modello ZTNA si sta sempre di più affermando sul mercato come l'alternativa alle VPN tradizionali.

VPN vs VPNaaS vs ZTNA

La tabella di seguito, riporta le principali e generiche differenze tra quelle che sono le caratteristiche delle soluzioni VPN, VPNaaS e ZTNA, mettendole a confronto.

	VPN	VPNaaS	ZTNA
Architecture	Centralized Gateway	Cloud-based Gateway	Zero Trust Architecture
Access Control	Network-based	IP-based	Identity and Context
Traffic Flow	Backhauling	Direct to Applications	Least Privilege Access
Security Posture	Static Perimeter Defense	Cloud-based Security Fabric	Continuous Microsegmentation
Scalability	Limited	Scalable	Highly Scalable

I benefici dello Zero Trust Network Access (ZTNA)

In estrema sintesi, i benefici derivanti da un modello Zero Trust Network Access (ZTNA) sono:

- *Sicurezza:* attraverso la combinazione di caratteristiche chiave, come la segmentazione avanzata, il controllo degli accessi, la visibilità dettagliata e la riduzione della superficie d'attacco, il modello ZTNA, definisce un ecosistema di sicurezza robusto e resistente alle sofisticate minacce digitali. La segmentazione avanzata, pilastro fondamentale di ZTNA, suddivide l'accesso alle risorse ed applicazioni aziendali in modalità altamente selettiva e controllata. Questo approccio non solo protegge le risorse critiche ma contribuisce anche a contenere e isolare eventuali violazioni

della sicurezza. Il controllo degli accessi, basato su politiche granulari, si adatta dinamicamente al contesto dell'utente e del dispositivo. Ciò significa che l'accesso alle risorse è strettamente regolamentato, garantendo che solo gli utenti autorizzati possano interagire con determinate applicazioni o servizi. Tale precisione riduce in modo significativo il rischio di accessi non autorizzati.
La visibilità unificata offre una panoramica completa delle attività di rete, consentendo un monitoraggio costante per individuare rapidamente comportamenti anomali o attività sospette. Questa chiarezza operativa è cruciale per una risposta tempestiva alle minacce, limitando gli impatti negativi di eventuali violazioni.
La riduzione della superficie d'attacco è conseguenza diretta di una combinazione sinergica di segmentazione, controllo degli accessi e visibilità dettagliata. Limitare l'accesso solo a ciò che è essenziale minimizza le opportunità per gli aggressori di sfruttare vulnerabilità, rendendo l'ambiente di rete notevolmente più sicuro. A questo si aggiunge il modello di erogazione SaaS del servizio ZTNA che non richiede hardware dedicato da installare e conseguente esposizione di concentratori VPN su internet, eliminano di fatto un potenziale punto di osservazione ed attacco dall'esterno.

- *Semplicità:* i più recenti servizi ZTNA basati su architetture cloud-native. ed erogati in modalità SaaS, non richiedono ovviamente appliance o hardware dedicato e sono completamente gestiti dal fornitore stesso sollevando le aziende e le loro risorse IT dalla gestione e monitoraggio di complesse architetture infrastrutturali. Questi servizi cloud sono dunque progettati per garantire affidabilità, disponibilità e scalabilità automatica all'aumentare delle richieste di traffico. Garantiscono l'esperienza utente migliore possibile, senza interruzioni dell'attività e le integrazioni via API con i principali servizi IDP, EDR e SIEM, aiutano ad accelerare il processo di implementazione, offrendo una maggiore protezione. Spesso le piattaforme cloud ZTNA sono caratterizzate dalla loro semplicità di configurazione, gestione e monitoraggio attraverso un'interfaccia utente centralizzata che permette di definire le policy di sicurezza in modo consistente ed intuitivo, a favore della produttività.
- *Esperienza d'uso:* l'approccio di Zero Trust Network Access (ZTNA) si manifesta come un'esperienza utente che trascende la semplice sicurezza, abbracciando l'efficienza operativa e la libertà di connessione. Gli utenti sono immersi in un ambiente dove la sicurezza è integrata con trasparenza, garantendo al contempo la rapidità e la facilità d'uso. La navigazione diretta e governata attraverso i servizi di Secure Web Gateways (SWG) aggiunge un ulteriore livello di controllo, filtrando il traffico web in modo intelligente e creando un ambiente digitale sicuro e conforme alle politiche aziendali. Altra caratteristica che accomuna le principali soluzioni ZTNA è quella di prevedere anche casi d'uso di tipo "agentless", ovvero, la possibilità di

erogare un servizio di accesso remoto ZTNA senza l'ausilio di agenti sui dispositivi degli utenti a vantaggio di una maggiore flessibilità e migliore gestione specialmente nei casi in cui questo servizio sia riservato, ad esempio, ad utenze esterne come fornitori, partner e consulenti. In sintesi, l'esperienza utente con ZTNA è all'avanguardia, unendo agilità e sicurezza in un connubio che si adatta in modo impeccabile alle esigenze evolute delle dinamiche di lavoro moderne.

La migrazione verso lo Zero Trust Network Access (ZTNA)

La migrazione verso il modello ZTNA è un processo strategico che richiede una pianificazione meticolosa, tenendo conto dell'infrastruttura esistente e delle politiche di sicurezza presenti e future. Ecco una visione sommaria dei passaggi chiave coinvolti:

- *Valutazione dei requisiti e dei rischi:* le aziende che desiderano intraprendere il percorso verso lo ZTNA devono fare una valutazione approfondita dei propri requisiti e del contesto evolutivo. Identificare quali applicazioni e risorse necessitano della protezione ZTNA è cruciale poiché garantiscono un'implementazione mirata ed efficace del modello in linea con gli obiettivi di sicurezza.
- *Scelta della soluzione adeguata:* fondamentale per il processo di migrazione è la valutazione attenta dei fornitori ZTNA presenti sul mercato. Questa valutazione dovrebbe concentrarsi sulle funzionalità, le opzioni di implementazione e le capacità di integrazione, assicurandosi che la soluzione selezionata possa incontrare senza problemi le esigenze specifiche dell'organizzazione. Questo passaggio costituisce la base per una riuscita implementazione di ZTNA.
- *Sperimentazione e test:* prima di una completa implementazione, le aziende spesso optano per una fase sperimentale. Ciò comporta un rollout graduale e un testing approfondito per ridurre al minimo le interruzioni ed identificare potenziali problemi e casi d'uso che non sono stati contemplati inizialmente e che possono anche mettere in crisi il successo del progetto stesso. Un testing rigoroso consente regolazioni e ottimizzazioni, assicurando una transizione più fluida verso il ZTNA senza arrecare interruzioni del servizio e producendo i necessari quick win per supportare l'iniziativa nel medio-lungo termine.
- *Formazione e adozione:* una migrazione di successo verso ZTNA coinvolge una formazione completa sia per gli utenti finali che per l'IT. L'educazione sui nuovi protocolli di accesso e le pratiche di sicurezza è fondamentale, promuovendo una cultura di consapevolezza della sicurezza. Questo approccio proattivo garantisce che gli utenti siano ben informati sui cambiamenti, riducendo la probabilità di incidenti di sicurezza e promuovendo l'integrazione di successo di ZTNA nelle operazioni quotidiane.

Seguendo questi passaggi di buon senso, le organizzazioni possono attuare efficacemente il processo di migrazione, massimizzando i benefici di ZTNA e riducendo al minimo potenziali interruzioni e rischi di sicurezza.

Best practices Zero Trust Network Access (ZTNA)

Il servizio ZTNA dimostra la sua massima efficacia quando si integra in modo armonioso con l'ecosistema più ampio delle soluzioni di sicurezza di un'azienda.

L'interoperabilità con strumenti e piattaforme esistenti, non solo amplifica la capacità di ZTNA di adattarsi alle specifiche esigenze aziendali, ma crea anche un sinergismo a favore di una migliore postura di sicurezza.

Tra le possibili integrazioni vale la pena citare:

- ***Sistemi di Identity Provider (IdP):*** ottimizza la gestione degli utenti e delle autorizzazioni. L'integrazione con sistemi IdP consente una gestione centralizzata delle identità, semplificando il processo di assegnazione dei privilegi e garantendo una corretta gestione delle credenziali.
- ***Sistemi di Controllo dell'Accesso alla Rete (NAC):*** combinare ZTNA con NAC per un'autenticazione robusta del dispositivo e la sua conformità, garantendo che solo dispositivi autorizzati e conformi ottengano l'accesso.
- ***Sistemi Endpoint Detection and Response (EDR):*** l'integrazione tra ZTNA e soluzioni di sicurezza endpoint EDR estende la protezione anche ai dispositivi utente, garantendo una copertura completa contro varie forme di minacce.
- ***Sistemi SIEM:*** l'integrazione con SIEM consente una visione unificata delle attività di rete e su internet, semplificando la risposta agli incidenti e migliorando la capacità di individuare pattern di minacce.

ZTNA nell'ambito della strategia SASE

Il modello Zero Trust Network Access (ZTNA) è parte del più ampio modello Security Service Edge (SSE) completando il framework SASE (Secure Access Service Edge).

SASE consolida varie funzioni di sicurezza di rete, tra cui SD-WAN, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) e Digital Experience Monitoring (DEM), in un servizio unificato basato su cloud.

Questa integrazione completa fornisce alle organizzazioni una soluzione onnicomprensiva per l'accesso sicuro e la protezione dei dati attraverso diversi punti di accesso.

Come dicevamo in apertura, il viaggio dall'edge al cloud continua....e non si ferma!

Viaggiare porta spesso cambiamento, si esce dalla comfort zone, si fa qualcosa di nuovo.

La realtà è che abbiamo raggiunto una nuova tappa: quello a cui siamo sempre stati abituati e "legati" da decenni, sta lasciando il posto a nuove forme e soluzioni per fare sicurezza, come abbiamo cercato di raccontarvi in quest'articolo.

Ci piace pensare e programmare la nostra prossima tappa insieme, dandovi il nostro punto di vista su come vediamo la trasformazione delle infrastrutture digitali, pienamente sicure.

Lo faremo passo dopo passo, e il prossimo sarà quello dello Unified SASE!

Strategie di data security nell'era dell'AI Generativa

[A cura di Patrizio Rinaldi, Microsoft]

Nel mondo digitale in continua evoluzione, le minacce informatiche si trasformano e si intensificano ad ogni avanzamento tecnologico o variazione degli equilibri geopolitici.

Col sorgere dei due conflitti militari che stanno tristemente caratterizzando la nostra quotidianità, con un coinvolgimento diretto delle potenze mondiali tecnologicamente più avanzate, abbiamo assistito ad un esponenziale intensificarsi degli attacchi informatici di molteplice natura.

Parallelamente, l'affermarsi dell'Intelligenza Artificiale Generativa è stato l'elemento distintivo dell'anno appena trascorso. Il cuore pulsante di questa innovazione è l'utilizzo di nuovi approcci, nuovi modelli (LLM e non solo), che permettono di semplificare l'interazione con gli strumenti di AI (linguaggio naturale, immagini, video, etc..) e ottenere la produzione di un contenuto contestualizzato, comprensibile e assimilabile a ciò che potrebbe derivare dalla produzione umana.

Il tema della Cybersecurity va quindi oggi declinato con un focus importante sul dato, sull'uso che se ne fa, sulla sua produzione, condivisione e conservazione e, non da ultimo, della sua protezione.

Il dato, infatti, è l'oro nel nuovo ordine mondiale affermatosi con l'avvento della Società dell'Informazione, in cui la capacità di elaborare e trasmettere informazioni digitalizzate è diventata il fattore chiave per lo sviluppo economico, sociale e culturale (Società dell'informazione - Wikipedia) [1].

Ci troviamo quindi a ribadire che l'elaborazione di un dato, la capacità di eseguire un calcolo e restituirne un risultato esatto in tempi più rapidi di quanto possa fare la menta umana, è ancora alla base del valore indiscusso dell'informatica. Ma le informazioni digitalizzate, sempre più dettagliate grazie alle pressoché infinite potenzialità degli strumenti di calcolo odierni, usate in modo inappropriato possono diventare una fonte di rischio enorme per enti pubblici e organizzazioni private, mettendo in gioco non solo la loro sicurezza, ma anche il destino stesso delle comunità e delle relazioni globali.

Emerge quindi con chiarezza la necessità impellente di una robusta strategia di data governance come fondamento imprescindibile per difendere le organizzazioni dall'inarrestabile ascesa dei rischi cyber. In un panorama in cui i dati sono il cuore pulsante delle organizzazioni pubbliche e private, la loro sicurezza non può prescindere da

un approccio oculato e strutturato, capace di tessere una rete difensiva intorno alle informazioni vitali, assicurandone l'integrità, la confidenzialità e la disponibilità.

La data governance non è più una mera pratica aziendale, ma il baluardo cruciale contro le tempeste digitali, un faro che guida attraverso i flutti pericolosi della cybersicurezza, assicurando la continuità operativa e la fiducia dei soggetti coinvolti; più spesso di quanto immaginiamo anche la vita delle persone.

L'uso improprio dei dati può infatti essere uno strumento potente nelle mani di movimenti politici, in grado di plasmare gli assetti economici e sociali di un intero paese. I dati manipolati possono essere sfruttati per influenzare le masse, orientare le elezioni e alterare il corso della storia in maniera subdola ma profonda.

Il pericolo, tuttavia, non si esaurisce nel contesto nazionale. La minaccia di un ransomware, ad esempio, non solo implica la richiesta di un riscatto monetario, ma alimenta anche un circolo vizioso in cui i fondi ottenuti vengono spesso reinvestiti per potenziare le stesse reti che operano in modo malevolo. Questo ciclo perpetuo rende la lotta contro le esfiltrazioni dei dati un campo di battaglia sempre più complesso e imprevedibile.

Le dimensioni del fenomeno del cybercrime sono ben rappresentate nel grafico che segue.

Figura 1 - Microsoft Data Security Index report

In ambito geopolitico, la manipolazione dei dati assume contorni ancor più gravi, trasformandosi in uno strumento di vantaggio strategico in territori di guerra. Gli effetti di queste azioni, come abbiamo purtroppo visto in passato, si riflettono in modo tangibile sulle relazioni internazionali, con conseguenze che vanno ben oltre l'ambito informatico.

In questo contesto, la necessità di una solida strategia di data governance emerge come imperativo categorico. Proteggere il dato non è solo preservare informazioni sensibili, ma è difendere la stabilità, la prospettiva economica, la democrazia e la sicurezza globale. La data governance diventa così la chiave maestra per contrastare il rischio derivante dalle esfiltrazioni malevole dei dati, salvaguardando il tessuto stesso della nostra società interconnessa.

Le regolamentazioni

Riconoscendo l'importanza dei dati come risorse vitali da proteggere, le organizzazioni internazionali e le autorità competenti agiscono promuovendo regolamentazioni atte a rispondere alla sfida, che naturalmente influenzano le strategie di security da adottare.

Tra le regolamentazioni più rilevanti in questo ambito, possiamo citare:

- il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nell'Unione Europea nel 2018, che stabilisce principi e obblighi per il trattamento dei dati personali, come la liceità, la trasparenza, la limitazione della finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità, la riservatezza, la responsabilizzazione, il consenso, il diritto di accesso, il diritto di rettifica, il diritto all'oblio, il diritto alla portabilità, il diritto di opposizione, il diritto alla limitazione del trattamento, il diritto di non essere sottoposti a decisioni automatizzate, ecc. Il GDPR prevede anche sanzioni severe per le violazioni, che possono arrivare fino al 4% del fatturato annuo globale o a 20 milioni di euro, a seconda del caso più grave;
- la Convenzione di Budapest sulla criminalità informatica, entrata in vigore nel 2004, che è il primo trattato internazionale che definisce e sanziona i reati informatici, come l'accesso illecito, l'intercettazione illecita, l'interferenza con i dati, l'interferenza con i sistemi, l'abuso di dispositivi, la falsificazione informatica, la frode informatica, la pornografia infantile, le violazioni della proprietà intellettuale, ecc. La Convenzione di Budapest prevede anche la cooperazione tra le parti contraenti per la prevenzione, l'investigazione e la persecuzione dei reati informatici, attraverso lo scambio di informazioni, l'assistenza reciproca, l'estradizione, ecc.;
- l'European Data Strategy, che punta a far dell'Unione Europea un punto di riferimento di società basata sui dati, creando un mercato unico per consentire il libero flusso dei dati tra settori e Stati membri. L'accesso e l'utilizzo dei dati sono fondamentali per stimolare l'innovazione e la crescita, con benefici tangibili come la medicina personalizzata, una migliore mobilità e politiche più efficaci. Il Data Governance Act facilita la condivisione dei dati e mira a generare valore per la società, garantendo allo stesso tempo il controllo ai cittadini e la fiducia alle aziende.

