Rapporto

2023

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 non sono positivi. Soprattutto per l'Italia.
Siamo al centro del fenomeno e non si intravede al momento una possibile inversione di tendenza.

Ci sono una serie di fattori che concorrono a questa situazione.
L'Italia in base all'indice DESI (Digital Economy and Society Index) della Commissione Europea sui 27 Paesi membri dell'Unione Europea è ventesima per livello di digitalizzazione complessiva, è terzultima per popolazione con competenze digitali almeno di base (42%), contro una media UE del 56%, ed è quartultima per competenze digitali avanzate (22%), contro una media UE del 31%.
L'Italia è ultima (!) nel continente per quota di laureati in ambito ICT sul totale della popolazione con una laurea (1,3% rispetto a un valore UE del 3,9%).

A questa situazione già di per sé critica, che spiega la grandissima difficoltà di aziende, Pubbliche amministrazioni e Autorità nel trovare risorse da inserire nei propri staff, si aggiunge una cronica carenza di risorse economiche.

Secondo lo studio dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano nel 2022 l'Italia ha speso nel 2022 per prodotti e servizi di sicurezza informatica un miliardo e ottocentocinquanta milioni.
Si tratta dell'0,1% del Pil dato in crescita del 18% rispetto al 2021 ma si tratta pur sempre, in valore assoluto, della metà di Germania, Francia, Canada e Giappone e di un terzo di Stati Uniti e Regno unito.

Un quadro quindi delicato in cui però si devono considerare anche i fattori positivi.
Innanzitutto il ruolo dell'ACN, che sta guidando e diventando punto di riferimento per il Paese nel suo insieme.
Ma anche avere ora una strategia nazionale di cybersicurezza e l'obiettivo di un polo strategico nazionale rappresentano grandi passi avanti in una logica di fronte comune.
Aggiungerei anche la leva normativa, che continua a fare la sua parte come dimostrano i recenti provvedimenti NIS 2 e DORA.
E, infine, la consapevolezza. Sia nelle PMI che nelle grandi imprese la cybersecurity è la priorità di investimento numero uno da almeno due anni il che dimostra, unitamente al fatto che sempre più spesso di cyber si parla nei C.d.A., che a livello manageriale molto si è fatto per portare consapevolezza sul tema della sicurezza informatica.

Serve ora continuare su questa strada.
Serve aumentare gli sforzi e possibilmente fare fronte comune.
Trovare strade per mettere a fattor comune gli investimenti senza disperderli in rivoli di poca efficacia.

Tante piccole difese, non fanno una grande difesa.
Servono economie di scala e messa a fattor comune di esperienze, competenze, skill, risorse.

È difficile, soprattutto in un paese così diviso come l'Italia, ma si può fare.

*** *** ***

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una ampia serie di fonti.
I dati per l'anno 2022 confermano da un lato le previsioni in merito alla crescita dei casi di Information Warfare ma anche la tendenza a una sempre maggiore gravità dei casi che ci troviamo ad analizzare.

In questo scenario il nostro Paese è pesantemente coinvolto, anche e più di altri.
Abbiamo subito un notevole incremento di attacchi andati a segno nel 2022 e questo ci porta a dire che dal 2022 "l'Italia è nel mirino" in quanto subisce ormai il 7,6% degli attacchi globali (contro un 3,4% del 2021).

A maggior ragione serve una grande consapevolezza e un grande impegno di tutti per riuscire a ottenere già dal 2023 un miglioramento di una situazione che rischia di diventare insostenibile nel medio-lungo periodo.

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 2023.

Oltre 70.000 copie scaricate e più di 500 articoli pubblicati nel 2022, 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 2022**, confrontandoli con i dati raccolti nei 4 anni precedenti.
Ci siamo avvalsi anche in questa edizione dei dati relativi agli attacchi in Italia rilevati dal **Security Operations Center (SOC) di FASTWEB**.
L'analisi degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso degli ultimi 12 mesi.
Segue un'analisi realizzata da Libraesva sul**l'evoluzione dell'e-mail security in Italia** ed un approfondimento sulla **Sanità, tra cyberattacchi e rischi per la salute**, realizzato dalle Women for Security**.**
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, ed un contributo realizzato dagli **esperti del CERT di Banca d'Italia sullo scenario evolutivo della minaccia ransomware**.

Seguono tre survey.
- La prima, realizzata da Netwrix, che ha intervistato 720 professionisti **sul passaggio al Cloud e sulle problematiche di sicurezza riscontrate.**
- La seconda **sulla gestione del rischio cyber nelle grandi organizzazioni italiane,** realizzata dall'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano.
- La terza **sulla Cybersecurity nelle micro e piccole imprese,** una Survey di CNA Milano e dell'Unione Artigiani Milano.

Questi sono infine i temi trattati nella sezione FOCUS ON:
- **Access Broker e attacchi basati sull'identità: tendenze e protezione**, a cura di CrowdStrike
- **Infrastrutture Critiche (perimetro di cybersecurity nazionale),** a cura di Fortinet
- **Cyber Resilienza**, a cura di Microsoft
- **La nuova direttiva NIS 2 tra obbligo normativo e opportunità di migliorare la resilienza**, a cura di Servitecno
- **La Supply Chain come Kill Chain - La sicurezza nell'epoca Zero Trust**, a cura di Trend Micro
- **Enterprise Architecture per il supporto all'Information Security Management,** a cura di Consulthink
- **Intelligenza Artificiale - Un approccio alla gestione dei rischi per le aziende**, a cura di Tamara Devalle e Andrea Pasquinucci.
- **SOC: scenario attuale e pianificazione per il 2023**, a cura di Federica Maria Rita Livelli.

Continuiamo anche in questa edizione del Rapporto le interviste dedicate agli attori istituzionali (Autority, Agenzie, Forze dell'Ordine e Centri di Competenza) con cui il Clusit ha stretto accordi operativi per diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
Riportiamo quindi **un'intervista ad Agostino Ghiglia, Componente del Garante per la protezione dei dati personali,** che contribuisce al Rapporto Clusit con un pezzo **su Metaverso e Cybersecurity**.

Analisi dei principali cyber attacchi noti del 2022 a livello globale

Italia nel mirino

Come di consueto in questa prima sezione del Rapporto CLUSIT 2023, giunto ormai al suo undicesimo 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 2022.

Osservando la situazione dal punto di vista quantitativo, negli ultimi 5 anni la situazione è peggiorata nettamente, seguendo un trend pressoché costante. Confrontando i numeri del 2018 con quelli del 2022 la crescita del numero di attacchi rilevati è stata del 60% (da 1.554 a 2.489).

Nello stesso periodo la media mensile di attacchi gravi a livello globale è passata da 130 a 207. Oltre alla maggiore frequenza, anche la nostra valutazione della Severity media (indice di gravità) di questi attacchi è drasticamente peggiorata, il che rappresenta un significativo moltiplicatore dei danni.

Considerato che questa analisi riguarda attacchi andati a buon fine (cioè effettivamente avvenuti, non solo tentati) divenuti di dominio pubblico, l'osservazione di queste dinamiche conferma la nostra convinzione che, rispetto al periodo 2011-2017, nell'ultimo lustro si sia verificato un cambiamento sostanziale nei livelli globali di cyber-insicurezza, al quale non è corrisposto un incremento sufficiente delle contromisure adottate dai difensori.

Come abbiamo scritto commentando i dati del 2021, ormai "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 si è aggiunto il conflitto tra Russia ed Ucraina, che ha scoperchiato un vaso di Pandora di capacità cibernetiche offensive, utilizzate dai contendenti, dai loro alleati e in generale da tutti i principali attori globali, a supporto di attività di cyber-intelligence, di cyber-warfare e di operazioni ibride.

Per quanto ancora oggi in ambito intelligence e militare prevalgano gli attacchi effettuati tramite il cyberspazio (tipicamente di natura clandestina, sotto la soglia del conflitto aperto) rispetto a quelli condotti verso il cyberspazio (con finalità di degrado, negazione o distruzione

di sistemi e infrastrutture digitali), questa proporzione è ragionevolmente destinata a cambiare. D'ora in poi le infrastrutture critiche e molte altre piattaforme digitali sensibili, meno tutelate a livello normativo ma comunque essenziali per la collettività, saranno bersagli designati, costantemente al centro del mirino di numerosi attori, governativi e non.

Questo processo di rapida adozione e messa in campo di strumenti cyber-offensivi sofisticati sarà difficilmente reversibile, e in prospettiva potrebbe causare gravi conseguenze in un mondo già fortemente digitalizzato ma sostanzialmente impreparato ad affrontare minacce di questa natura.

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", nel contesto di crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa.

In questo mutato scenario anche il nostro Paese risulta inevitabilmente coinvolto, come dimostra il significativo incremento di attacchi andati a segno nel 2022. Potremmo dire che dal 2022 "l'Italia è nel mirino", ricevendo ormai il 7,6% degli attacchi globali (contro un 3,4% del 2021). Per questa ragione da questa edizione abbiamo aggiunto un capitolo specifico e svolto alcune considerazioni puntuali su quanto osservato, nella speranza di contribuire ad un incremento della consapevolezza nazionale rispetto a queste minacce crescenti.

In questo senso auspichiamo che il PNRR (Piano nazionale di ripresa e resilienza), che complessivamente alloca circa 45 miliardi di euro per la "transizione digitale", possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune (anche) in ambito cyber, e che non abbia come esito un ampliamento incontrollato della superficie di attacco esposta dal Paese, ma al contrario una sua complessiva, significativa riduzione.

Per realizzarsi, questo obiettivo (assolutamente prioritario e strategico) richiederà una governance stringente in ottica cyber security di tutti i progetti di digitalizzazione previsti dal Piano, supportata da una visione politica salda, che non accetti compromessi e pressioni esterne, e (finalmente) la valorizzazione delle risorse umane con competenze cyber (in termini di talenti e di esperienze) del Paese, ed il loro sviluppo in termini quantitativi e qualitativi.

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

Analisi dei principali cyber attacchi noti a livello globale del 2018-2021 e del 2022

In questa sezione offriamo una panoramica degli incidenti di sicurezza di pubblico dominio più significativi avvenuti a livello globale nell'anno precedente, confrontandoli con i dati raccolti nei 4 anni precedenti.
Lo studio si basa sull'analisi di oltre 16.000 cyber attacchi noti, andati a buon fine e di particolare gravità, a partire dal 2011, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali, o che comunque prefigurano scenari particolarmente preoccupanti.

Nel periodo che prenderemo in esame, tra gennaio 2018 e dicembre 2022 si sono verificati un totale di 9.633 cyber attacchi, così suddivisi:

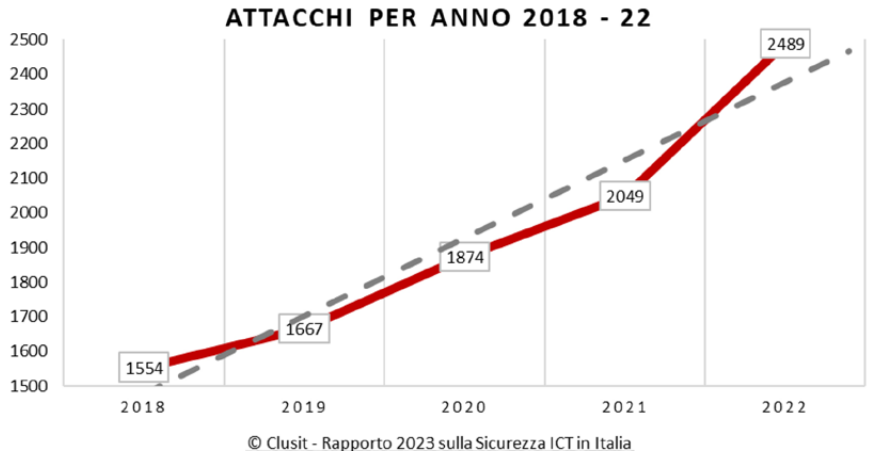


Fig. 1: *Andamento dei cyber attacchi nel periodo 2018 - 22*

Il nostro campione rappresenta il 58.4% del totale degli incidenti classificati in 12 anni, con una media complessiva di 161 attacchi al mese nell'intero periodo (erano 39 nel 2011, 130 nel 2018, e sono 207 nel 2022).

Nell'ultimo anno abbiamo registrato 2,489 incidenti, il numero maggiore di sempre ed è interessante notare come nel 2022 la realtà abbia superato le previsioni indicate in grigio dalla linea di tendenza.