L'entrata in vigore del Data Act nel gennaio 2024 ha rafforzato ulteriormente la strategia, consentendo un maggiore utilizzo dei dati attraverso nuove regole che disciplinano l'accesso e l'uso dei dati in tutti i settori economici dell'UE;

- la Convenzione 108 del Consiglio d'Europa per la protezione delle persone con riguardo al trattamento automatizzato dei dati di carattere personale, entrata in vigore nel 1985, che è il primo trattato internazionale che riconosce il diritto alla protezione dei dati personali come diritto umano, e che stabilisce principi e garanzie per il trattamento dei dati personali, come la qualità dei dati, la finalità, la proporzionalità, la sicurezza, la trasparenza, il controllo, il diritto di accesso, il diritto di rettifica, il diritto di opposizione, ecc. La Convenzione 108 prevede anche la cooperazione tra le parti contraenti per la promozione e il monitoraggio del rispetto dei principi e delle garanzie, attraverso il Comitato consultivo, il Commissario per i diritti umani, il Comitato dei Ministri, ecc.;
- il Digital Operational Resilience Act (DORA), entrato in vigore nell'Unione Europea nel 2023, che stabilisce standard e requisiti per la gestione e la mitigazione dei rischi informatici e di sicurezza per il settore finanziario, come il risk management, il testing, il reporting, l'oversight, ecc. Il DORA si applica a 20 tipi diversi di entità finanziarie e a fornitori di servizi informatici di terze parti critici e prevede sanzioni per le violazioni, che possono arrivare fino al 2% del fatturato annuo globale o a 10 milioni di euro, nei casi più gravi.

A queste, che sono solo alcune delle più rilevanti, si possono aggiungere regolamentazioni locali come, ad esempio, le linee guida emanate dall'Agenzia per l'Italia Digitale per assicurare la protezione dei dati personali degli utenti che consultano i siti e i servizi online della pubblica amministrazione. Tra le principali possiamo annoverare: l'informativa sul trattamento dei dati personali [2], le linee guida sul documento informatico [3], linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni [4] e le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (agid.gov.it) [5] e le *linee guida del Garante delle Privacy.*

Iniziano inoltre a diffondersi regolamentazioni legate all'utilizzo degli strumenti basati su Intelligenza Artificiale, come *l'EU AI Act (first regulation on artificial intelligence | News | European Parliament (europa.eu),* alla stregua di pronunciamenti locali come l'analisi condotta dal Garante della Privacy sul tema *Intelligenza artificiale e ruolo della protezione dei dati personali.*

L'insieme delle regolamentazioni ha un impatto significativo sulle politiche legate alla data security, in quanto impone alle organizzazioni di adottare misure tecniche e organizzative adeguate a proteggere i dati da accessi, modifiche, divulgazioni o distruzioni non autorizzati, e di dimostrare la conformità alle norme e alle leggi

vigenti. Inoltre, favoriscono la creazione di uno spazio di fiducia e di sicurezza per il flusso dei dati tra i paesi e le regioni, e la collaborazione tra le autorità competenti per la prevenzione e il contrasto dei reati informatici; quindi, rappresentano un asset fondamentale per stabilire regole comuni su cui confrontarsi.

Tuttavia, i regolamenti forniscono le linee guida e stabiliscono i criteri da rispettare, lasciando alle organizzazioni autonomia sul corretto soddisfacimento dei requisiti. Questo impone di adottare una strategia metodica e lungimirante che si basa su aspetti organizzativi, di pianificazione strategica e di implementazione tecnologica su cui investire.

Dimensionamento del rischio legato al governo e protezione del dato

Secondo il report *State of Data Governance and Empowerment Report*, *Enterprise Strategy Group, July 2022*, più dell'80% degli operatori del settore valuta il furto o la perdita di dati personali e/o di proprietà intellettuale come rischi interni ad alto impatto. Inoltre, gli incidenti provocati da personale interno malintenzionato è una delle tipologie di incidenti più difficili da individuare e sui quali gli operatori del settore si sentono maggiormente scoperti in termini di strumenti di rilevazione e governo del fenomeno. Forrester, ad esempio, indica che rischi provenienti dall'interno delle organizzazioni sono causa del 26% delle violazioni di sicurezza segnalate nell'ultimo anno. Ciò che è ancora più significativo è che oltre la metà di questi incidenti si sono rivelati intenzionali (*Internal incidents cause roughly a quarter of breaches, with more than half intentional," Forrester, July 2023*).

È quindi chiaro che gli aspetti da considerare quando si affronta in maniera strutturale la tematica della protezione del dato sono di varia natura.

Proviamo a consolidarli in 3 macrocategorie di rischio:

- **il rischio esterno**: rappresentato da minacce, come hacker, criminali informatici o terroristi, che possono compromettere la protezione del dato, accedendo al dato senza autorizzazione o alterandolo, distruggendolo o diffondendolo. Questo tipo di rischio può causare danni materiali, come il furto di informazioni sensibili, il ricatto, la frode, il sabotaggio o la perdita del dato, o danni immateriali, come la violazione della riservatezza, della sicurezza, della reputazione o del vantaggio competitivo delle organizzazioni. Un esempio di rischio esterno è rappresentato dal caso Equifax. Nel 2017, l'azienda ha subito un enorme data breach. Attori malevoli hanno sfruttato una vulnerabilità nel software del sito web dell'azienda per accedere a dati sensibili di circa 148 milioni di persone. Questi dati includevano nomi, numeri di previdenza sociale, date di nascita, indirizzi e, in alcuni casi, numeri

di patente. Inoltre, i numeri di carta di credito di circa 209.000 consumatori e documenti di credito di circa 182.000 consumatori sono stati esposti. (Home | Equifax Data Breach Settlement (equifaxbreachsettlement.com) [6];

- **il rischio interno**: rappresentato da abusi, come insider, cioè persone che lavorano all'interno dell'organizzazione che protegge il dato, e che possono usare il dato in modo illecito, per scopi personali, professionali o politici. Questo tipo di rischio può causare danni simili a quelli del rischio esterno, ma con il vantaggio di avere un accesso privilegiato e una maggiore conoscenza del dato e dei sistemi. Un esempio di rischio interno è rappresentato al caso Cash App Investing. Nel 2021 Un ex dipendente ha scaricato rapporti aziendali dopo aver lasciato l'azienda, esponendo i dati sensibili di più di otto milioni di utenti. I dati esposti includevano nomi dei clienti, numeri di conto di intermediazione Cash App, valore del portafoglio del cliente, titoli e certa attività di trading Class Action Filed Over Cash App Investing Data Breach Affecting 8.2M Customers [7];
- **il rischio di non conformità**: rappresentato dalla violazione delle direttive nazionali ed internazionali in materia di protezione del dato, che stabiliscono i principi, i diritti, i doveri e le sanzioni applicabili alla protezione del dato. Questo tipo di rischio può causare danni legali, come multe, azioni giudiziarie, provvedimenti amministrativi o penali, o danni economici, come la perdita di clienti, di reputazione, di competitività o di opportunità di mercato. Un esempio di rischio di non conformità è il caso di Facebook, il più grande social network al mondo, che nel 2018 è stato coinvolto nello scandalo di Cambridge Analytica, una società di consulenza politica che ha sfruttato i dati di milioni di utenti di Facebook senza il loro consenso, violando il Regolamento generale sulla protezione dei dati (GDPR), la normativa europea in materia di protezione dei dati personali Caso Cambridge Analytica - Pagina informativa - Garante Privacy [8].

Una recente pubblicazione dello studio *Microsoft Data Security Index* rivela che gli episodi di violazione della sicurezza, caratterizzati da accessi non autorizzati ai dati, rappresentano una problematica ricorrente e attuale. Nell'ultimo anno il 74% delle organizzazioni intervistate ha subito almeno un incidente di sicurezza con esposizione dei dati aziendali, per una media di 59 incidenti nel periodo di osservazione per singola organizzazione (**circa 1 ogni 6 giorni**). Il 20% di questi eventi è stato considerato grave, con un potenziale costo annuo fino a 15 milioni di dollari. E questi numeri sono da considerarsi ottimistici poiché non tutte le organizzazioni sono in grado di rilevare accessi non voluti ad un dato, il che lascia pensare ad un fenomeno ben più diffuso.

Le vulnerabilità o lacune di processo si manifestano in varie dimensioni a causa di un insieme diversificato di fattori. Tra quelli che influenzano la sicurezza dei dati, i più

rilevanti sono la complessità dei dati, la conformità normativa, la mancanza di competenze, la gestione delle identità e degli accessi, e le minacce interne ed esterne.

Secondo il *Global Data Protection Index (GDPI) 2023 di Dell Technologies*, il 76% delle aziende italiane ha subito almeno un'interruzione dei sistemi informatici legata a incidenti o attacchi nel 2023, con un costo medio stimato tra 500 mila e 1 milione di dollari.

Causes of data security incidents	Most common incidents in the past 12 months	Least prepared to prevent in the next 12 months
Malware or ransomware	50%	41%
Compromised accounts	38%	35%
Denial-of-service (DoS) attacks	35%	33%
Negligent insiders	32%	29%
Inadvertent insiders	31%	32%
Malicious insiders	31%	35%
Physical property	29%	29%

Data Security Incidents Summary

Andando ad analizzare i dati, il malware o ransomware rappresentano il primo elemento di rischio, con un incremento significativo delle attività guidate da remoto (Human Operated Ransomware).

Nel 2023, secondo il *Microsoft Digital Defense Report*, questo tipo di attacco è raddoppiato e nel 13% dei casi ha comportato esfiltrazione del dato senza ricorre alla cifratura, attraverso una copia remota dei dati dell'organizzazione. Questo evidenzia ulteriormente quanto il dato sia strategico e a volte obiettivo finale di un attacco. Sempre dallo stesso report è interessante il dato relativo ai profili delle aziende attaccate e di quali siano i vettori che determinano il fattore di rischio principale: il 70% delle organizzazioni colpite hanno meno di 500 dipendenti, con ripercussioni gravissime in termini finanziari se comparate alla dimensione organizzativa.

Inoltre, è evidente che l'assenza di un approccio di gestione ad ampio spettro, olistico, costituisce un'importante sfida sia tecnica che organizzativa da affrontare. Se è vero che la quasi totalità degli attacchi ha origine da compromissione di dispositivi non gestiti dall'organizzazione, altrettanto vero è che questo aspetto va affrontato in termini tecnologici ma soprattutto organizzativi. Infatti, ciò che è possibile fare in ambito tecnico per una maggiore attenzione al rispetto delle buone pratiche di sicurezza, si scontra spesso con un piano organizzativo e normativo non lineare o ben definito che rallenta o inficia l'adozione delle misure tecniche previste.

Altro dato interessante è quello relativo agli indicatori che mostrano la percentuale di esfiltrazioni o esposizioni non lecite di dati avvenute tramite un attore che opera internamente all'organizzazione. Il cosiddetto "insider" (che sia intenzionalmente determinato ad un utilizzo improprio delle informazioni oppure solo per mancanza di procedure e/o formazione) rappresenta un rischio concreto a cui far fronte. Sebbene le organizzazioni tendano a evitare di divulgare i dettagli di tali incidenti, è importante riconoscere che gli insider rappresentano ancora il metodo più efficace per infiltrarsi nei sistemi interni di un'organizzazione. Di conseguenza, a volte vengono sfruttati (volontariamente o involontariamente) da attori sostenuti dallo stato o da gruppi criminali informatici per ottenere un accesso iniziale all'ambiente organizzativo. *ENISA Threat Landscape 2023.pdf, page 21*; *Insider Threat Mitigation Guide (cisa.gov)*

Ovviamente gli scenari di conflitto rappresentano un moltiplicatore dell'indice di rischio. È interessante constatare come, negli ultimi mesi, le strategie di attacco siano cambiate passando da una strategia incentrata sul blocco o distruzione dei servizi ad una fase di "intelligence" in cui l'esfiltrazione del dato risulta l'obiettivo finale dell'attaccante, che ovviamente avrà tutto l'interesse a mantenere invisibile tale operazione con il rischio di non accorgersi mai dell'avvenuta sottrazione (MDDR).

Figura 2 - Microsoft Data Security Index report

È inoltre cruciale sottolineare che, affinché un'organizzazione possa implementare efficacemente le politiche e le misure di protezione adeguate per i propri dati, tenendo conto sia della sicurezza che della conformità normativa, diventa essenziale avere una chiara comprensione della natura dei dati, della loro ubicazione, del loro utilizzo e del modo in cui si muovono all'interno dell'organizzazione.

Dal *Microsoft Data Security Index* emerge che il 76% degli operatori del settore sono preoccupati per la proliferazione dei dati fantasma e la "vulnerabilità dell'ignoto", rispetto ad una stima relativa alla produzione del dato che raddoppierà entro il 2026.

Facendo uno sforzo di sintesi, ecco alcuni dei più comuni impatti derivanti da un data breach o un accesso non conforme ai dati:

- la perdita di dati, che può comportare la violazione della privacy, la perdita di proprietà intellettuale, la perdita di competitività, la perdita di fiducia, la perdita di reputazione, la perdita di opportunità, ecc.;
- il danno ai sistemi, che può comportare la compromissione dell'integrità, della funzionalità, della disponibilità, della qualità, della performance, dell'affidabilità, dell'interoperabilità, ecc. dei sistemi informatici, delle reti, delle applicazioni, dei dispositivi, ecc.;
- l'impatto sull'attività, che può comportare la riduzione della produttività, della redditività, della crescita, della sostenibilità, della continuità, della resilienza, ecc. delle organizzazioni, dei processi, dei servizi, dei prodotti, ecc.;
- l'effetto sulla società, che può comportare la minaccia alla sicurezza nazionale e internazionale, alla democrazia, alla pace, alla stabilità, alla cooperazione, alla giustizia, ai diritti umani, all'ambiente, alla salute, all'istruzione, alla cultura, ecc.;
- il danno reputazionale, che può comportare la perdita di credibilità, la diminuzione della fiducia del pubblico, la svalutazione del marchio, la perdita di clienti, la difficoltà nel recupero dell'immagine pubblica, ecc.

Approccio strategico alla sicurezza del dato e ruolo dell'AI

La protezione dei dati è una responsabilità fondamentale per le organizzazioni, le quali devono essere consapevoli dei rischi e rispettarne le implicazioni al fine di assicurare la sicurezza dei dati e il rispetto dei diritti degli interessati, in linea con le normative vigenti. A tal fine, è essenziale adottare adeguate misure tecniche e organizzative, quali la pseudonimizzazione, la cifratura, la sicurezza informatica, la formazione del personale, la valutazione d'impatto, la nomina di un responsabile per la protezione dei dati, la notifica delle violazioni, la cooperazione con le autorità di controllo e la consultazione degli interessati. È altresì importante integrare i principi di protezione dei dati fin dalle fasi iniziali di progettazione delle applicazioni, delle

procedure, delle architetture dei sistemi e degli ambienti, stabilendoli come modalità predefinita e non come opzione aggiuntiva.

In questo tipo di contesto le organizzazioni dovrebbero adottare una strategia organizzativa in grado di gestire la complessità di questa sfida, di cui aspetti fondamentali sono:

- acquisizione di competenze specifiche in materia;
- convergenza fra unità organizzative con diverse responsabilità al fine di definire politiche efficaci, coerenti al contesto organizzativo, agli obiettivi tattici e strategici dell'organizzazione e ai requisiti regolatori, realizzabili e misurabili;
- dotazione di asset aziendali capaci di tradurre efficacemente le policy in operatività e che possano essere utilizzati a supporto di una corretta gestione del dato, della sua protezione e del suo (volontario o involontario) utilizzo in ambiti non consentiti.

Un elemento cruciale nella definizione di una strategia di cybersicurezza è quindi la convergenza tra le varie figure professionali che detengono competenze e responsabilità nella protezione dei dati e nella sicurezza informatica. Tra queste figure troviamo il CISO (Chief Information Security Officer), il CTO (Chief Technology Officer), il DPO (Data Protection Officer), Il CIO (Chief Information Officer) ed il CDO (Chief data Officer).

Queste figure dovrebbero cooperare strettamente per definire una strategia efficace ed efficiente, considerando sia gli aspetti tecnologici che quelli legali, organizzativi e aziendali. In particolare, dovrebbero:

- condividere obiettivi, priorità e budget relativi alla sicurezza informatica e alla protezione dei dati, in accordo con la strategia aziendale e le esigenze dei clienti;
- selezionare soluzioni tecnologiche adeguate ad assicurare l'uso corretto dei dati e proteggerli da malintenzionati, valutando benefici, costi e rischi associati;
- definire le politiche atte all'adempimento dei requisiti regolamentatori e di operatività in accordo con gli obiettivi dell'organizzazione;
- implementare soluzioni tecnologiche in modo sicuro e resiliente, aderendo alle best practice e agli standard di qualità, monitorando le performance e gestendo gli incidenti;
- formare e coinvolgere dipendenti, fornitori e partner sulla cultura della sicurezza e della privacy, promuovendo comportamenti responsabili e consapevoli;
- comunicare e rendere conto al top management e alle autorità di controllo delle attività e dei risultati ottenuti in ambito di cybersicurezza e protezione dei dati.

Per quanto riguarda invece la componente tecnologica, ovvero gli strumenti che permettono alle organizzazioni di tramutare un requisito di policy nell'operatività, è interessante partire da un dato che mostra una grande sovrapposizione di soluzioni di sicurezza. Secondo uno studio di IBM Cyber Resilient Organization Study 2021 | IBM [9], le organizzazioni hanno una sovrabbondanza di strumenti di cybersecurity (50 in media). Di questi, meno del 50% è effettivamente utilizzato e di questo 50% non tutte le funzionalità sono operative.

Le ragioni di questa situazione sono sicuramente da imputare a 2 fattori principali:

- la complessità degli ecosistemi da proteggere è aumentata esponenzialmente;
- esiste una stratificazione storica di sistemi e di procedure di acquisto.

Per analizzare come la situazione attuale interagisce con le tendenze e le necessità contemporanee, è indispensabile considerare una pluralità di fattori. Tuttavia, per una valutazione efficace e mirata, è cruciale concentrarsi su tre aspetti fondamentali.

La situazione contingente rispetto alle tendenze di investimento: conflitti mondiali, inflazione, instabilità economica di molti paesi portano le organizzazioni a contrarre gli investimenti. Il presente è quindi costellato di tagli al budget, anche sulle voci di spesa destinate alla cybersecurity, per diminuire l'esposizione finanziaria in favore di posizioni conservative in vista di "tempi migliori" e investimenti su aree considerate strategiche.
Utile uno studio di PricewaterhouseCoopers sul tema (*Decoding CEO Sentiments – gennaio 2024*), che restituisce buoni spunti su come relazionarsi con i propri CEO configurando la cybersecurity all'interno degli investimenti strategici

Necessità di aumentare il livello di trust della supply chain: è sempre più evidente che una postura di sicurezza adeguata non può prescindere dall'estensione delle buone pratiche di monitoraggio anche sui fornitori. Per questo è necessario valutare e scegliere un ristretto numero di partner a cui affidarsi, attraverso una validazione della loro solidità sul mercato anche in termini prospettici e in relazione alle misure specifiche adottate in ottica cybersecurity.

Di questo tema parlano diversi studi, fra cui quello di KPMG (*Cybersecurity considerations 2024*), mettendo in risalto una questione a lungo discussa soprattutto dopo l'attacco SolarWinds del dicembre 2020 con il potenziale coinvolgimento di 300.000 aziende inserite nella catena di fornitura dei prodotti alterati dall'attaccante. Non per ultimo, lo studio di Gartner Gartner Top Strategic Cybersecurity Trends 2023 [10], mette al primo posto fra i temi da affrontare per un nuovo approccio alla cybersecurity proprio quello del consolidamento delle piattaforme, per l'indiscussa opportunità di efficientamento che ne deriva.

Guadagnare efficienza e visibilità rispetto ad ecosistemi complessi: come dimostrato da diversi studi, spesso la proliferazione di soluzioni in ambito cybersecurity aumenta la complessità e riduce l'efficienza. Questo perché la mancanza di interazione nativa fra soluzioni differenti comporta progettualità di integrazione che generano ritardi, aumenta i costi, e genera potenziale inefficienza e crea delle zone d'ombra che potrebbero generarsi fra una soluzione e l'altra.

Considerando che l'MTT (Middle Time to Triage) rappresenta un elemento cruciale per determinare se un evento sia effettivamente dannoso, consentendo così di organizzare tempestivamente una risposta efficace, diventa evidente l'importanza di rivedere gli asset strategici su cui si fonda la strategia di cybersecurity. Questo processo di revisione è fondamentale per assicurare che l'approccio adottato sia non solo efficiente ma anche adeguatamente esteso a coprire tutte le possibili minacce, garantendo così la massima protezione.

Dal Data Security Index rilasciato da Microsoft e hypotesis, emerge che le organizzazioni che impiegano un numero più elevato di soluzioni di cybersecurity sono 3 volte più esposte ad incidenti rispetto ad organizzazioni dello stesso tipo che hanno consolidato la loro piattaforma di protezione.

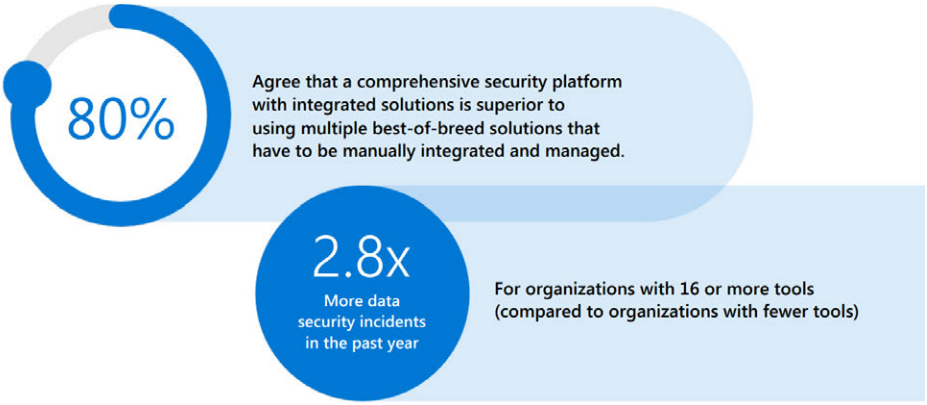
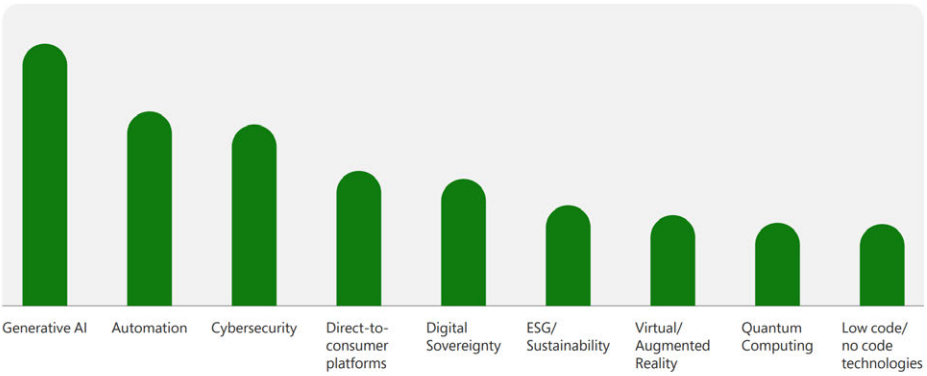


Figura 3 - Data Security Index - Microsoft/hypothsis

Partendo da queste considerazioni possiamo analizzare il ruolo che l'Artificial Intelligence può avere nel contesto della protezione del dato. Partiamo dal fornire un'indicazione importante sul tema delle priorità da considerare quando si rappresenta una strategia di cybersecurity a chi deve decidere come investire i capitali a disposizione (CEO/CFO).



Source: IDC, C-Suite Tech Agenda: Priorities and of AI, doc #US51335623, November 2023

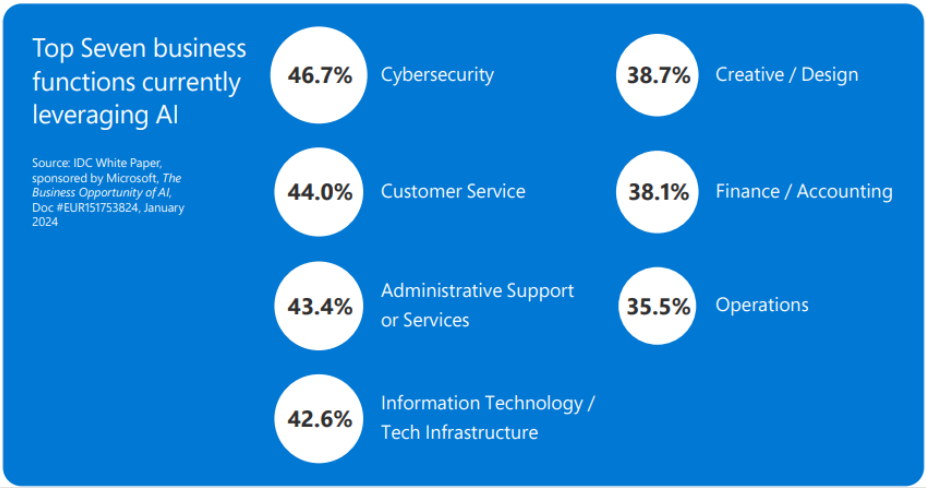
Considerando che l'Intelligenza Artificiale (AI) ha influenzato il nostro panorama digitale per oltre cinquanta anni, l'impetuoso slancio osservato negli ultimi venti mesi può essere attribuito alla democratizzazione delle tecnologie AI, resa possibile dall'introduzione del trattamento del linguaggio naturale nelle loro funzionalità. Questo sviluppo ha notevolmente facilitato l'accesso e l'uso dell'AI da parte di un'ampia gamma di utenti, stimolando un'adozione diffusa e trasformando radicalmente il modo in cui interagiamo con le tecnologie digitali.

Vantaggi indiscussi sono quelli legati alla produttività personale. Il recente studio di Ambrosetti (AI 4 Italy: Impatti e prospettive dell'Intelligenza Artificiale Generativa per l'Italia e il Made in Italy) [11] afferma che l'impatto economico apportato dall'introduzione di questi strumenti porterà benefici per un valore fino a 312 miliardi di Euro, pari al 18% del PIL italiano.

È significativo notare che il 78% delle organizzazioni intervistate ha riferito di aver già implementato o di avere l'intenzione di implementare strumenti di Intelligenza Artificiale Generativa, evidenziando un consenso generale sull'importanza di questa tecnologia. Questo dato indica chiaramente che l'AI Generativa rappresenta una notevole opportunità, attirando l'interesse di coloro che sono incaricati di prendere decisioni strategiche sugli investimenti.

Dal l recente studio di IDC, *The business opportunity of AI* emerge che la cybersecurity è il primo caso d'uso di utilizzo dell'Artificial Intelligence. Il già citato studio di Gartner (Gartner Top Strategic Cybersecurity Trends 2023) [10] suggerisce inoltre l'adozione di sistemi Human-Centric come fulcro di una strategia di cybersecurity in

grado di aiutare gli operatori del settore a guadagnare efficacia: l'AI di tipo generativo rappresenta quindi uno strumento che permette di aumentare la produttività e l'efficacia dei professionisti della sicurezza.



Più nel concreto, quale potrebbe essere l'aiuto dell'AI generativa in una strategia di cybersecurity che comprenda la difesa del dato come uno degli obiettivi primari? Per rispondere questa domanda proviamo a analizzare alcune evidenze.

Una strategia di protezione del dato è essenzialmente basata su alcuni principi base:

- identificazione, che consiste nel riconoscere e valutare i dati, i sistemi, le minacce, le vulnerabilità, i rischi, gli obiettivi, le priorità, le responsabilità, ecc. relativi alla data security;
- pianificazione, che consiste nella creazione di policy che dettino le linee guida di come è opportuno gestire e proteggere i dati in relazione ai dettami normativi e agli obiettivi dell'organizzazione;
- attuazione, che consiste nella messa in opera delle policy di controllo attraverso l'adozione di strumenti adatti allo scopo, coadiuvata da un'attività di divulgazione verso l'utente finale;
- rilevazione, che consiste nel monitorare e analizzare i dati, i sistemi, le attività, gli eventi, gli incidenti, le anomalie, ecc. relativi alla data security, attraverso l'uso di strumenti e metodi appropriati, come raccolta dei log, l'auditing, il test, la scansione, l'allarmistica, la reportistica, ecc.;

- risposta, che consiste nel reagire e intervenire in modo tempestivo ed efficace agli attacchi cibernetici o alle violazioni della data security, attraverso l'attivazione di piani e procedure prestabiliti, come il contenimento, l'eradicazione, il recupero, la notifica, l'escalation, la mitigazione, l'investigazione, ecc.;
- ripristino, che consiste nel riparare e ripristinare i dati o i sistemi danneggiati o persi a seguito di attacchi cibernetici o violazioni della data security, attraverso l'implementazione di soluzioni e misure opportune, come il backup, il ripristino, il disaster recovery, il business continuity, il patching, l'hardening, l'upgrading, ecc.;
- miglioramento, che consiste nel migliorare e aggiornare continuamente la data security e la strategia di cybersecurity, attraverso il feedback, la revisione, la valutazione, la misurazione, la verifica, la validazione, l'ottimizzazione, l'innovazione, l'apprendimento, ecc.

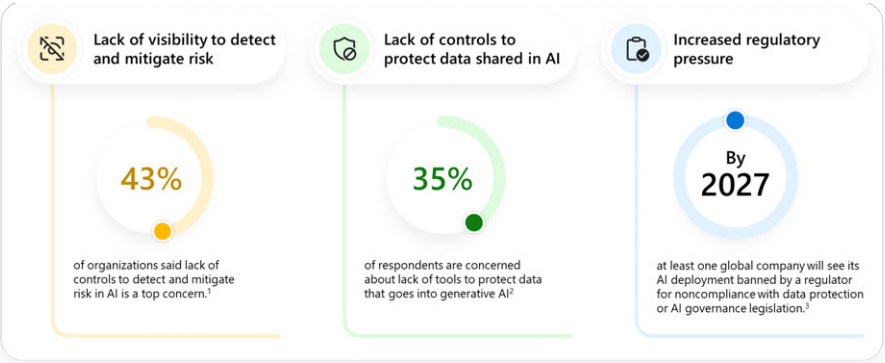


Figura 4 - 1. Data Security Index report, Oct 2023 commissioned by Microsoft; 2. Survey of 658 data security professions, Mar 2023, commissioned by Microsoft- 3. Gartner Security Leader's Guide to Data Security, Sep 2023

In questo contesto, è essenziale riconoscere la vasta diversità dei sistemi utilizzati attualmente dalle organizzazioni a livello globale per comprendere che l'identificazione dei dati rappresenta di per sé un'attività critica e complessa. Secondo la Cloud Security Alliance, le organizzazioni usano in media 147 servizi cloud pubblici che includono SaaS, PaaS e IaaS. (*Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022).*

Data l'enorme complessità ed eterogeneità che rappresenta lo standard de facto degli ecosistemi informatici moderni, strumenti basati sull'AI possono intervenire apportando grandi benefici, sia in termini di analisi e pianificazione, che in termini di operatività e reportistica.