Il picco massimo dell'anno e di sempre si è registrato a marzo con 238 attacchi.
Questa è la distribuzione mensile degli attacchi nel 2022:

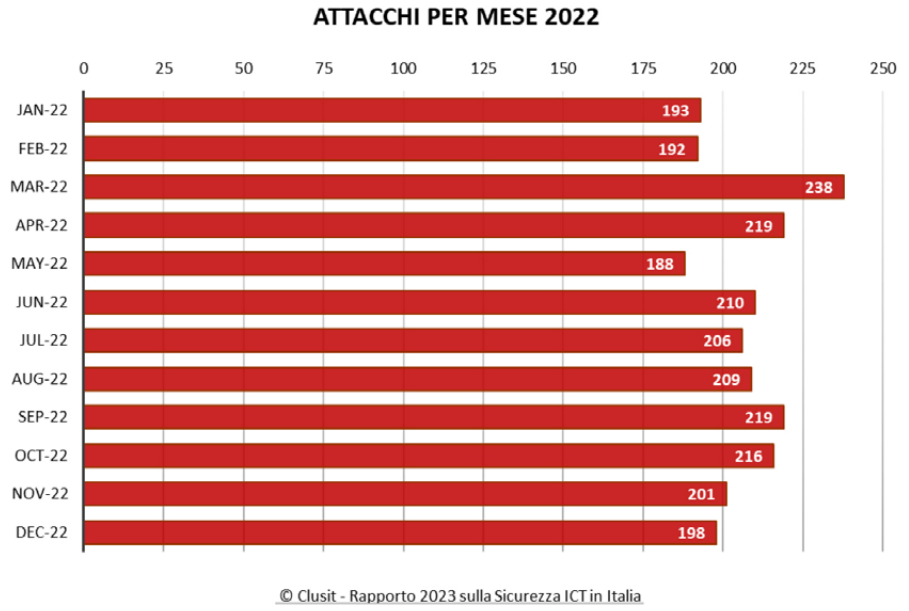


Fig. 2: *Numero di attacchi per mese nel 2022*

Come si evince dal grafico successivo, i mesi più attivi caratterizzati da un numero di incidenti superiore alla media (indicata dalla linea blu) sono stati marzo, aprile, luglio, agosto, settembre e ottobre:

Di seguito una rappresentazione sintetica delle medie mensili negli ultimi 4 anni.

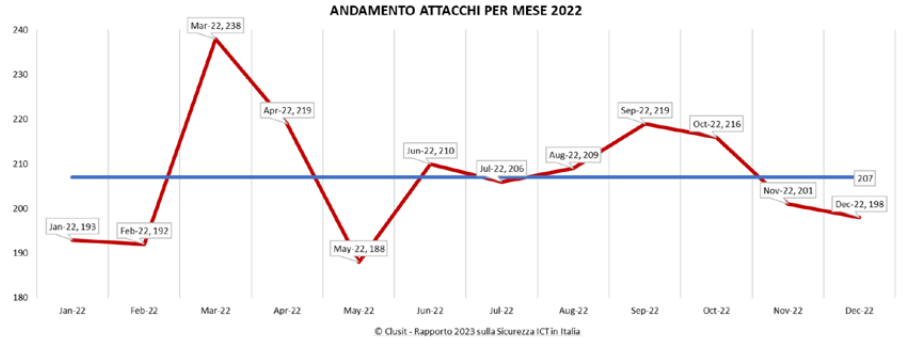


Fig 3: *Andamento mensile degli attacchi nel 2002 e media mensile*

Di seguito una rappresentazione sintetica delle medie mensili negli ultimi 5 anni.

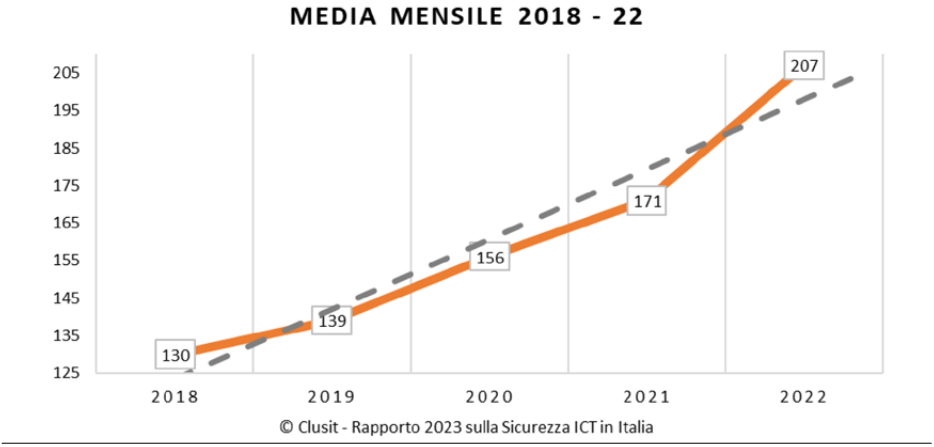


Fig 4: *Andamento delle medie mensili nel periodo 2018-22*

Anche in questo caso, il dato dell'ultimo anno ha superato i trend indicati in grigio dalla linea di tendenza.

Distribuzione degli attaccanti per tipologia (2018 – 2022)

Analizzando lo storico degli attaccanti dal 2018 al 2022 (Fig. 4) si nota che si mantiene la prevalenza degli attaccanti del tipo "cybercrime", con un andamento regolarmente in crescita come numero di attacchi. La crescita, sia pure con numeri più bassi, si mantiene anche per le altre tipologie di attaccanti. In particolare, per il cybercrime nel 2022 si osservano oltre 2.000 attacchi (2.043) che scendono a 259 per spionaggio e sabotaggio, a 103 per information warfare e a solo 84 per l'attivismo.

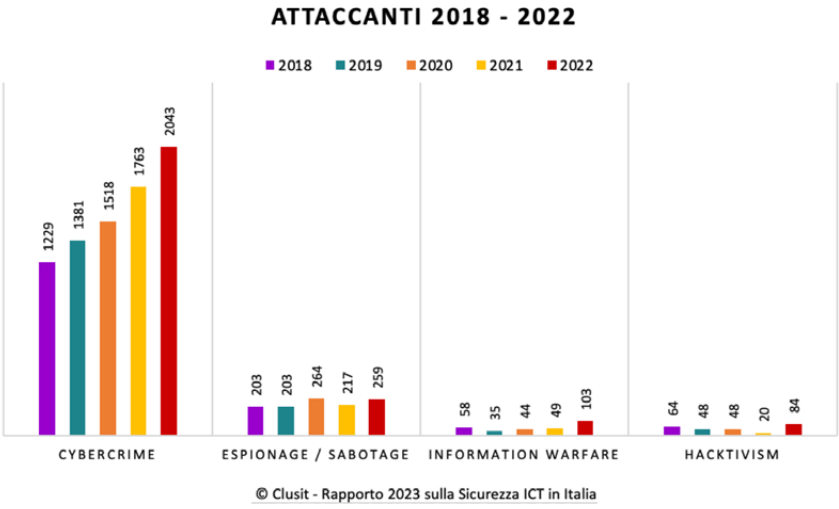


Fig. 5: *Distribuzione degli attaccanti dal 2018 al 2022*

La visualizzazione degli stessi dati in termini percentuali consente una lettura da un punto di vista diverso (Fig. 5), infatti gli attaccanti per la tipologia Cybercrime sono in leggera flessione rispetto al 2021 (82% contro 86%) con uno scarto di ±1% rispetto a 2020 e 2019 e in aumento del 3% rispetto al 2018.