Operativamente parlando, proviamo ad affrontare il tema attraverso una schematizzazione in 3 diverse fasi:

1 individuare e proteggere i dati sensibili: ovvero, determinare dove si trovano i dati, di che tipo di dati si tratta e come vengono utilizzati o condivisi. Classificare i dati importanti per l'organizzazione e applicare le misure di sicurezza appropriate, come la crittografia, le restrizioni di accesso e le marcature visive;
2 comprendere il contesto dell'utente e rilevare i rischi critici: ovvero, rilevare i rischi critici legati a come vengono accedute e utilizzate le informazioni, evidenziando l'importanza della gestione del rischio interno. Il rischio interno è rappresentato dalle persone che hanno informazioni sui tuoi dati, sui sistemi informatici e sulle pratiche di sicurezza. Questo processo deve comprendere dipendenti, fornitori, collaboratori e partner. Per prevenire il rischio interno, serve monitorare e analizzare il comportamento degli utenti e intervenire in caso di attività sospette o inappropriate;
3 prevenire la perdita di dati: ovvero, individuare strategie e soluzioni di prevenzione della perdita di dati (DLP) per evitare che questi vengano esposti in ambienti non affidabili o violino i contesti normativi, senza che sia compromessa la produttività e in considerazioni di condizioni che possono cambiare nel tempo.

Per ognuno di questi aspetti è possibile elencare numerose capacità offerte da soluzioni basate su modelli di Machine Learning e Artificial Intelligence che possono rappresentare un importante vantaggio per affrontare le sfide attuali.

L'intelligenza artificiale e l'apprendimento automatico possono infatti aiutare a scoprire i dati sensibili (come la proprietà intellettuale e i segreti commerciali) e a classificarli automaticamente. Queste tecnologie si basano sull'uso di algoritmi che analizzano grandi quantità di dati, apprendono dagli insights e poi prendono decisioni informate. I modelli di apprendimento automatico migliorano le prestazioni nel tempo man mano che vengono addestrati, esposti a più dati. Questa tecnologia di classificazione può coprire l'intero patrimonio di dati, scansionandoli, etichettandoli e proteggendoli ovunque si trovino, da quelli on-premise a quelli basati sul cloud, dai servizi software-as-a-service (SaaS) alle applicazioni native del sistema operativo.

La capacità dell'IA di elaborare enormi quantità di dati in tempo reale consente di pensare ad una visibilità estesa di ambienti eterogenei e distribuiti, e un'identificazione tempestiva di comportamenti anomali. Ciò non solo protegge da potenziali attacchi e minacce informatiche, ma può anche migliorare la conformità alle normative sulla privacy e alla sicurezza dei dati.

L'Intelligenza Artificiale generativa, integrata con strumenti adatti allo scopo, può inoltre svolgere un ruolo cruciale nel rilevare e individuare prontamente tipologie

di dati che non dovrebbero essere esposti o condivisi. Attraverso algoritmi di riconoscimento pattern e analisi avanzata, l'AI può contribuire a identificare anomalie e violazioni della sicurezza, anticipando potenziali rischi prima che causino danni irreparabili.

Consideriamo inoltre l'impatto in termini di produzione di reportistica in relazione all'avvento di normative come la NIS2 e quali siano le potenzialità in questo ambito dell'AI di tipo generativo.

L'AI di tipo generativo permette inoltre un'interazione semplificata con gli strumenti di governo, riducendo i tempi legati alla presa di coscienza di un fenomeno, all'interpretazione dello stesso attraverso la capacità di aumentare in maniera contestuale il grado di competenza un operatore.

Algoritmi di Machine Learning possono essere impiegati per calcolare il livello di rischio di una determinata condizione e adattare politiche di sicurezza da adottare in base ad un calcolo estemporaneo del livello di rischio. L'indiscusso beneficio di policy adattabili si riflette sulla possibilità di lasciare che un operatore interagisca nel migliore dei modi con le informazioni, bloccando solamente le situazioni valutate rischiose.

Questi aspetti vanno di pari passo con la capacità nascente rappresentata dal binomio Artificial Intelligence e automazione che semplificano la vita in molti campi attraverso azioni autonome, contestualizzate e contestuali in termini temporali, che possono ridurre drasticamente i livelli di rischio.

D'altra parte, con l'aumento dell'uso dell'AI, diventa essenziale migliorare la sicurezza dei dati per consentirne un utilizzo responsabile e prevenire i rischi di un utilizzo non desiderato. Le preoccupazioni delle organizzazioni riguardo l'uso dell'AI (in particolar modo di quella generativa) includono la mancanza di controllo sui dati condivisi, la mancanza di controlli per rilevare e mitigare l'uso rischioso dell'AI, la mancanza di trasparenza su come sono addestrati i modelli generativi di AI e la perdita di informazioni confidenziali.

A queste preoccupazioni serve rispondere ancora una volta con un approccio strutturato che veda, già in fase di pianificazione della strategia aziendale, l'impiego di strumenti che possano governare i nuovi canali rappresentati dall' AI Generativa attraverso l'adozione di soluzioni di monitoraggio e controllo più possibile integrate, per guadagnare efficienza e visibilità.

In sintesi, sebbene l'utilizzo di strumenti di Intelligenza Artificiale generativa porti con sé rischi intrinseci legati alla manipolazione di dati riservati, il suo potenziale

nell'individuare e prevenire violazioni della sicurezza rappresenta un aspetto cruciale nella gestione moderna dei dati sensibili. La sfida consiste nell'equilibrare la massimizzazione dei vantaggi derivanti dall'utilizzo di questa tecnologia con una rigorosa governance dei dati, assicurando che la sua implementazione avvenga nel rispetto della privacy e della sicurezza.

Nonostante alcuni aspetti da tenere sotto controllo, è unanime il riconoscimento del potenziale dell'AI generativa, specialmente considerando che i fornitori di mercato stanno sviluppando innovazioni per favorire un utilizzo responsabile dell'AI da parte delle imprese.

D'altro canto, il ruolo degli esperti di cybersecurity non è quello di limitare la spinta evolutiva ma di ridurne i fattori di rischio attraverso un approccio organico e capace di accogliere l'innovazione. L'uso di applicazioni e piattaforme cloud per collaborare, insieme alla nuova era dell'AI generativa, promettono di migliorare notevolmente la produttività delle persone e permettono modalità di lavoro flessibili e nuovi modi per interagire, produrre e sfruttare il sapere, rendendo le applicazioni cloud e la tecnologia AI fondamentali per il miglioramento della nostra quotidianità.

Conclusioni

In questo capitolo ci siamo concentrati sui fattori cruciali da considerare nella pianificazione e nell'attuazione di una strategia di cybersecurity finalizzata ad assicurare la corretta protezione dei dati, anche in relazione all'introduzione degli strumenti di Intelligenza Artificiale nella quotidianità operativa e nelle strategie di investimento.

Basandoci su ricerche condotte dai principali attori del mercato, desideriamo sottolineare quanto segue:

- adottare una solida strategia di governance e sicurezza dei dati è essenziale per prevenire gravi conseguenze derivanti dall'uso improprio delle informazioni, nel rispetto delle normative vigenti e per assicurare la solidità delle organizzazioni e delle istituzioni. Questo aspetto è particolarmente rilevante considerando il contesto geopolitico attuale e l'introduzione di nuove tecnologie che comportano nuovi rischi da considerare attentamente;
- un elemento fondamentale di una strategia di cybersecurity è assicurare una copertura completa di tutti gli ambiti e dei servizi forniti dall'organizzazione, identificando un numero limitato di partner in grado di fornire soluzioni e servizi interoperabili, migliorando così l'efficienza e la capacità di risposta dell'organizzazione.

- le soluzioni di Intelligenza Artificiale, soprattutto quelle che utilizzano strumenti generativi, possono costituire una leva per accelerare gli investimenti nel campo della cybersecurity. Inoltre, contribuiscono al governo dei complessi ecosistemi delle organizzazioni moderne grazie alla loro capacità unica di semplificare la complessità e renderla comprensibile agli operatori. Queste tecnologie rappresentano un elemento essenziale per aumentare la produttività e, di conseguenza, l'efficienza ed efficacia nel campo della cybersecurity.

Sitografia

[1] https://it.wikipedia.org/wiki/Societ%C3%A0_dell%27informazione
[2] https://www.agid.gov.it/it/privacy-policy
[3] https://www.agid.gov.it/sites/default/files/repository_files/manualeconservazione_nuovelgv24092021-signed.pdf
[4] https://www.agid.gov.it/it/linee-guida
[5] https://trasparenza.agid.gov.it/archivio19_regolamenti_0_5385.html
[6] https://www.equifaxbreachsettlement.com/
[7] https://www.classaction.org/news/class-action-filed-over-cash-app-investing-data-breach-affecting-8-2m-customers
[8] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8376626
[9] https://www.ibm.com/resources/guides/cyber-resilient-organization-study/
[10] https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
[11] https://acadmin.ambrosetti.eu/dompdf/crea_wmark.php?doc=L2F0dGFja-G1lbnRzL3BkZi9haS00LWl0YWx5LW1pY3Jvc29mdC1yZXBvcnQtMjAyMy0yM-DIzMDkwMTA5LnBkZg%3D%3D&id=18602&muid=corporate

Sviluppo sicuro del codice software

[A cura di Roberto Obialero]

Analisi del contesto

Il tema di garantire la fruizione di applicazioni software scritte in modo sicuro, ovvero senza presenza di vulnerabilità indotte dallo stesso codice sorgente utilizzato per la loro creazione è relativamente poco conosciuto.

Generalmente tali buone pratiche non vengono insegnate nei percorsi di formazione degli sviluppatori software e nelle diverse fasi di design e realizzazione delle applicazioni non vengono sufficientemente approfonditi i requisiti sulla loro sicurezza.

A questo si può aggiungere anche la costante necessità di anticipare i rilasci del software, rinunciando ad alcune fasi di esecuzione dei test, per mantenere il vantaggio competitivo rispetto alla concorrenza.

Va infine considerata la poca propensione delle organizzazioni clienti a richiedere che, oltre ai requisiti funzionali, vengano rispettati anche dei requisiti di sicurezza informatica in un mercato ancora lontano dall'espressione di un livello qualitativo di alto livello.

Tutti questi fattori portano alla commercializzazione di prodotti software che nel corso del loro ciclo di vita richiedono l'applicazione di un numero importante di aggiornamenti per garantirne la sicurezza: a titolo esemplificativo nel corso del solo 2023 Microsoft ha reso disponibile oltre 900 aggiornamenti alla suite dei suoi prodotti durante le campagne mensili denominate "patch Tuesday", ma anche altri grandi concorrenti quali Adobe, Oracle, Google, SAP e Mozilla possono vantare dei numeri altrettanto rilevanti.

Le cause del fenomeno sono molteplici e possono essere ricercate nella mancata conoscenza delle buone prassi nel settore, nella mancata integrazione di un processo accurato di testing di sicurezza nella pipeline di produzione del software e soprattutto dalla mancata diffusione di una cultura che dovrebbe da un lato essere impartita agli aspiranti sviluppatori software già a livello universitario e dall'altro parte del DNA dei settori IT delle imprese.

Analizzando i percorsi di formazione "certificati" dalle organizzazioni che offrono training specializzato nella sicurezza il panorama risulta relativamente ristretto con la formazione specifica offerta dai più autorevoli soggetti quali SANS, ISC2 e pochi altri.

Un plauso va rivolto ai progetti internazionali collaborativi su base volontaria che nel corso degli anni hanno prodotto documentazione validissima a supporto degli sviluppatori e dei tester coinvolti nel processo.

Nel dettaglio il progetto OWASP (Open Web Application Security Project)[1], forte di una diffusa collaborazione tra sviluppatori ed aziende del settore, ha pubblicato nel corso degli anni documentazione caratterizzata da un eccellente livello qualitativo che è diventata un riferimento per gli attori coinvolti: oltre al "Top 10 Web Application Security Risk" ripreso nella totalità dei tool impiegati per la verifica della sicurezza delle applicazioni web sono degni di nota le guide specifiche per i designer e per i tester, le guide per gli sviluppatori di codice mobile ed il "Software Assurance Maturity Model".

Un altro progetto interessante e rappresentato da "Common Weakness Enumeration"[2], proposto in origine dal SANS Institute ed attualmente mantenuto da MITRE Corporation; tale progetto, che oltre alle applicazioni web tiene conto anche delle tecnologie client server è partito dall'elenco dei "CWE Top 25 Most Dangerous Software Weaknesses" per poi essere esteso anche a "CWE Most Important Hardware Weaknesses" fino ad abbracciare recentemente il tema "2023 CWE Top 10 KEV Weaknesses" che, in collaborazione con CISA indica le vulnerabilità di cui è ormai noto lo sfruttamento.

Attacchi facilitati da vulnerabiltà software

Le vulnerabilità software hanno indubbiamente favorito delle attività illecite; nella tabella seguente sono elencati alcuni attacchi informatici rappresentativi occorsi nel 2023.

[1] https://owasp.org/#

[2] https://cwe.mitre.org/index.html

Data	Problema	Impatto	Riferimento
4/1/2023	Vulnerabilità nelle API impiegate in ambito automotiv	Esposizione dati personali	https://www.bleepingcomputer.com/news/security/toyota-mercedes-bmw-api-flaws-exposed-owners-personal-info/
23/1/2023	Accesso non autorizzato a repository di sviluppo software	Data breach	https://www.valencesecurity.com/resources/blogs/circleci-says-hackers-stole-encryption-keys-and-customers-secrets
28/4/2023	Accesso non autorizzato a repository di sviluppo software	Esecuzione codice malevole	https://gbhackers.com/git-project-security-vulnerabilities/
5/5/2023	Vulnerabilità plugin software CMS (oltre 2M di installazioni)	Possibile attacco XSS sui siti web che utilizzano il plugin	https://www.bleepingcomputer.com/news/security/wordpress-custom-field-plugin-bug-exposes-over-1m-sites-to-xss-attacks/
6/7/2023	Vulnerabilità software telecamere VDS	Accesso ad informazioni personali	https://ciso.economictimes.indiatimes.com/news/vulnerabilities-exploits/cert-in-warns-of-information-disclosure-vulnerability-in-bosch-ip-camera-severity-rating-medium/
17/8/2023	Vulnerabilità software	Possibile attacco DOS	https://www.cisa.gov/news-events/alerts/2023/08/17/atlassian-releases-security-update-confluence-server-and-data-center

Cambio di paradigma devops

Nel corso degli ultimi anni, per venire incontro alle esigenze legate ad una maggior efficienza ed alla necessità di rilasciare continui aggiornamenti riducendo al contempo i rischi per le organizzazioni si è affermato il paradigma di sviluppo DevOps, basato su un'architettura applicativa a micro servizi.

Il termine deriva dalla contrazione delle parole "Development", ovvero le attività di sviluppo software caratterizzate da una forte dipendenza dai nuovi e spesso mutevoli requisiti di business e "Operations", ovvero le attività di gestione ICT che tendono a privilegiare le esigenze di disponibilità delle informazioni salvaguardando nello stesso tempo i costi associati; questo connubio deve naturalmente conciliarsi con le esigenze di qualità del prodotto software rilasciato.

Nella figura seguente viene riportata in forma grafica l'intersezione tra i concetti appena declinati.

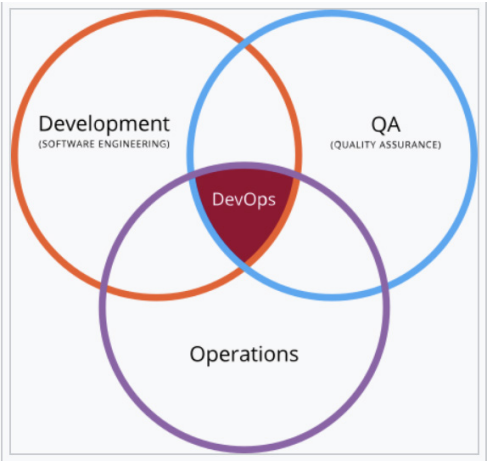


Figura 1 - Fonte WikiPedia *(Rapporto CLUSIT 2024)*

Come vedremo nei paragrafi successivi questo cambio di approccio ha un impatto significativo sull'esecuzione dei test funzionali e di sicurezza nella pipeline del processo di sviluppo software.

Sicurezza applicativa nei principali framework di sicurezza

Il tema della sicurezza del software applicativo viene indirizzato nei principali framework generali adottabili a livello internazionale; nei successivi paragrafi sono raggruppati i principali controlli applicabili al processo di sviluppo sicuro del software.

Controlli ISO/IEC 27002:2002

Nella recente versione del principale framework utilizzato nella certificazione dei sistemi di gestione della sicurezza delle informazioni lo sviluppo viene trattato in una sezione dei controlli tecnologici; nella figura seguente sono dettagliati i controlli associati alle rispettive funzioni di sicurezza.

Controlli tecnologici	8.26 Requisiti di sicurezza delle applicazioni		Protect	
Controlli tecnologici	8.27 Sicurezza nell'architettura dei sistemi e nei principi di ingegnerizzazione sicura		Protect	
Controlli tecnologici	8.28 Sviluppo sicuro		Protect	
Controlli tecnologici	8.29 Test di sicurezza in fase di sviluppo e di accettazione	Identify		
Controlli tecnologici	8.30 Sviluppo affidato all'esterno	Identify	Protect	Detect
Controlli tecnologici	8.31 Separazione degli ambienti di sviluppo, test e produzione		Protect	
Controlli tecnologici	8.32 Gestione dei cambiamenti		Protect	
Controlli tecnologici	8.33 Dati di test		Protect	
Controlli tecnologici	8.34 Protezione dei sistemi informativi durante gli audit e i test		Protect	

Figura 2 - Subset controlli ISO/IEC 27002 *(Rapporto CLUSIT 2024)*

Controlli NIST Cybersecurity Framework V1.1

In attesa della imminente formalizzazione della nuova versione 2.0 del framework americano NIST si può notare come il tema dello sviluppo sicuro del software non abbia una copertura troppo dettagliata, pur essendo presente.

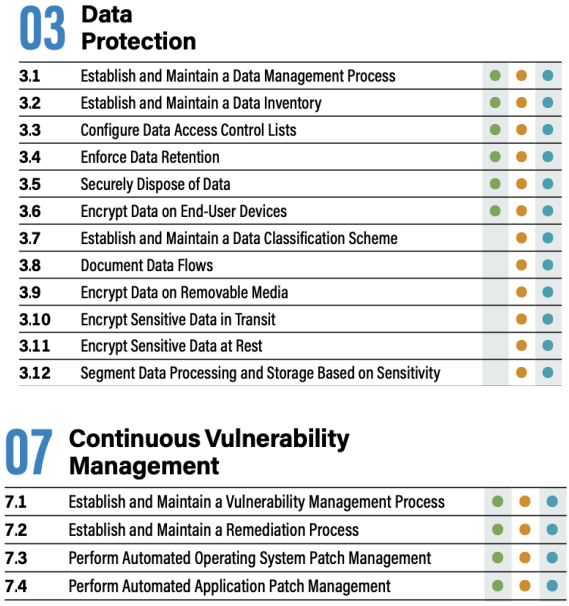
Function	Category	Subcategory
IDENTIFY (ID)	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio
PROTECT (PR)	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).
		PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità

Figura 3 - Subset controlli NIST CSF v1.1 *(Rapporto CLUSIT 2024)*

Controlli CIS CSC V.8

Come si può evincere dalla figura seguente, nell'ambito dei 153 "Critical Security Controls" che contraddistinguono il framework di sicurezza del CIS-Center for Internet Security viene data ampia copertura al tema della sicurezza delle applicazioni, cui è stata attribuita una specifica categoria di controlli.

Mentre nella prima colonna, evidenziata in verde, sono contrassegnati i controlli dell'Implementation Group 1, definiti "Basic Cybersecurity Hygiene" si può notare che buona parte dei controlli, evidenziati in arancione, viene suggerita per tutte le realtà con un buon livello di complessità che debbano affrontare le minacce più comuni.



03 Data Protection

3.1	Establish and Maintain a Data Management Process	●	●	●
3.2	Establish and Maintain a Data Inventory	●	●	●
3.3	Configure Data Access Control Lists	●	●	●
3.4	Enforce Data Retention	●	●	●
3.5	Securely Dispose of Data	●	●	●
3.6	Encrypt Data on End-User Devices	●	●	●
3.7	Establish and Maintain a Data Classification Scheme		●	●
3.8	Document Data Flows		●	●
3.9	Encrypt Data on Removable Media		●	●
3.10	Encrypt Sensitive Data in Transit		●	●
3.11	Encrypt Sensitive Data at Rest		●	●
3.12	Segment Data Processing and Storage Based on Sensitivity		●	●

07 Continuous Vulnerability Management

7.1	Establish and Maintain a Vulnerability Management Process	●	●	●
7.2	Establish and Maintain a Remediation Process	●	●	●
7.3	Perform Automated Operating System Patch Management	●	●	●
7.4	Perform Automated Application Patch Management	●	●	●

16	Application Software Security		
16.1	Establish and Maintain a Secure Application Development Process	●	●
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	●	●
16.3	Perform Root Cause Analysis on Security Vulnerabilities	●	●
16.4	Establish and Manage an Inventory of Third-Party Software Components	●	●
16.5	Use Up-to-Date and Trusted Third-Party Software Components	●	●
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	●	●
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	●	●
16.8	Separate Production and Non-Production Systems	●	●
16.9	Train Developers in Application Security Concepts and Secure Coding	●	●
16.10	Apply Secure Design Principles in Application Architectures	●	●
16.11	Leverage Vetted Modules or Services for Application Security Components	●	●
16.12	Implement Code-Level Security Checks		●
16.13	Conduct Application Penetration Testing		●
16.14	Conduct Threat Modeling		●

Figura 4 - Subset controlli CIS CSC v8 *(Rapporto CLUSIT 2024)*

Sicurezza applicativa nelle principali normative europee

Analizzando le previsioni contenute nelle principali normative europee sul tema data protection e cybersecurity si possono trovare diversi riferimenti riconducibili allo sviluppo sicuro di applicazioni.

Regolamento GDPR

Nell'ambito delle regole fissate dal Regolamento GDPR il principio più importante è senz'altro declinato nell'Art. 25 relativo al tema "Privacy by design/by default" che richiama in modo specialistico il metodo dell'introduzioni di controlli sulla privacy/sicurezza sin dalle prime fasi della progettazione di una nuova soluzione/trattamento dati personali.

Il tema dello sviluppo sicuro è inoltre affrontato indirettamente anche negli Art. 28, relativo agli obblighi cui è soggetto il responsabile del trattamento (in riferimento a delle attività di sviluppo software esternalizzato), oltre all'Art. 32, relativo alle misure di sicurezza da applicare al trattamento di dati personali.

Direttiva NIS2

Nell'ambito della nuova Direttiva NIS2 viene sancito nell'Art. 21.2.d l'obbligo di valutare i rischi relativi alla catena di fornitura, sempre in riferimento ad uno sviluppo software affidato all'esterno, mentre nel successivo Art. 21.2.e si fa riferimento al processo di acquisizione, sviluppo e manutenzione di sistemi informatici, con particolare riferimento alla gestione delle vulnerabilità.

Regolamento Cyber Resilience ACT

Il tema dello sviluppo sicura del software viene trattato in modo molto dettagliato nel Regolamento Cyber Resilience Act (CRA), relativo ai requisiti cybersecurity per i prodotti che impiegano elementi digitali, tra cui il software applicativo, di sistema ed il firmware che auspicabilmente vedrà la luce entro la fine del 2024.

Analizzando la bozza di proposta della normativa si trovano parecchi elementi applicabili: in particolare all'Art. 5 viene definito il principio relativo alla possibile commercializzazione di prodotti soltanto se il produttore sia in grado di rispettare determinati processi di lavorazione e requisiti essenziali di sicurezza.

Come le normative precedenti anche il CRA è di natura "risk based"; tale principio viene affermato nell'Art. 10, che sottopone l'obbligo della valutazione dei rischi in capo al fabbricante.

Nell'Art. 24 vengono poi affrontati i criteri di valutazione di conformità al regolamento ed i requisiti ritenuti essenziali a garanzia degli elementi di riservatezza, integrità e disponibilità delle informazioni trattate, che dovranno soddisfare i prodotti, anche in virtù della loro destinazione d'uso, prima di essere messi in commercio.

Processo di sviluppo e test di sicurezza applicativa

Le problematiche evidenziate nei paragrafi precedenti possono essere indirizzate efficacemente adottando un adeguato programma che indirizzi la sicurezza sin dalle prime fasi di progettazione dell'applicazione software e non si concluda con la fase di deilvery ma segua tutto il ciclo di vita dell'applicazione, spesso intesa con l'acronimo SSDLC, ovvero Secure Software Development Life Cycle.

Partendo dal presupposto che gli attori coinvolti nel processo sono essenzialmente tre:

1. il cliente finale, ovvero l'entità che utilizza il software;
2. il fornitore, che può essere anche nell'area organizzativa del cliente nel caso di servizio di sviluppo software interno;
3. il team operativo di sviluppo, che può essere caratterizzato in modo interno o esterno.

Il processo di progettazione e gestione dell'applicazione software, declinato secondo il paradigma DevSecOps, può essere schematizzato nella figura seguente[3].

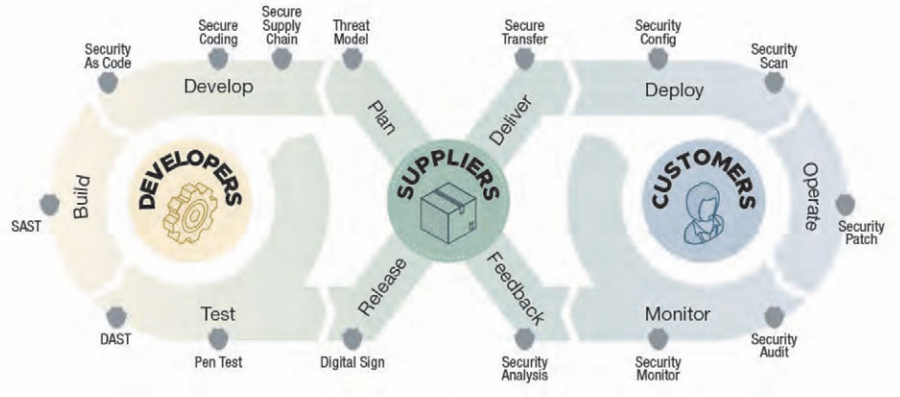


Figura 5 - Processo di sviluppo sicuro del software *(Rapporto CLUSIT 2024)*

Fasi del processo di sviluppo sicuro del software

A fronte della presentazione dei requisiti da parte del cliente il fornitore provvede a progettare le fasi di sviluppo tenendo conto dei modelli di minaccia, ovvero tutto quello che potrebbe pregiudicare la sicurezza del prodotto.

Il Developer team Inizia la fase di sviluppo approntando la cosiddetta SBOM (Software Bill Of Materials) per comprendere a titolo preliminare se e quali componenti esterni, che potrebbero introdurre delle vulnerabilità, verranno impiegati nel progetto, poi ha inizio la fase di scrittura del codice software; una volta completata questa fase è opportuno che un team separato, cui vengono attribuite le responsabilità delle attività di testing, provveda ad effettuare, tramite specifici tool automatici, l'analisi statica del codice SAST (Static Application Security Testing).

Nel caso di presenza di vulnerabilità è opportuno correggerle tempestivamente per poi passare alla fase build del software ed a verificarne contestualmente l'esecuzione nell'ambiente di test mediante dei tool DAST (Dynamic Application Security Testing) ed una verifica finale, generalmente effettuata in modo manuale, della sua sicurezza da parte di team di ethical hacker (che eseguiranno un penetration test sia di tipo infrastrutturale che applicativo).

[3] https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

A questo punto il prodotto è pronto per essere firmati digitalmente (a garanzia della sua provenienza ed integrità) per poi essere trasferito in modo sicuro e rilasciato nell'ambiente di test del cliente.

A questo punto sarà responsabilità del cliente seguire le indicazioni di installazione e configurazione sicura suggerite dal fornitore, oltre ad effettuare una verifica di sicurezza prima di metterlo in esercizio.

Nelle attività di manutenzione operativa il cliente dovrà inoltre occuparsi di installare le patch di sicurezza rilasciate dal fornitore e verificare periodicamente che il buon livello di sicurezza iniziale sia sempre garantito; nel caso in cui nelle fasi di monitoraggio venissero rilevate delle problematiche il cliente informerà tempestivamente il fornitore in modo da risolvere rapidamente la vulnerabilità riscontrata.

Conclusioni

Abbiamo visto insieme le implicazioni negative derivanti dalla mancanza di una cultura "Security by Design" applicata all'area dello sviluppo del software di cui si parla da almeno venti anni, ma che sinora è stata poco indirizzata.

I vantaggi della sua applicazione sono sicuramente riconducibili all'adozione di best practices internazionali nel settore Application Security, che una volta acquisite dalle organizzazioni, le contraddistingueranno sotto il profilo qualitativo e rappresenteranno sicuramente un vantaggio competitivo, con la possibilità di dimostrarlo a clienti e prospect creando al tempo stesso del valore aggiunto.

Inoltre costituiranno un passo importante verso la conformità normativa EU e di settore, che rappresenta una grossa preoccupazione per la comunità dei CISO aziendali nei prossimi anni.

Infine l'adozione delle buone prassi sul tema dello sviluppo sicuro del software costituirà indubbiamente un arricchimento delle competenze in capo ai team sviluppatori e di testing.

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phishing***.
Account take-over	Acquisizione illecita di un account al fine di impersonificare la vittima (ad esempio di effettuare transazioni finanziarie sui suoi conti).
ACDC (Advanced Cyber Defence Center)	Progetto europeo la cui finalità è offrire soluzioni e creare conoscenza per aiutare le organizzazioni in tutta Europa a combattere le botnet. (www.acdc-project.eu/).
AISP (Account Information Service Provider)	Prestatori di servizi di informazione sui conti di pagamento che forniscono ai clienti che detengono uno o più conti di pagamento online presso uno o più Istituti di Credito, servizi informativi relativi a saldi o movimenti dei conti aperti.
Analytics-As-A-Service	Servizi on demand per l'analisi di dati utilizzabili anche nell'ambito della sicurezza, ad esempio, per passare al setaccio i dati della rete aziendale e individuare eventi anomali ed eventuali attacchi.
Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	Vulnerabilità che consente ad un attaccante di accedere a file tramite richieste Web remote.
Attacchi Pivot back	Tipo di attacco nel quale viene compromessa una risorsa nel public cloud per ottenere informazioni che possono poi essere usate per attaccare l'ambiente on premise.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
BEC fraud (Business e-mail compromise)	Tipi di attacco phishing mirati verso figure aziendali al fine di convincere le vittime a trasferire somme di denaro o rilevare dati personali. (Vedi anche ***CEO fraud***)

Blocj	Tecnica utilizzata nell'ambito dell'***e-voting***. Con la firma elettronica cieca (blind signature) la preferenza espressa dall'elettore viene cifrata. Successivamente viene apposta la firma elettronica da un ufficiale elettorale, che autentica il voto e infine si ha il deposito nell'urna.
Blockchain	Tecnologia che consente la registrazione di transazioni, in uno scenario trustless, fra gli attori della stessa blockchain mediante l'utilizzo di un registro digitale immodificabile presente su vari nodi della rete, costituito da blocchi (block) fra loro concatenati (chain).
Booter-stresser	Strumenti a pagamento che consentono di scatenare attacchi ***DDOS.***
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo ***DDOS***.
Buffer overflow	Evento che ha luogo quando viene superato il limite di archiviazione predefinito di un'area di memorizzazione temporanea.
CAL (Cybersecurity Assurance Level)	Indicatore dinamico dello sforzo necessario per garanzia la sicurezza di un elemento, derivante dai rischi relativi a tutti i suoi asset.
Captatore informatico	Software che viene immesso in dispositivi elettronici portatili al fine di intercettare comunicazioni o conversazioni tra presenti, il cui uso è specificatamente regolamentato dal Codice Penale.
Carding	Scambio e compravendita di informazioni riguardanti carte di credito, debito o account bancari, che vengono poi utilizzate per eseguire truffe di carattere finanziario acquistando beni o trasferendo fondi ai danni dei legittimi proprietari.
CEO Fraud	Tipi di attacco phishing mirati verso figure aziendali ad altissimo profilo, generalmente amministratori delegati, presidenti dell'azienda, direttori finanziari, etc.