Il calo percentuale della tipologia Cybercrime va a "vantaggio" dell'Information warfare che raggiunge il 4%, tornando ai valori del 2018, dopo aver subito una leggera decrescita dal 2019 al 2021 (2%). La stessa considerazione vale anche per l'attivismo, che dopo una continua decrescita di un punto percentuale all'anno dal 2018 al 2021 (dal 4% all'1%), nel 2022 ritorna al 3%.

Infine, lo spionaggio/sabotaggio perde un punto percentuale rispetto al 2021, dopo aver raggiunto il massimo del 14% nel 2020, all'epoca soprattutto a causa di azioni di spionaggio industriale legato al Covid (principalmente verso enti di ricerca, laboratori, cliniche, etc…). Si può supporre che la crescita di Information warfare e soprattutto di attivismo possa essere dovuta almeno in parte alla guerra in Ucraina, che ha stimolato le azioni anche "digitali"

degli attivisti e ha sollecitato la diffusione di informazioni di propaganda e contro-propaganda. Tale crescita, assieme a quella dell'hacktivism sembra, come detto sopra, tratteggiare uno scenario in cui si sia ridotta la portata del "comune" cybercrime, il che rende ancora una volta importante sottolineare come in valore assoluto queste tre categorie abbiano raggiunto, nel 2022, i propri massimi storici.

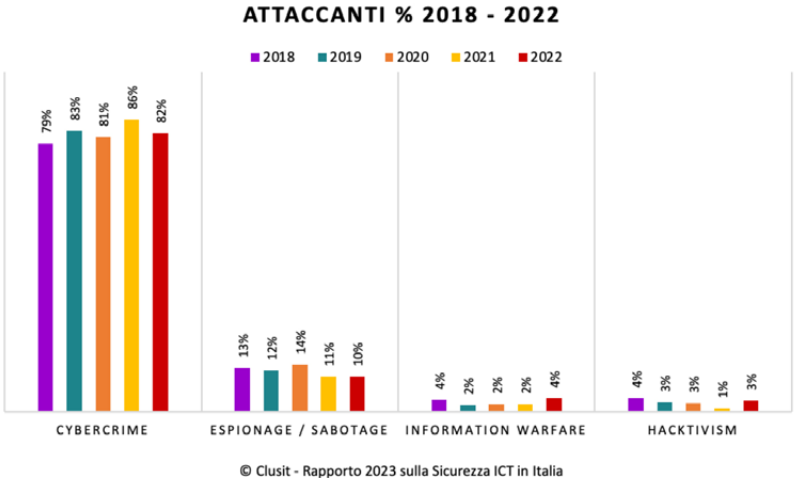


Fig. 6: *La distribuzione percentuale degli attaccanti tra il 2018 e il 2022*

È interessante anche soffermarsi sui dati percentuali del 2022 (Fig. 6) che mostrano con immediatezza l'enorme preponderanza degli attaccanti Cybercrime: è comunque un settore che attira grande attenzione da parte del crimine, probabilmente per i significativi risvolti economici legati alla sempre maggiore diffusione degli attacchi ransomware.
Dalla stessa figura emerge ancora, come dai dati storici, il ruolo significativo degli attaccanti che ricadono nella categoria "spionaggio/sabotaggio" con un 11%, mentre Information Warfare e Hacktivism sono rispettivamente al 4% e 3%.
Questo non deve stupire in alcun modo, per due ragioni. I governi potrebbero perpetrare i propri attacchi con modalità che possano essere attribuite ad altri attori. Non sono infatti famosi, militari e servizi, per le rivendicazioni pubbliche delle loro operazioni.
Quanto all'hacktivism, oggi molte campagne tese a colpire la reputazione delle organizzazioni sono molto più efficaci sui social che non con defacement o tecniche analoghe.

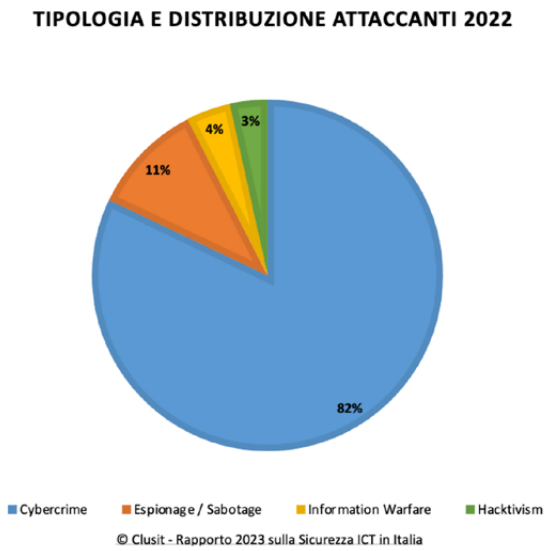


Fig. 7: *Andamento percentuale della tipologia di attaccanti nel 2022*

Distribuzione delle vittime per categoria (2018 – 2022)

Il dato più saliente che emerge dall'analisi delle vittime degli attacchi nel periodo 2018-2022 (Fig. 8) è la diminuzione di tutte le tipologie tranne che per il Financial, Manufacturing e News e Multimedia. La categoria Financial vede un aumento di un punto (8%) rispetto a 2021 e 2020 (7%). È possibile che questa tendenza dipenda dalla diffusione delle criptovalute, che incoraggia gli attaccanti a esplorare questa nuova possibile fonte di "reddito". Il Manufacturing vede un aumento costante dal 2% del 2018 al 5% del 2022. Sono solo 3 punti ma in sostanza è più che raddoppiato: anche in questo caso è lecito fare l'ipotesi che possa dipendere dalla sempre maggiore diffusione dell'IoT nella manifattura e dalla tendenza verso l'interconnessione dei sistemi industriali. Come è (purtroppo) noto, molto spesso gli oggetti connessi in rete non sono sufficientemente protetti e diventano un punto di accesso facile per gli attaccanti. Infine, le vittime nel settore News e Multimedia, dopo un calo drastico dal 5% al 2% tra il 2018 e il 2020, sono protagoniste di un più che raddoppio tra il 2020 e il 2022, dove ritornano al 5%: una componente di questo aumento è senz'altro riferibile al conflitto in Ucraina, nell'ambito di attività di disinformazione / propaganda e disruption di media outlets "nemici".