CERT (Computer Emergency Response Team)	Struttura destinata a rispondere agli incidenti informatici e alla rilevazione e contrasto alle minacce. Fra i principali obiettivi di un CERT (vedi CERT Nazionale): - fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini; - incrementare la consapevolezza e la cultura della sicurezza; - cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione; - facilitare la risposta ad incidenti informatici su larga scala; - fornire supporto nel processo di soluzione di crisi cibernetica.
CFC (Cyber Fusion Center)	Approccio olistico e multidisciplinare alla gestione della sicurezza che mira a superare la tradizionale suddivisione fra compiti (intelligence, analisi, risposta…) e team.
CLOSINT (Close Source Intelligence)	Processo di raccolta di informazioni attraverso la consultazione di fonti chiuse, cioè non accessibili pubblicamente: intelligence feed, fonti governative, informazioni classificate, etc.
Cloud weaponization	Tipo di attacco nel quale l'attaccante ottiene un primo punto d'ingresso nell'infrastruttura cloud attraverso la compromissione e il controllo di alcune machine virtuali. L'attaccante utilizza poi questi sistemi per attaccare, compromettere e controllare migliaia di altre macchine, incluse altre appartenenti allo stesso service provider cloud dell'attacco iniziale, e altre appartenenti ad altri service provider pubblici.
CNOs (Computer Network Operations)	Tipologia di ***Information warfare*** finalizzato all'attacco e distruzioni delle informazioni presenti sui sistemi informativi avversari, alla distruzione delle reti e dei sistemi stessi e alla difesa delle proprie.
CNP (Card-Not-Present)	Indica un pagamento effettuato senza la presenza fisica di una carta di pagamento, ad esempio su Internet.
CoA (Courses of Action)	Nella dottrina militare identifica un piano che descrive le strategie e le azioni operative scelte per portare a termine una determinata missione. Nell'ambito della ***Cyber Intelligence*** rappresenta le attività poste in essere rispettivamente dagli attaccanti o dai difensori per la conduzione o il contrasto delle azioni funzionali ad un attacco cyber.

Constituency	Nell'ambito di un ***CERT*** indica a chi è rivolto il servizio (ad esempio Pubblica Amministrazione Centrale, Regioni e Città metropolitane).
Context-based access	Tecnica che condiziona l'accesso alla valutazione dinamica del rischio della singola transazione, modulando eventuali azioni aggiuntive di verifica. Ad esempio le soluzioni di autenticazione e autorizzazione, sia nel caso di login che di disposizione di operazioni, non si limitano più ad autorizzare o bloccare un'operazione, ma offrono una gamma intermedia di possibilità, come ad esempio autorizzare un'operazione, ma con dei limiti, oppure richiedere verifiche aggiuntive.
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.
Counterintelligence	Identificazione, valutazione, neutralizzazione e sfruttamento delle attività di intelligence svolte da entità avversarie.
Course of action matrix	Metodologia per l'identificazione, la prioritizzazione e la rappresentazione sinottica delle azioni da intraprendere, in caso di possibili intrusioni. È composta da: - due azioni passive: Discover e Detect - cinque attive - *Deny*, *Disrupt*, *Degrade*, *Deceive*, *Destroy*).
Credential Stuffing	Attacco nel quale vengono utilizzate coppie di user id/password raccolte in precedenza in modo fraudolento.
Cryptojacking	Processo che sfrutta illegalmente le risorse informatiche di una vittima per generare criptovaluta. In sostanza gli aggressori sottraggono potenza di calcolo installando un'applicazione di mining di criptovaluta sul sistema della vittima, che sia un PC o uno smartphone. La generazione di valuta virtuale, nota anche come criptovaluta, è molto dispendiosa in termini di potenza di elaborazione, motivo per cui gli aggressori devono infettare un vasto numero di vittime e utilizzarne la potenza di calcolo per generare nuove unità monetarie virtuali.

Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
CTW (Check-the-Web)	Piattaforma tecnologiche appositamente creata in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet, il cui ruolo principale è di anticipare e prevenire l'abuso terroristico di strumenti online, nonché di svolgere un ruolo consultivo proattivo a tale riguardo nei confronti degli Stati membri dell'UE e del settore privato.
CVSS versione 3 (Common Vulnerability Scoring System)	Sistema di valutazione delle vulnerabilità che fornisce un modo per acquisire le principali caratteristiche di una vulnerabilità e per produrre un punteggio numerico che rifletta la sua gravità, nonché una rappresentazione testuale di tale punteggio. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. (*https://www.first.org/cvss/specification-document*)
CSIRT (Computer Security Incident Response Team)	Struttura sostanzialmente simile ad un ***CERT.***
CTI (Cyber Threat Intelligence)	Disciplina che si occupa di raccogliere e analizzare dati eterogenei - provenienti da diverse sorgenti informative interne ed esterne -per estrarre informazioni utili a conoscere le caratteristiche dell'attore della minaccia, in modo da poter attribuire un profilo di rischio specifico per i propri asset e sviluppare azioni di contrasto efficaci. In particolare, le attività di CTI si esplicano attraverso un processo di raccolta, classificazione, integrazione e analisi di dati grezzi relativi a minacce che operano nel cyberspazio.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.

Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cyber Kill Chain	La cyber kill chain è un modello definito dagli analisti di Lockheed Martin come supporto decisionale rispetto alla rilevazione e risposta alle minacce. Esso include le seguenti fasi: reconnaissance, weaponization, delivery, exploitation, installation and persistence, command and control (C2), actions.
Cybersquatting	Attività volta ad appropriarsi di nomi di dominio di terzi, in particolare di marchi commerciali di rilievo, al fine di trarne profitto.
Cyber resilience	Capacità di un'organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Cyber-reasoning systems	Sistemi sviluppati per individuare automaticamente le vulnerabilità delle reti più complesse implementando algoritmi cognitivi.
Cyber-weapon	***Malware*** (o anche hardware) progettato o utilizzato per causare danni attraverso il dominio cyber. *(NATO Cooperative Cyber Defence Centre of Excellence).*
CYBINT (Cyber Intelligence)	Disciplina che trae origine dalla declinazione classica delle attività di intelligence con riferimento alle peculiarità del dominio di ricerca informativa in ambito cyber. L'attività CYBINT si evolve includendo attività di analisi strategica e analisi di contesto su trend di eventi, scenari geopolitici e previsionali.
Data Leakage	Trasferimento non autorizzato di informazioni riservate.
DDoS (Distributed Denial of Service)	Attacchi ***DOS*** distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DDoS-for-hire	Letteralmente servizio DDoS da noleggiare.
Deep Fake	Algoritmi di deep learning in grado di creare foto o video falsi.
Deep Web	L'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (Google, Bing…).
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.

DES (Data Encryption Standard)	Algoritmo per la cifratura dei dati a chiave simmetrica.
DGA (Domain generation algorithms)	Algoritmo utilizzato da alcuni ***malware*** per la generazione di migliaia di nomi di dominio alcuni dei quali sono utilizzati dai loro server ***C&C***.
Diamond Model	Framework strutturato per l'analisi tecnica di possibili intrusioni. *(Adversary, Infrastructure, Victim, Capability).*
Digital Scarcity	In una ***blockchain*** la capacità di rendere non riproducibili informazioni digitali come file o pagamenti.
DMARC (Domain-based Message Authentication, Reporting and Conformance)	Standard di autenticazione delle e-mail che aiuta a prevenire la falsificazione del mittente (spoofing) e il phishing.
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS cache poisoning	Tipo di attacco nel quale l'attaccante inserisce corrispondenze Indirizzo-IP alterate all'interno della cache del meccanismo di risoluzione degli indirizzi IP. Come risultato la cache userà l'indirizzo IP alterato in tutte le successive transazioni. L'indirizzo che comparirà nella barra URL di un browser sarà quello corretto e desiderato, ma il corrispondente indirizzo IP utilizzato sarà quello alterato e tutto il traffico di rete sarà quindi reindirizzato verso il sito replica controllato dai cyber criminali e nel quale si simulano log in per tracciare tutti i fattori di autenticazione inseriti.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.
DNSSEC (Domain Name System Security Extensions)	Insieme di specifiche per garantire alcuni aspetti di sicurezza delle informazioni fornite dai ***DNS.***

Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti); • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di ***C&C*** si parla di ***DDOS*** (Destribuited Denial of Service).
Double extortion	Attacchi ransomware che, oltre a cifrare i file, ne fanno anche una copia di "sicurezza" con il loro trasferimento sui computer dei cyber criminali minacciando di procedere alla loro diffusione pubblica e/o metterli all'asta nel dark web per la vendita al miglior offerente.
Downloader	Software deputati a scaricare ulteriori componenti malevoli dopo l'infezione iniziale.
Drive-by exploit kit	Il fenomeno dei drive-by ***exploit kit*** è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli ***exploit kit***, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole anche in assenza di interazione dell'utente con la pagina.
DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di ***DDOS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.
Dropper	Codice che installa il ***malware*** sul computer della vittima.
Eavesdropping	Nell'ambito VOIP è un attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni

EDR (Endpoint Detection and Response)	Dispositivi la cui finalità è quella di mantenere un costante monitoraggio di eventi sospetti al fine di garantire una reazione preventiva e continua alle minacce.
Enterprise Architecture	Sistema informativo che, raccogliendo dati da tutte le funzioni dell'organizzazione, li collega in un unico modello informativo consentendo di visualizzare complessivamente lo stato dell'organizzazione e contemporaneamente di immaginarne la possibile evoluzione futura, rinforzandone la capacità di reagire ad eventi esterni.
Evasion	Nell'ambito delle applicazioni di IA attacco che consiste nel confondere la classificazione del dato in ingresso, da parte di un algoritmo precedentemente addestrato, manipolandone il contenuto.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
FIDO2	Meccanismo di autenticazione avanzata che standardizza l'uso dei dispositivi di autenticazione per l'accesso ai servizi online, sia in ambiente mobile che desktop.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
Ghost broking	Pratica secondo la quale il frodatore, spacciandosi per agente di un'impresa assicurativa, a seguito del pagamento di un "premio" rilascia al cliente una polizza assicurativa, ovviamente falsa.
GRE (Generic Routing Encapsulation)	Protocollo di tunneling che incapsula vari protocolli di livello rete all'interno collegamenti virtuali point-to-point.

Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Hate speech	Il Comitato dei ministri del Consiglio d'Europa definisce gli hate speech come le forme di espressioni che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o più in generale l'intolleranza, ma anche i nazionalismi e gli etnocentrismi, gli abusi e le molestie, gli epiteti, i pregiudizi, gli stereotipi e le ingiurie che stigmatizzano e insultano. RECOMMENDATION No. R (97) 20 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON "HATE SPEECH" - Adopted by the Committee of Ministers on 30 October 1997
Hit & Run (o Pulse wave)	Attacchi di breve durata, ma frequenti nell'arco di poche ore.
HMI (Human Machine Interface Systems)	Componente fondamentale dei sistemi IT industriali, che permette all'operatore umano di interagire con gli ambienti di controllo, supervisione e acquisizione dati (supervisory control and data acquisition - SCADA).
Honeypot	Letteralmente barattolo del miele. Indica un asset esca isolato verso cui indirizzare e raccogliere informazioni su eventuali attacchi, al fine di tutelare il reale sistema informativo.
HTTP POST DoS Attack	Attacco che sfrutta un difetto di progettazione di molti server web. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght'. Visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad una ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.
HUMINT (HUMan INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione. (*Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it*)

Kill Switch	Termine generico per indicare un dispositivo che serve a bloccare in modo forzato un'attività.
IBAN Swapping	Sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
ICMP (Internet Control Message Protocol)	Protocolli che consentono ai dispositivi di una rete di comunicare informazioni di controllo e messaggi.
ICS (Industrial Control System)	Sistemi di controllo industriale.
IDS (Intrusion detection system)	Dispositivo in grado di identificare modelli riconducibili a possibili attacchi alla rete o ai sistemi.
IGA (Identity Governance & Administration)	Strumento di governance ed amministrazione delle identità che aiuta a garantire un provisioning, un re-provisioning ed un deprovisioning accurato dell'accesso degli utenti.
IMEI (International Mobile Equipment Identity)	Codice univoco che identifica un terminale mobile
IMSI (International Mobile Subscriber Identity)	Codice univoco internazionale che combina SIM, nazione ed operatore telefonico.
Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…
Infostealer	***Malware*** finalizzato a sottrarre informazioni, quali ad esempio credenziali, dal dispositivo infetto.
Instant phishing	Tecnica di attacco nella quale nell'istante in cui l'utente inserisce le credenziali, o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi in real time, queste informazioni per effettuare azioni dispositive.

Interception and Modification	Nell'ambito VOIP intercettazione di comunicazioni lecite tra utenti ed alterazione delle stesse con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
Intrusion software	***Spyware*** (definizione della Commissione Europea nell'ambito della regolamentazione dell'esportazione di prodotti ***dual use***). Un "intrusion software", ad esempio, può essere utilizzato da una società di security per testare la sicurezza di un sistema informatico e al contempo essere usato da uno Stato non democratico per controllare e intercettare le conversazioni dei propri cittadini.
IoA (Indicatori di attacco)	Informazioni funzionali all'individuazione di un potenziale attacco anche prima che ci sia contatto diretto tra attaccante e attaccato.
IoC (Indicatori di compromissione)	Qualsiasi informazione che possa essere utilizzata per cercare o identificare sistemi potenzialmente compromessi (indirizzo IP/nome dominio, URL, file hash, indirizzo email, X-Mailer…) (Common Framework for Artifact Analysis Activities – ENISA)
IP Fragmentation	Tipo di attacco ***DDOS*** (Destribuited Denial of Service) che sfrutta il principio di frammentazione del protocollo IP.
IPMI (Intelligent Platform Management Interface)	Specifica di una interfaccia di basso livello utilizzata da diversi costruttori che consente ad un amministratore di sistema di gestire server a livello hardware. Attraverso la BMC (Baseboard Management Controller) consente, tra le altre cose, l'accesso al BIOS, ai dischi ed ai dispositivi hardware in generale e, di fatto, il controllo del server. IPMI contiene una serie di vulnerabilità ampiamente descritte e conosciute e, in definitiva, non dovrebbe essere aperto all'esterno.
IPS (Intrusion prevention system)	Dispositivo in grado non solo di identificare possibili attacchi, ma anche di prevenirli.
Jamming	Interferenza intenzionale o volontaria di un segnale elettromagnetico al fine di disturbare, bloccare o impedire la ricezione corretta del segnale da parte dei dispositivi destinatari.

LOTL (Living Off The Land)	Tipo di attacco basato su strumenti nativi preinstallati nel sistema operativo.
MAAS (Malware as a Service)	Modello di erogazione del codice malevole dove un team di esperti "produce" malware, sviluppa exploits e si occupa della loro ricerca e sviluppo, mentre una catena di distributori si occupa di procacciare i clienti.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di una banca, al fine di poterle riutilizzare.
Meaconing	Interferenza con i segnali di navigazione, come quelli provenienti dai sistemi GPS, al fine di alterare le informazioni di posizione e indirizzare in modo errato i dispositivi di navigazione o di localizzazione.
Memcached	Software spesso usato sui server web per effettuare caching di dati e per diminuire il traffico sul database o sul backend. Il server memcached è pensato per non essere esposto direttamente su Internet, per questo nella sua configurazione di default non richiede autenticazione e risponde sia via TCP che via UDP.
MFA (Multi-Factor Authentication)	Autenticazione a più fattori, nella quale si combinano più elementi di autenticazione per rendere più complessa la compromissione del sistema.
MFU (Malicious File Upload)	Attacco ad un web server basato sul caricamento remoto di ***malware*** o più semplicemente di file di grandi dimensioni.
Mining	Creazione di nuova criptovaluta attraverso la potenza di calcolo degli elaboratori di una ***blockchain***.
MitC (Man in the Cloud) *Definizione coniata dall'azienda Imperva*	Tipo di attacco nel quale la potenziale vittima è indotta a installare del software malevolo attraverso meccanismi classici come l'invio di una mail contenente un link a un sito malevolo. Successivamente il malware viene scaricato, installato, e ricerca una cartella per la memorizzazione di dati nel cloud sul sistema dell'utente. Successivamente, il malware sostituisce il token di sincronizzazione dell'utente con quello dell'attaccante.

Mules	Soggetti che consentono di "convertire" attività illegali in denaro (cash out) ad esempio attraverso attività di riciclaggio.
NTP (Network Time Protocol)	***Protocollo*** che consente la sincronizzazione degli orologi dei dispositivi connessi ad una rete.
OF2CEN (On line Fraud Cyber Centre and Expert Network)	Piattaforma in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. "Eu-of2cen" (European Union Online Fraud Cyber Centre Expert Network) è il progetto ideato dalla Polizia di Stato, gestito dalla Polizia postale e delle comunicazioni, e finanziato dall'Unione europea per il contrasto al cybercrime finanziario. (*https://www.poliziadistato.it*)
OPSEC (Operation Security)	Processo mediante il quale, durante un'operazione di intelligence, si previene l'esposizione involontaria di informazioni sensibili/riservate/classificate riguardanti le proprie attività, intenzioni o capacità.
Oracoli	Fonti esterne (API di un sito, output di un oggetto IoT…) alla ***blockchain*** per alimentare uno smart contract e scatenarne o influenzarne l'esecuzione.
OSINT (Open Source INTelligence)	Attività di intelligence tramite la consultazione di fonti aperte di pubblico accesso.
OT (Operation Technology)	Componenti hardware e software dedicati al monitoraggio ed alla gestione di asset fisici in ambito industriale, trasporti…
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.

PHI (Protected Health Information)	Informazioni personali relative alla salute fisica o mentale di una persona fisica, comprese le relative valutazioni, cure… ed i relativi pagamenti, indipendentemente dalla forma o dal media utilizzato per la loro rappresentazione.
Phishing	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.
Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Ping flood	Attacco basato sul continuo ping dell'indirizzo della macchina vittima. Se migliaia e migliaia di computer, che fanno parte di una ***botnet***, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
Ping of Death	Attacco basato sull'inoltro di un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
PIR (Priority Intelligence Requirements)	Requisiti informativi che orientano le priorità nella pianificazione delle attività di intelligence.
Plausible Deniability	Capacità di un soggetto, in genere in posizione gerarchica elevata, di negare di essere a conoscenza di azioni dannose commesse da soggetti di livello più basso, in assenza di prove che possano dimostrare il contrario.
Poisoning	Nell'ambito delle applicazioni di IA attacco che consiste nel contaminare i dati di addestramento per impedire al sistema di funzionare correttamente.
Port Sweeping	Scansione di vari sistemi alla ricerca di una specifica porta in ascolto.
PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. (*Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it*)
Pulse wave (o Hit & Run)	vedi Hit & Run

QTSP (Qualified Trust Service Provider)	Un ***prestatore di servizi fiduciari*** che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.
Ransomware	***Malware*** che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati (crypto-ransomware), o impedendo l'accesso al dispositivo (locker-ransomware).
RDP (Remote Desktop Protocol)	Protocollo per la comunicazione remota fra computer (in particolare per le comunicazioni tra Terminal Server e il client Terminal Server).
Resilienza	"La capacità di un'organizzazione di assorbire gli shock e di adattarsi ad un contesto in continua evoluzione". Definizione da ISO 22316:2017
Resource ransom	Tecnica di attacco che nel mondo cloud consiste nel tentare di bloccare l'accesso a risorse nel cloud compromettendo l'account cloud pubblico della vittima e tentando di cifrare o limitare in altro modo l'accesso al maggior numero possibile di risorse cloud.
Retrieving data	Fase di ricerca e raccolta dei dati relativi all'obiettivo individuato durante un'attività ***OSINT***. In questa fase gli analisti sfruttano i motori di ricerca, scandagliano i siti web alla ricerca di documenti di interesse avendo cura di conservare ogni traccia raccolta come ad esempio testi, URL, video, immagini, documenti, etc.
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
SAST (Static Application Security Testing)	Analisi statica del codice finalizzata alla individuazione di vulnerabilità.
SBOM (Software Bill of Materials)	Inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda.

Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.
Security Architecture *(NIST)*	Insieme di rappresentazioni logiche e fisiche di un'architettura di sistema rilevanti dal punto di vista della sicurezza, che raccoglie le informazioni su come il complessivo sistema sia organizzato in domini di sicurezza, e ne fa uso per rinforzare le policy che prescrivono come dati ed informazioni debbano essere protetti all'interno di un dominio di sicurezza e nelle relazioni tra i domini.
Service Abuse	Tecniche di attacco in ambito VOIP in cui si utilizza l'infrastruttura della rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
Side-channel attacks	Tecnica di attacco nella quale l'attaccante tenta di posizionare una macchina virtuale sullo stesso server fisico della potenziale vittima.
SIEM (Security information & event management)	Sistema per la raccolta e normalizzazione dei log e per la correlazione degli eventi finalizzato al monitoraggio della sicurezza.
SIGINT (SIGnals INTelligence)	Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la COMINT e la ELINT. (Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)
Sinkhole	Tecnica per reindirizzare il traffico di rete verso uno specifico server al fine, ad esempio, di analizzarlo.
SMB (Server Message Block)	Protocollo per la condivisione di file e stampanti nelle reti locali. Se esposto su internet può essere utilizzato per accedere a documenti e file condivisi.
Smoking Guns	Termine che indica una prova (quasi) certa dell'aver commesso un crimine.

SOAR (Security Orchestration Automation and Response)	Approccio che consente di orchestrare le tecnologie di sicurezza al fine di avere una gestione il più possibile automatizzata della raccolta, analisi e risposta agli eventi di sicurezza.
SOC (Security Operations Center)	Centro la gestione delle funzionalità di sicurezza e per il monitoraggio degli eventi che potrebbero essere una fonte di minaccia.
Social Threats	Versione VOIP del furto d'identità finalizzata a impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni; ad esempio, furto di informazioni aziendali riservate.
SOCMINT (Social Media Intelligence)	Ramo dell'Open Source Intelligence specificatamente dedicato alla raccolta di informazione attraverso i social network.
SOP (Standard Operating Procedure)	Procedure operative standard che indicano i passi da seguire durante la conduzione di indagini ***OSINT***, consentendo di rendere efficiente l'esecuzione di operazioni ripetitive e di ottenere uniformità nelle prestazioni, nella qualità degli output ed evitando il mancato rispetto di standard e normative di settore, eventualmente imposte dalla propria organizzazione.
Spear phishing	***Phishing*** mirato verso specifici soggetti.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
SQL injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDLC (Secure Software Development Life Cycle)	Programma che indirizza la sicurezza sin dalle prime fasi di progettazione di un'applicazione software e non si conclude con la fase di delivery, ma segue tutto il ciclo di vita dell'applicazione.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.

SSH (Secure Shell)	***Protocollo*** cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo ***TAXII.***
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.
TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante ***STIX***.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.

Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come ***prestatore di servizi fiduciari qualificato*** o come prestatore di servizi fiduciari non qualificato.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
UDP Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	***Protocollo*** di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.

VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.
Vetting	Il processo di identificazione dei partecipanti 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.
Whaling	Letteralmente "caccia alla balena"; è un'ulteriore specializzazione dello ***spearphishing*** che consiste nel contattare una persona interna all'azienda spacciandosi per un dirigente della stessa. Di solito si tratta di truffe finanziarie e il bersaglio è l'amministrazione con l'obiettivo di indurre la vittima a eseguire, con l'inganno, un pagamento a beneficio del truffatore.
Wiper	Tipologia di virus che hanno come unico scopo quello di distruggere il sistema target (IT e OT).
XDR (Extended Detection and Response)	Dispositivi che integrano tutte le componenti della soluzione di sicurezza in un'unica piattaforma di individuazione (detection) e risposta agli incidenti (Incident Response) portando l'intelligenza di protezione fino al terminale del dipendente, sia esso un computer o uno smartphone.

XSS (Cross Site Scripting)	Vulnerabilità che sfrutta il limitato controllo nell'input di un form su un sito web mediante l'uso di qualsiasi linguaggio di scripting.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.
Zero Trust	Paradigma i cui principi fondamentali sono: si assuma che l'ambiente sia ostile, non si distingua tra utenti interni ed esterni, non si assuma "trust" (da cui il nome), si eroghino applicazioni solo a device e utenti riconosciuti e autenticati, si effettuino analisi dei log e dei comportamenti utente. In pratica occorre trattare tutti gli utenti nello stesso modo, utenti della stessa azienda o esterni, che siano nel perimetro della rete aziendale o meno, che i dati a cui vogliono accedere siano dentro l'azienda o da qualche parte nel cloud.
Zoom bombing	Irruzione virtuale in una videoconferenza finalizzata a creare disturbo.

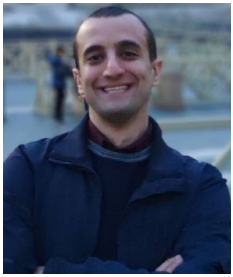
Gli autori del Rapporto Clusit 2024

Claude Bazzucchi, Sr. Project manager e PMO Team leader per area International del Professional Services di RSA, inizia la sua carriera 27 anni fa, prima come consulente tecnico poi con ruoli manageriali, sempre nei servizi professionali, a continuo contatto con i clienti. Col passare degli anni si è sempre più focalizzato su progetti di sicurezza, principalmente Identity governance e Access control, lavorando in tutti settori dell'industria privata e nella pubblica amministrazione. Gli ultimi 4 anni in RSA lo hanno portato a focalizzarsi unicamente su queste tematiche, aiutando i clienti a trarre massimo beneficio dalla tecnologia RSA.

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

Elio Biasiotto, ricopre il ruolo di Senior Consultant in Cisco Talos, dove si occupa di Incident Response e Threat Intelligence. Ha maturato esperienza nella gestione di incidenti informatici in Italia e in organizzazioni multinazionali, specializzandosi in Digital Forensics e Malware Analysis. Nato in Veneto, risiede attualmente in Olanda dove collabora in ambito di Cyber Threat Intelligence in conferenze e gruppi di studio locali come autore di articoli o speaker.

Appassionato del proprio lavoro, svolge anche attività di sensibilizzazione sul tema della sicurezza e della privacy.



Mario Boemi, ha conseguito la Laurea Magistrale in Informatica presso l'Università degli Studi di Messina nel 2012. Vanta un'esperienza di circa 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.

Roberto Branz, Channel Executive Manager per RSA Italia, si occupa di Cyber Security dai primi anni 2000, ha maturato l'esperienza presso il distributore Computerlinks, poi diventato Arrow, come Brand Manager prima e responsabile della divisione Security in seguito. Da sempre attento alle nuove sfide che i partner dell'IT security italiana devono affrontare ha un'ampia esperienza del canale dei più importanti brand del panorama Cyber Security. Nel suo attuale lavoro da molta enfasi alla semplificazione nelle comunicazioni verso il mercato dei temi della sicurezza informatica e del valore strategico che la sicurezza informatica ha nel favorire business e i servizi delle varie organizzazioni. Recentemente il lavoro in RSA gli ha permesso di focalizzarsi sul mattone fondamentale di ogni procedura informatica ovvero l'identità digitale.

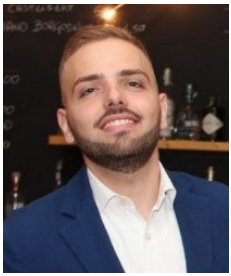
Giancarlo Butti, ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Referente ESG(*) e Inclusion del Comitato Scientifico del CLUSIT. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 150 corsi e seminari tenuti presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, 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 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 25 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT e del BCI. Partecipa a numerosi gruppi di lavoro. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

(*) Già ricercatore nell'ambito delle energie rinnovabili (UNESCO - International directory of new and renewable energy information sources and research centers, 1986).

Carmelo Califano, in Cisco dal 2001, attualmente ricopre il ruolo di Designated Service Manager, con un focus particolare su Email Security, a supporto dei clienti che adottano la soluzione. In passato ha progettato, messo in opera e fornito consulenza su sistemi distribuiti DNS, AAA e DHCP a numerosi Service Provider in EMEA. Laureato in Ingegneria Elettronica presso l'Università degli Studi di Napoli "Federico II", nel 2023 ha conseguito un Master in Cybersecurity presso la Graduate School of Management (GSoM) del Politecnico di Milano. Collabora con Clusit al progetto "SicuraMente Clusit" per sensibilizzare gli studenti sui rischi derivanti dalle minacce informatiche.

Davide Costanigro, è Solution Architect nella divisione Aruba di Hewlett Packard Enterprise in Italia. Dal 2021 è focalizzato nello sviluppo delle tecnologie SD-WAN ed SSE nell'ambito delle architetture SASE per il mercato Italiano e Israeliano. Dopo aver concluso gli studi di Ingegneria nel 1999, frequenta un Master in Telecomunicazioni e nel 2000 comincia il proprio percorso professionale nell'ambito delle tecnologie di networking in diverse aziende, nelle quali ricopre ruoli presales in ambito networking per i mercati SMB, enterprise e settore pubblico. Nel 2015 entra a far parte di HPE Aruba ricoprendo il ruolo di Channel Systems Engineer per poi spostarsi nell'attuale posizione lavorativa.

Martina D'Agnolo, da sempre affascinata dal mondo dell'informatica, ha conseguito la laurea in Economics Management and Computer Science presso l'Università Bocconi e sta perfezionando la sua formazione con la Laurea Magistrale in Cyber Risk, Strategy and Governance. Attualmente, riveste il ruolo di Cyber Security Professional presso il CSIRT di Fastweb, dove mette in pratica le sue competenze multidisciplinari.



Francesco De Feo, è un esperto Cyber Threat Analyst con una passione per l'informatica fin dall'infanzia. Ha conseguito la laurea triennale in Informatica e il master in Cyber Security con lode nel 2020. Con oltre 4 anni di esperienza lavorativa, principalmente in Security Operations Center (SOC), ha sviluppato una competenza completa nel riconoscimento e nella gestione delle minacce digitali, acquisendo esperienza su diverse piattaforme SIEM ed EDR. Attualmente, lavora presso NTT DATA, dedicandosi all'Incident Response e alla Threat Intelligence.

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.

Alessandro Ercoli, ricopre il ruolo di Manager del team dei System Engineer in HPE Aruba Italia. Ha una lunga esperienza in HPE, in ambito networking, dove ha ricoperto diversi ruoli. Esperto in soluzioni di Infrastrutture di accesso Unified Wired&Wireless e di quelle per il Data Center. Completano il suo profilo, le competenze in ambito SASE, SD-WAN e Cloud Based solution.

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

Ivano Gabrielli, laureato in Giurisprudenza e Scienze Politiche con il massimo dei voti, master in Scienze della Sicurezza e master in Homeland Security, è nella Specialità Polizia Postale e delle Comunicazioni dal 2006. Dopo 3 anni in forza al Compartimento Polizia Postale e delle Comunicazioni di Genova, dal 2009 è al Servizio Polizia Postale del Dipartimento della PS. Dal maggio 2012 ha ricoperto l'incarico di Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Dal luglio 2017 è nominato Direttore della III Divisione del Servizio Polizia Postale e delle Comunicazioni, a cui fanno riferimento il Centro Nazionale Anticrimine Informatico

per la Protezione delle Infrastrutture Critiche – CNAIPIC, la Sezione Cyber Terrorismo e la Sezione per il contrasto al Financial Cyber Crime. Dal gennaio 2022 è Direttore del Servizio Polizia Postale e delle Comunicazioni.

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 ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi, membro del Comitato Direttivo di Clusit, è fondatore e senior partner di Rexilience. Già esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale/CERT-AGID (2015-2020) con la responsabilità dello sviluppo del CERT della Pubblica Amministrazione, già membro (mandati 2010-12, 2012-15, 2015-17 e 2017-20) dell'Advisory Board dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA). In oltre trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di audit e assessment, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Ha collaborato per oltre venti anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo. Ha partecipato a progetti internazionali di contrasto alla cybercriminalità e al cyberterrorismo con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). È docente in numerosi Master Universitari. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri. L'Università di Roma Tor Vergata gli ha conferito la laurea magistrale honoris causa in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.