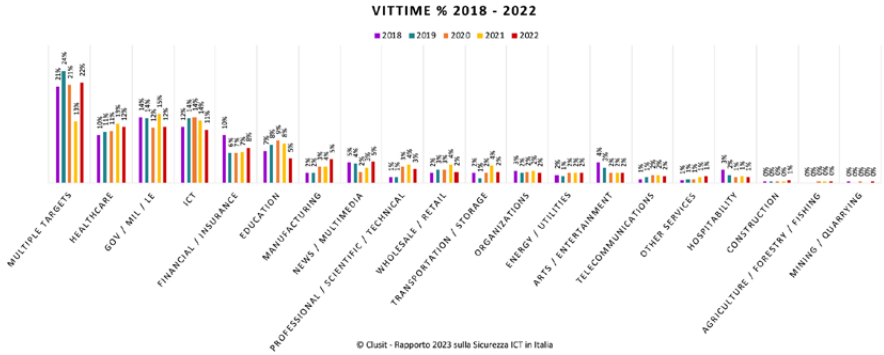


Fig. 8: *Distribuzione percentuale della tipologia di vittime dal 2018 al 2022*

Se ci focalizziamo sulla top 10 della percentuale delle vittime colpite (Fig.9), notiamo una "ricrescita" dei Multiple Targets (22%) che ritorna ai valori 2020 (21%) dopo il brusco calo 2021 (13%). Le tipologie Gov (12%), ICT (11%) e Education (8%) calano tutte del 3% rispetto all'anno precedente. Education e ICT hanno avuto il loro picco, rispettivamente 9% e 14%, entrambe nel 2020, che, lo ricordiamo, è stato l'anno della pandemia da Covid19 in cui tutte le organizzazioni e aziende hanno attivato lo smart working, con un incremento di utilizzo di risorse ICT, come la scuola che è andata in gran parte in didattica a distanza.

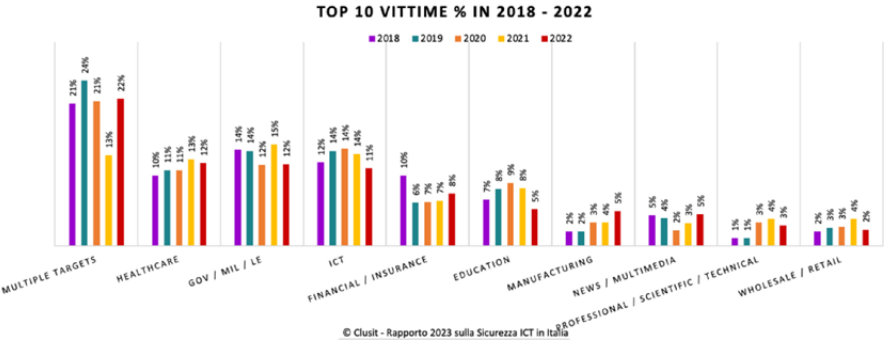


Fig. 9: *Le prime 10 categorie di vittime colpite in valore percentuale*

La Fig. 10 rende con maggiore immediatezza dei grafici precedenti la distribuzione delle vittime per il 2022. I Multiple Targets, pur in netto aumento (vedi Fig.9) sono meno di un quarto di tutte le tipologie di vittime (22%). Healthcare, ICT e Gov si ripartiscono in modo quasi uguale un ulteriore 36%. Financial occupa un 8% mentre Education, News e Multimedia e Manufacturing si assetano tutte sul 5%, per un altro 15% del totale .

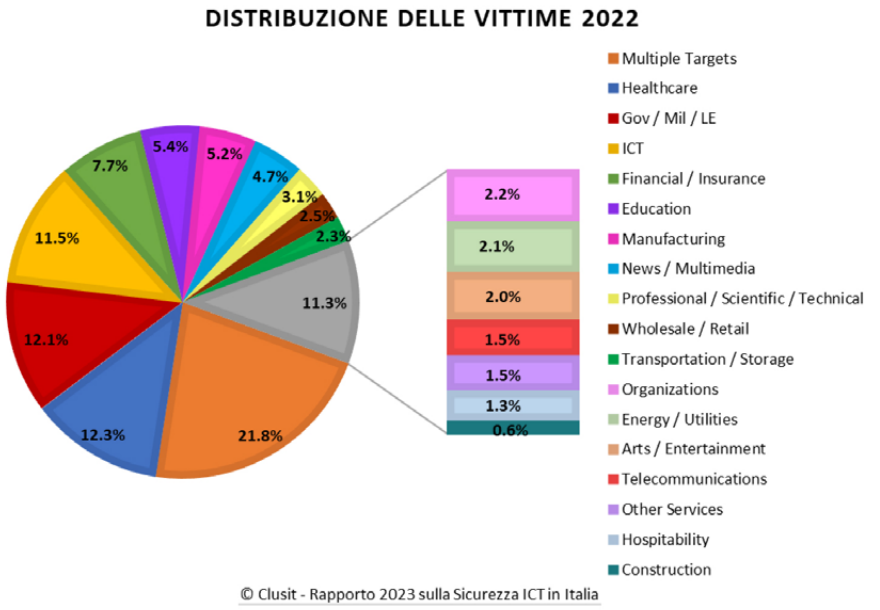


Fig. 10: *Distribuzione della tipologia di vittime nel 2022*

Distribuzione generale delle vittime per area geografica (2022)

La lettura dei dati della distribuzione geografica percentuale delle vittime (Fig. 11) dà indirettamente la fotografia di come stia variando la digitalizzazione nel mondo, ma anche, per altri versi, di quali sono i Paesi che si difendono meglio. L'America nel suo complesso diminuisce di 7 punti percentuali il numero di vittime rispetto all'anno precedente, con un 38%, contro un valore storico che ha oscillato dal 45% al 47% nei 5 anni di osservazione. È in forte crescita rispetto al 2021 il raggruppamento di vari Paesi che passa dal 19% del 2021 al 27% del 2022, avendo avuto un massimo del 31% nel 2019. Ancora in aumento di 3 punti percentuali rispetto al 2021 (21%) l'Europa (24%), che quasi raddoppia rispetto al 2018 (13%). In diminuzione l'Asia dal 12% del 2021 all'8% del 2022. Stabili Oceania e Africa rispettivamente al 2% e all'1%.

Che EU stia crescendo così velocemente può essere il frutto di due fattori. Da un lato, una sempre maggior digitalizzazione dei servizi nel "vecchio continente", che allarga così l'area di esposizione al rischio (d'altronde, i faldoni non possono essere attaccati informaticamente). Dall'altro, pesano un numero sempre maggiore di leggi che impongono la comunicazione degli incidenti, i percorsi di sostenibilità intrapresi da molte organizzazioni, nonché una centralità sempre più diffusa e pervasiva dei servizi digitali nella vita di aziende e persone.

L'interruzione dei servizi di un Internet Service Provider 20 anni fa non avrebbe trovato spazio neppure nei quotidiani locali. Oggi il disservizio di poche ore di un servizio o di una azienda sufficientemente noti finisce al telegiornale in prima serata. L'Europa quindi, sebbene non sia ancora medaglia d'oro per la digitalizzazione rispetto ad altri continenti, guadagna terreno anno su anno, avvicinandosi pericolosamente al numero di segnalazioni di incidenti dei cugini d'oltreoceano.

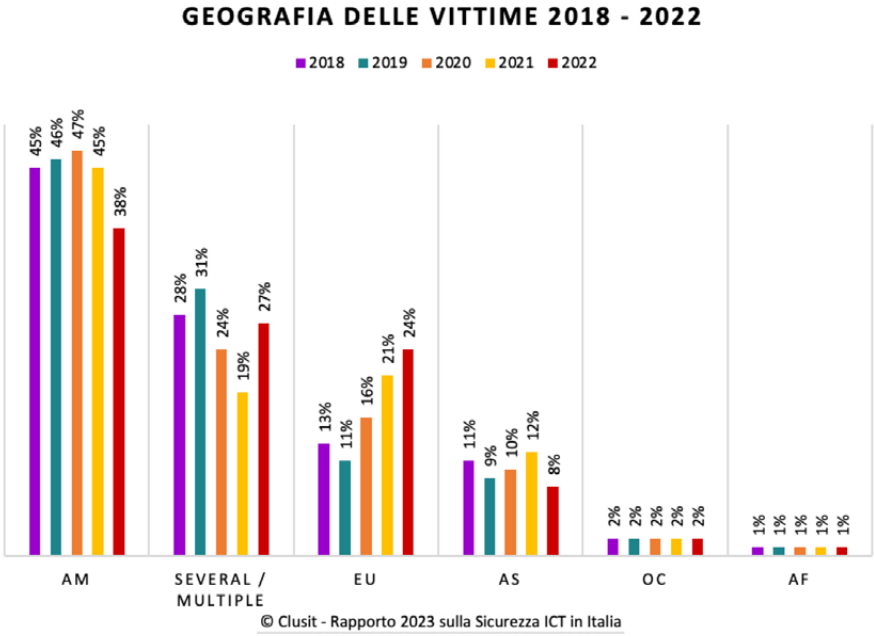


Fig. 11: *Distribuzione geografica percentuale della tipologia delle vittime nel periodo 2018-22*

La figura 12 presenta uno zoom sui dati 2022, confermando la preponderanza percentuale di vittime in America nel 2022 (38%), contro un Europa al 24% e Asia all'8%. Oltre un quarto degli attacchi (27%) è avvenuto parallelamente verso bersagli posti in diversi Paesi, oltre ad Oceania (2%) e Africa 1%.

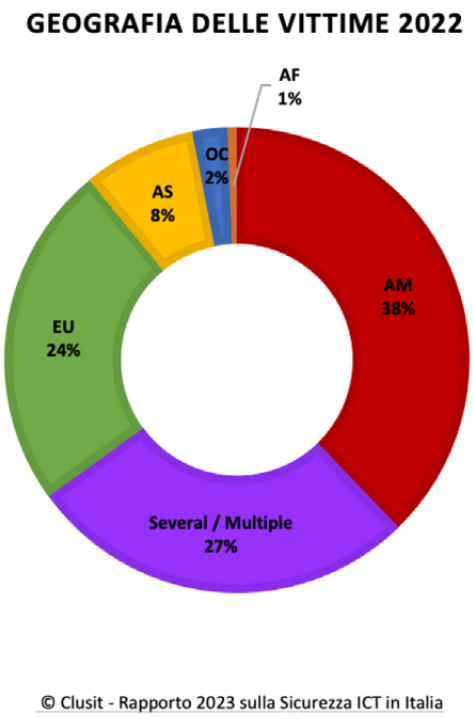


Fig. 12: *Distribuzione geografica delle vittime in percentuale per il 2022*

Distribuzione delle tecniche di attacco (2018 – 2022)

Il 64% degli incidenti hanno come causa azioni "maldestre", degli utenti o del personale ICT.

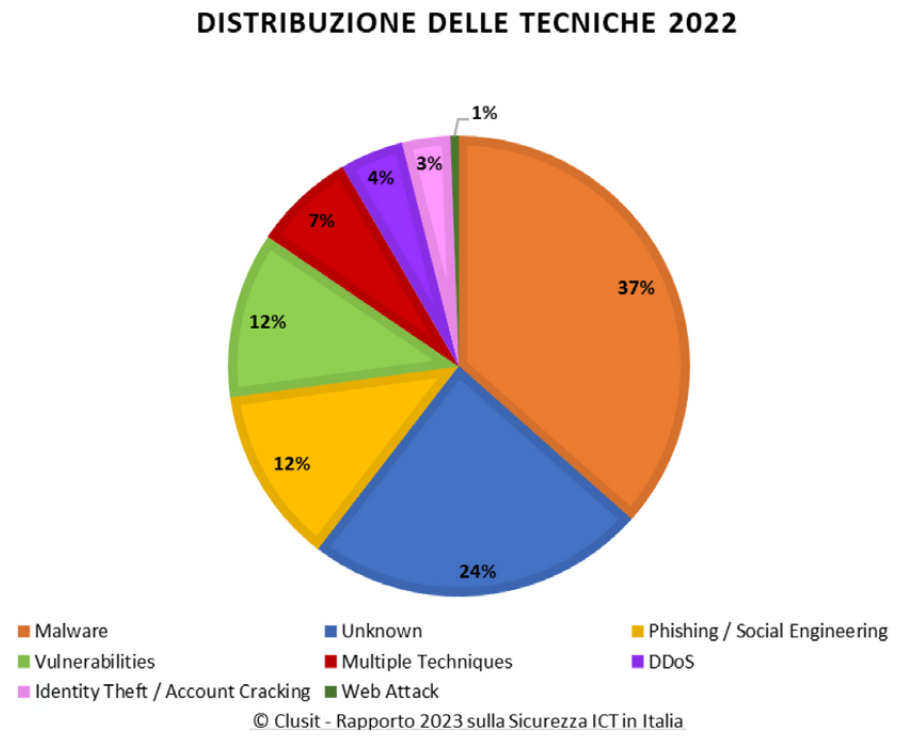


Fig. 13: *Distribuzione delle tecniche di attacco nel 2022*

Malware, Vulnerabilità (ad esclusione della componente di attacchi basati sui c.d. "0-day"), Phishing e Account Cracking dicono che ancora non sappiamo gestire correttamente i nostri account, non teniamo aggiornati i nostri dispositivi (o i nostri server/servizi) e clicchiamo incautamente "cose" sbagliate nelle mail. Problemi che conosciamo dal millennio scorso e sui quali, forse, oggi dovremmo avere una maturità, una postura, diversa da quella che abbiamo. Il Cybercrime in particolare ragiona con le stesse logiche economiche delle aziende tradizionali, ovvero del massimo risultato con il minimo sforzo, investimento, rischio. Perché sferrare un attacco basato su 0-day (alto investimento, competenze avanzate) quando ancora si riesce a violare una rete large enterprise indovinando o riutilizzando da altri data breach password degli utenti? Quando mancano le patch di gravi vulnerabilità pubblicate da mesi? La sempre maggior complessità degli ecosistemi gestiti rende la lotta sempre più impari: mentre chi difende ha un'area (per non citare il perimetro che non esiste più) smisurata da difendere fino all'ultimo dettaglio, all'attaccante basta un piccolo errore, una piccola dimenticanza per trovare l'attack path per lui funzionale.