Pier Paolo Glave, laureato in Ingegneria Elettronica con indirizzo Reti di Telecomunicazioni al Politecnico di Milano, ha lavorato come Software Engineer e Architect nei settori delle telecomunicazioni e della TV digitale, collaborando con Italtel, Ericsson, Pirelli e Sky Italia. Si occupa di cybersecurity dal 2017, lavorando nel gruppo di Customer Success in Cisco. In questo ruolo, ha aiutato più di 100 grandi aziende in Italia e nel Sud Europa a migliorare la sicurezza delle loro infrastrutture, utilizzando e configurando al meglio soluzioni di protezione come firewall, network access control, EDR, XDR, sistemi di analisi di rete. Detiene certificazioni sulla sicurezza informatica, tra cui CISSP, CISM, CCNP, ITIL. A titolo volontario ha collaborato con le scuole del territorio, per migliorare la sicurezza e la consapevolezza nell'uso di internet, insieme a Cisco e Telefono Azzurro. Dal 2023 è docente del corso di sicurezza informatica presso la UTE di Lainate.

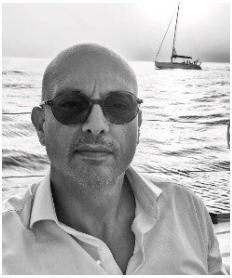
Serena Angela Gracco, laureata in Ingegneria Informatica con lode, ha consolidato la sua carriera nel campo della sicurezza informatica presso NTT Data, dove è entrata a far parte nel 2022. Attualmente riveste il ruolo di Cyber Threat Analyst nel Security Operations Center (SOC), dove si occupa inoltre di Threat Intelligence. La sua attività quotidiana nel SOC implica il monitoraggio e l'analisi delle potenziali minacce alla sicurezza informatica, contribuendo attivamente alla difesa proattiva delle reti e dei sistemi aziendali e maturando così esperienza nell'utilizzo di molteplici SIEM ed EDR.

Alberto Greco, è SE di CrowdStrike per l'Italia. L'inizio in CrowdStrike avviene nel gennaio 2022 con lo scopo di seguire il team dedicato al mercato enterprise e mid-market; il suo ruolo è agire da punto di congiunzione tra le esigenze di business dei clienti e le soluzioni tecnologiche di CrowdStrike: dall'endpoint al cloud, dal mondo identity alla threat intelligence, dall'XDR all'IT Operations. In passato è stato SE Enterprise per l'intero portfolio Palo Alto Networks, SE in Forcepoint con focus sulla network security, technical trainer Fortinet in Exclusive Networks e, prima ancora, network security specialist in Thales Alenia Space. Convinto sostenitore della frase "Se non lo sai spiegare in modo semplice, non l'hai capito abbastanza bene", Alberto è convinto che una diffusione della

cultura CyberSec ad ogni livello sia fondamentale per una piena consapevolezza delle problematiche e, ancor più, delle opportunità che ne derivano.

Jari Iannucci, laureato in Ingegneria delle Nanotecnologie con lode, vanta esperienze di ricerca sia in Spagna che in Inghilterra, consolidando così la sua capacità di operare in ambienti internazionali. Grazie al suo percorso lavorativo all'estero e al conseguimento del certificato IELTS, parla fluentemente l'inglese. Attualmente, all'interno del SOC di NTT Data, si occupa con competenza di Threat Detection e Threat Intelligence. Attraverso un cammino eterogeneo che lo ha portato a immergersi nel settore dell'informatica, ha acquisito una mentalità flessibile e adattabile, in grado di affrontare con successo varie sfide e situazioni.

Sergio Inglima Modica, ha conseguito la Laurea Magistrale in Informatica presso l'Università degli Studi di Palermo nel 2016. Da sempre appassionato di Sicurezza Informatica, oggi ricopre il ruolo di Technical Analyst e Cyber Security Professional presso il gruppo CSIRT di Fastweb. 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.



Vincenzo Iucci, Senior Director NTT DATA. Laureatosi in Ingegneria Elettronica dopo ardenti studi classici, Vincenzo ha scoperto la passione per la sicurezza informatica nel corso di uno stage e l'ha resa il filo rosso del proprio percorso professionale. In NTT DATA dal 2007, si è occupato dapprima di delivery tecnologica in diversi domini cyber per poi spostarsi gradualmente verso temi più architetturali con focus sulla protezione dei dati e del cloud. Oggi è responsabile della practice di Cybersecurity Architectures & Engineering.

Luca Lazzari, è Presales Manager in HP Italy dove lavora da 25 anni. Dopo 3 anni di consulenza IT per una software house di Bergamo ha iniziato il suo percorso in HP come Support Engineer per diventare poi Service Delivery Manager e dal 2010 lavora in ambito office printing come Presales Technical Consultant con focus sui temi di Security e Sustainability. Da circa un anno ricopre il ruolo di Presales Manager dei team printing and computing.

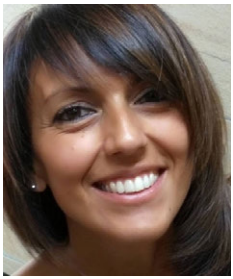
Federica Maria Rita Livelli, Certificata in Risk Management (FERMA/RIMAP certificazioni Iso 3100:2018) & Business Continuity (AMBCI Certification – BCI UK; CBCP Certification – DRI Usa), svolge consulenze in Risk Management & Business Continuity, oltre a effettuare un'attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni e università italiane e straniere. Ricopre il ruolo di Academy Training Director presso BEDISRUPTIVE CONSULTING Srl. È membro del BCI Cyber Resilience Group e del Comitato Direttivo e Scientifico di ANRA; del Comitato scientifico di CLUSIT, FERMA Digital Committee, 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 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.

Giuseppe Massa, rappresenta la Cybersecurity Governance di Cisco in Italia, come National Cybersecurity Officer ed è responsabile dei programmi di collaborazione, in ambito cyber, con ACN ed ENISA, con i Clienti Strategici e della Difesa. Laureato in Ingegneria Elettronica al Politecnico di Torino e specializzato in Telecomunicazioni, dopo un'esperienza da ricercatore sulle tecnologie xDSL e alcuni anni in Ericsson, è entrato in Cisco nel 1999. Ha ricoperto diversi ruoli nei gruppi tecnici di progettazione e prevendita in Cisco Italia e come manager in Cisco Olanda. È stato responsabile del primo progetto di Telefonia IP realizzato da Cisco in Italia nel 2000 e ha seguito la progettazione di oltre 600 reti e sistemi di telecomunicazione in Italia, Europa e Asia. Dal 2012 è specialista in Cybersecurity e nel corso della sua carriera ha conseguito diverse certificazioni tecniche, tra cui CISSP, ITIL, CCSP, CMNA.

Marco Mereghetti, classe '77, è Solution Manager di 7Layers, azienda specializzata in Cyber sicurezza. Segue in modo trasversale i diversi ambiti del settore e le sue evoluzioni, sempre più orientate alle tecnologie di IA. Nel corso della carriera, ha maturato un'esperienza di 18 anni in una società fashion multinazionale, diventando responsabile dell'area Network & Telco della Corporate. Ha preso parte, all'interno del team dedicato, ai progetti di evoluzione tecnologica di IT security, a stretto contatto con i partner tecnologici e gli integratori. In precedenza, la lavorato 5 anni per Italtel S.p.A., nel settore ICT, sviluppando competenze sistemistiche in diversi contesti tecnologici dell'infrastruttura IT, con un focus sui Firewall/IPS e le reti Cisco.



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.

Giovanni Napoli, è Presales Director per EMEA and APJ in RSA. Ha conseguito la Laurea in Scienze dell'Informazione nel 1994 presso l'Universita' Statale di Milano ed è certificato CISSP dal 2008. Con ormai 30 anni di esperienza in ambito IT e Cybersecurity ha lavorato per importanti Aziende del settore. Da circa 18 anni in RSA, dove ha potuto approfondire ancora più da vicino tematiche di antifrode, di threat detection and response, di governance risk and compliance e di identity, con lo scopo di poter servire al meglio i progetti dei propri clienti e partner. Ha una lunga esperienza di presales management e di hiring con una forte attenzione al Team e alla sua rispettiva crescita."

Andrea Negroni, entra a far parte del team HPE Aruba Networking a settembre 2023 con l'obiettivo di guidare l'adozione della piattaforma di sicurezza Security Service Edge (SSE) di HPE Aruba Networking, proveniente dall'acquisizione di Axis Security. Prima di unirsi a HPE Aruba Networking, ha trascorso oltre 24 anni presso Cisco Italia, ricoprendo ruoli inizialmente nell'area della prevendita e successivamente in posizioni manageriali. Ha gestito il canale cybersecurity per il Sud Europa, la Germania e l'Europa Centrale, e infine ha ricoperto il ruolo di leader della cybersecurity per l'Italia.

Roberto Obialero, Cybersecurity & Data Protection Advisor, ha una esperienza più che ventennale in ruoli, manageriali, di sviluppo business e tecnici nell'ambito dell'offerta di servizi di sicurezza informatica. Ricopre il ruolo CISO presso alcune organizzazioni supervisionando attività di gestione del rischio, definizione di strategie e roadmap cybersecurity, progetti di business continuity e vulnerability management, gestione di incidenti informatici e programmazione percorsi di security awareness. È in possesso delle certificazioni indipendenti GSTRT, GPPA e GCFA ottenute attraverso il programma SANS-GIAC americano, della certificazione ISO 27000 Lead Auditor e si è perfezionato in "Computer Forensics & Data Protection" e "Data Protection & Data Governance" presso l'Università Statale di Milano. Membro del Comitato Direttivo Clusit e della ECSO-CISO European Community collabora attivamente alla realizzazione di progetti di ricerca nell'ambito Cybersecurity & Data Protection con le principali community di settore; eroga formazione frontale o tramite webinar, speaker in occasione di diversi eventi di rilevanza nazionale, oltre ad aver contribuito alla redazione di diverse pubblicazioni e articoli per conto di riviste specializzate.

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.

Michela Pesante, laureata in Ingegneria Civile al Politecnico di Milano, ha lavorato in aziende del settore servizi IT come Xerox, Sysnet, PA Group. Da oltre 17 anni lavora nel settore della sicurezza informatica. In particolare, da 14 anni è Account Manager nel team commerciale di RSA Security, focalizzandosi sullo sviluppo di soluzioni di *Identity Access Management*, per le organizzazioni che operano in differenti settori industriali. La strategia aziendale di RSA è di supportare le organizzazioni secondo una strategia *Unified Identity Platform*, con un approccio di sicurezza trasversale per ogni esigenza di business, al fine di mitigare i rischi legati agli incidenti di sicurezza nel contesto dell'identità.

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.

Massimo Prato, è direttore Professional Services di Toshiba Tec Italia per la divisione Printing Office Solutions. Nelle sue responsabilità all'interno dei servizi professionali è specializzato nel ricercare partner tecnologici da intergrare in progetti complessi e nella gestione dei servizi innovativi. Per ASSOIT, l'Associazione Produttori Soluzioni di Stampa, Digitalizzazione e Gestione Documentale, ha curato la stesura del capitolo dedicato alla sicurezza dei sistemi di stampa.

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 ed 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.

Patrizio Rinaldi, vive a Roma e lavora nel campo dell'IT da oltre 25 anni. Ha iniziato la sua carriera presso software house nel nord Italia, dove ha operato come sistemista di rete in ambienti distribuiti e ha svolto il ruolo di docente per corsi di certificazione su varie tecnologie. Dopo alcuni anni di attività da libero professionista, durante i quali ha collaborato a progetti di resilienza delle infrastrutture informatiche dei principali gruppi bancari italiani, approda in Microsoft nella divisione servizi professionali dove ha trascorso 10 anni ricoprendo diversi ruoli. La sua esperienza comprende la definizione, progettazione e realizzazione di architetture complesse per la gestione dell'identità, la sicurezza e la collaborazione. Dal 2016 si dedica ad attività di advisory sui temi dell'identità digitale e della sicurezza informatica. È attualmente a capo del team italiano degli specialisti tecnici nell'ambito della Cybersecurity e Data Security di Microsoft, con la missione di aiutare organizzazioni pubbliche e private a integrare la sicurezza cibernetica e l'adesione agli standard normativi nel loro percorso di trasformazione digitale, affinché questi fattori rappresentino elementi abilitanti per ecosistemi informatici all'avanguardia.

Pier Luigi Rotondo, è specialista tecnico per le soluzioni IBM Security di Threat Management. Ha contribuito a molti progetti su soluzioni per il Threat Management, Threat Intelligence, Attack Surface Management, Identity e Access Governance, e Single Sign-on. Con una laurea in Scienze dell'Informazione presso Sapienza Università di Roma, Pier Luigi è coinvolto in attività accademiche su temi di sicurezza delle informazioni in Corsi di Laurea e Master presso l'Università di Roma e di Perugia. Per conto di IBM Italia scrive articoli divulgativi, e contribuisce permanentemente dal 2015 al Rapporto Clusit sulla Sicurezza ICT in Italia sul cybercrime nel settore finanziario, presentando i risultati IBM e le tendenze del mercato della cyber security. È membro del Comitato Scientifico del CLUSIT dal 2021.

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.

Felice Santosusso, attualmente Senior Enterprise Account Executive per RSA Italia, dopo la laurea in matematica ha consolidato le sue esperienze nei temi di cybersecurity e processi di gestione delle identità in importanti aziende del settore. Da sempre attento alle esigenze dei clienti, dapprima come executive nelle divisioni dei servizi e poi come account manager, i suo obbiettivi sono quelli di accompagnare i clienti nel trovare la soluzioni migliore alle complesse esigenze di gestione e sicurezza delle identità digitali.

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.

Gabriele Scialò, si è laureato nel 2020 in Bocconi, nel corso di Marketing Management, per poi intraprendere un'esperienza in ambito di realtà che operano nel modo delle telecomunicazioni, sia nazionali che internazionali. Oggi lavora per Fastweb, nel ruolo di Product Marketing Manager dei servizi security: segue il portafoglio dei servizi di Cybersecurity, contribuendo allo sviluppo dei prodotti relativi, partendo dall'analisi delle necessità del mercato fino alla costruzione del servizio e sua comunicazione.

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.

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

Pietro Valente, ricopre il ruolo di Senior Sales Engineer in RSA dal 2021, proponendo soluzioni evolute per la gestione delle Identità. Lavora da 18 anni nel campo della cybersecurity ed ha ricoperto in passato ruoli di progettazione e sviluppo di soluzioni cyber per importanti clienti nel settore delle telecomunicazioni, utilities e difesa e, per lunghi periodi, ha avuto l'opportunità di focalizzarsi specificatamente su tematiche di Identity Access Management e di sicurezza infrastrutturale. Pietro Valente è laureato in informatica, a seguito della quale ha poi conseguito significative certificazioni (CISSP-CISM-CEH-PMP); crede nel continuo arricchimento del know-how personale e del suo network partecipando a eventi e a tavole rotonde in ambito cybersecurity.

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.

Clusit
Associazione Italiana per la Sicurezza Informatica

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, Roma, Cagliari e Verona), gli Atelier della Security Summit Academy, Le Tavole Rotonde Verticali (Energy & Utilities, Health Care, Finance, Manufacturing).
- I Gruppi di Lavoro della Clusit Community for Security.
- Rapporti Clusit: Rapporto annuale, con aggiornamento semestrale, sulla sicurezza ICT in Italia, in produzione dal 2012.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa ogni anno nel mese di ottobre in Italia da Clusit.
- 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.

SECURITY SUMMIT ACADEMY

La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

SECURITY SUMMIT VERTICAL

Certificata dalla folta schiera di **relatori (più di 700** sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre **20.000 partecipanti**, e sono stati rilasciati circa **15.000 attestati** validi per l'attribuzione di oltre **48.000 crediti formativi** (CPE).
Nel 2023 i Security Summit sono stati oggetto di oltre **800 articoli e servizi su web, cartaceo, Radio e TV**.

L'edizione 2024

Il 2024 inizia con una edizione tutta in presenza, dal **19 al 21 marzo, a Milano**.
Seguiranno: il 19 giugno il Security Summit di **Roma**, il 18 settembre il Security Summit di **Cagliari**, il 24 ottobre il Security Summit di **Verona** e il 7 novembre un Security Summit Streaming Edition. Continueranno inoltre gli **Atelier della Security Summit Academy**, che si terranno tutto l'anno e gli **Eventi Verticali**, programmati il 28 maggio (**Energy & Utilities**), il 19 giugno /**Health Care**) e il 7 novembre (**Manufacturing**).

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

HPE aruba networking

netwrix

SECURITY SUMMIT

www.securitysummit.it