Rispetto all'anno precedente nel 2022 cresce il ricorso a Phishing Social Engineering (+2%), DDoS (in pratica raddoppiati rispetto al 2021) e tecniche multiple.

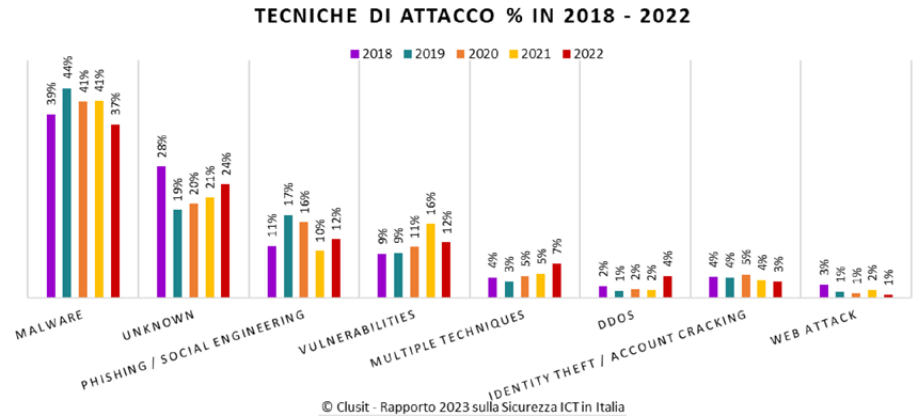


Fig. 14: *Distribuzione delle tecniche di attacco nel periodo 2018-22*

Analisi della "Severity" degli attacchi

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

Negli ultimi due anni, tuttavia, si è instaurata una tendenza preoccupante che ha visto prevalere in maniera consistente gli attacchi con Severity critica o alta.

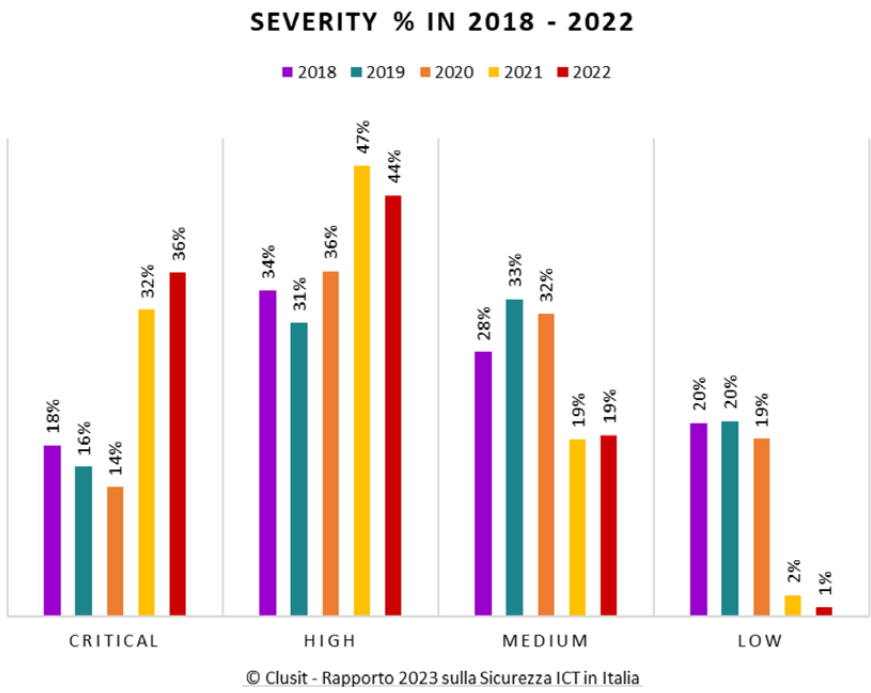


Fig. 15: *Andamento percentuale della Severity degli attacchi nel periodo 2018-22*

Nel 2022 gli attacchi con impatti gravi o gravissimi raggiungono l'80% del totale.

La crescita è continua e per gradini periodici. Dobbiamo fare qualcosa di diverso rispetto a quanto fatto in passato. Peraltro, il dato è sconsolante se abbinato ai risultati delle ricerche in Italia dell'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano: investiamo sempre di più, per subire più incidenti e avere maggiori impatti. Una forbice che si allarga anziché chiudersi. Cosa sbagliamo? È il sintomo che probabilmente dovremmo investire diversamente il denaro, rispetto a quanto fatto in passato, con un cambio radicale di approccio al problema.

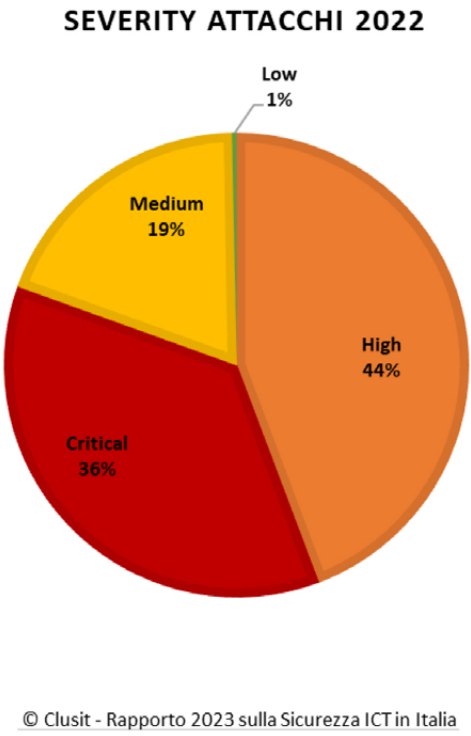


Fig. 16: *Distribuzione della Severity nel 2022*

Severity per tipologia di attaccante

Rispetto al campione esaminato si noti come gli impatti causati sia dai cyber criminali siano in netto aumento: dai poco più di 400 incidenti Critical del 2021 si è passati agli oltre 600 del 2022. Aumenta non solo il volume, quindi, ma anche la quantità di danni subiti dalle vittime.

La stessa considerazione può essere fatta rispetto alle spie industriali: dove a fronte di volumi simili, un numero rilevantissimo di incidenti che nel 2021 erano stimati ad alto impatto, nel 2022 diventano critici.

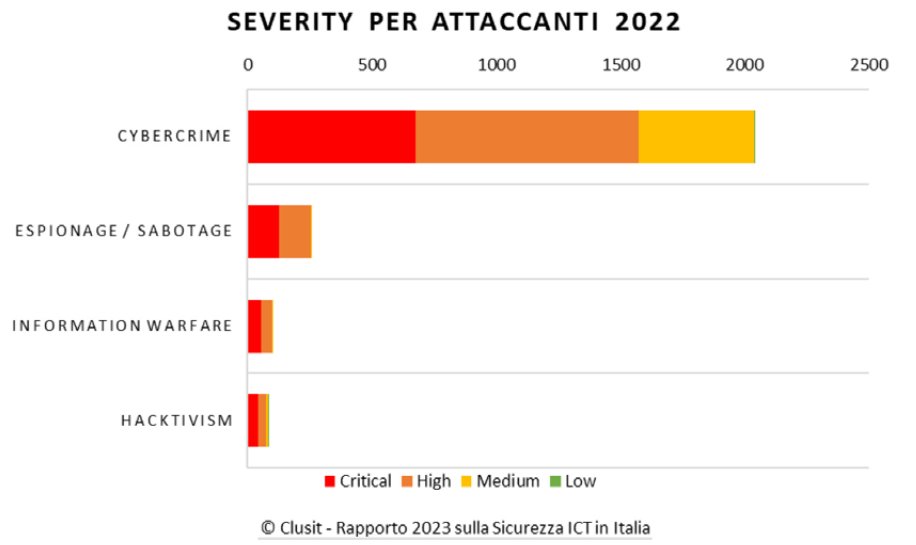


Fig. 17: *Distribuzione della Severity per attaccanti nel 2022*

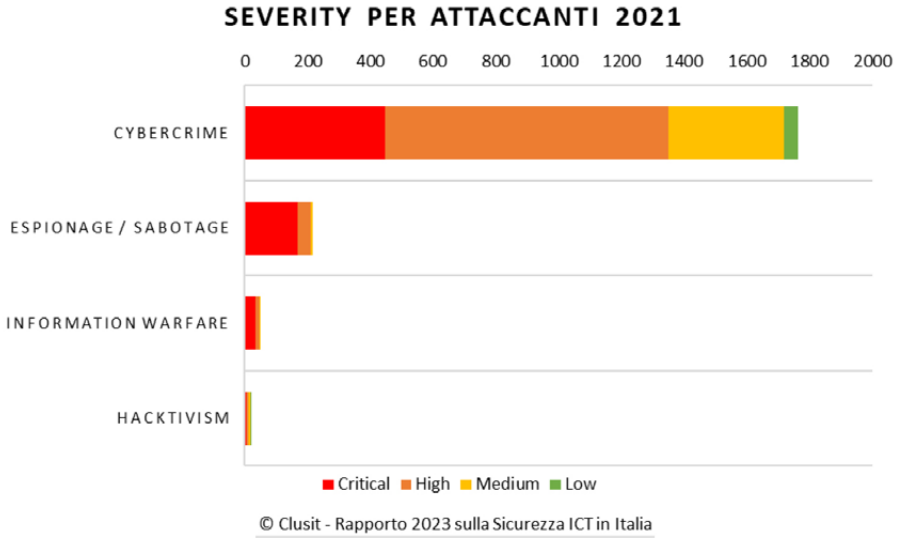


Fig. 18: *Distribuzione della Severity per attaccanti nel 2021*

Severity per tipologia di vittima

Il trend osservato, in generale sulla Severity per attaccante, si conferma anche osservando gli stessi dati clusterizzati per settore merceologico.
Complice, probabilmente, lo scenario geopolitico contingente le organizzazioni governative, militari e le forze di polizia passano dal primo posto al terzo a favore dei "multiple target". Questo è coerente con gli attacchi alle grandi infrastrutture critiche, alle loro filiere e agli attacchi mirati non contro la singola organizzazione, ma contro un ecosistema intero.
Inoltre, questo dato, è una vota di più sintomo di come gli attacchi siano sempre più ingegnerizzati, replicabili su larga scala, come molte delle notizie che sono apparse sui media nello scorso anno dimostrano.
Il settore Sanitario sale ulteriormente in classifica. Indipendentemente dalla tipologia di attaccante, infatti, resta un bersaglio appetibile sia per chi gli attacchi li vuole monetizzare, sia per chi voglia arrecare danni ai servizi fondamentali della società.
Le imprese del comparto ICT restano nella parte alta della classifica, anche a causa della loro particolare predisposizione, in virtù dell'alta digitalizzazione dei processi, ad avere una area esposta più ampia rispetto ad altri settori.
Notevole la scalata della classifica da parte del settore manufatturiero, che soprattutto per i cyber criminali si è dimostrato essere particolarmente redditizio nello scorso anno.
Si conferma quindi il trend, non solo di aumento degli incidenti, ma di aumento della Severity, nei settori maggiormente attenzionati nel 2022.

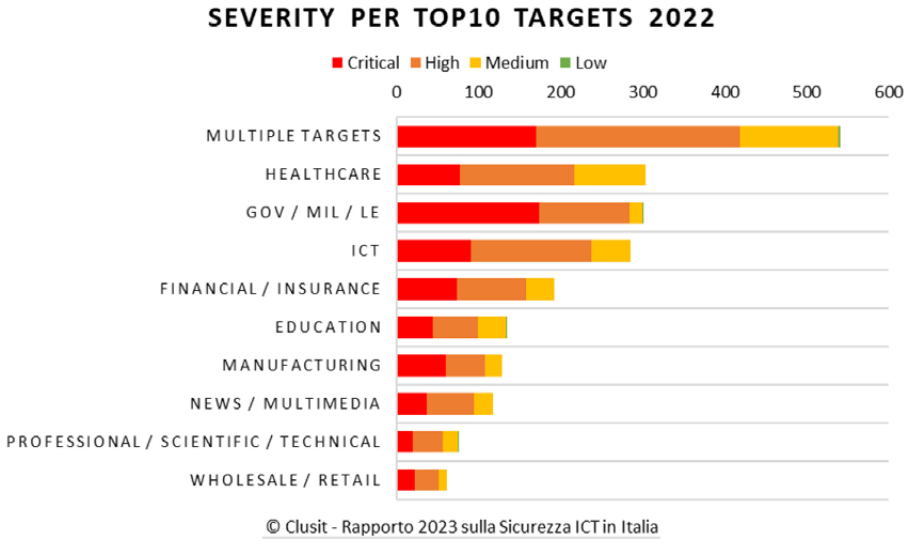


Fig. 19: *Distribuzione della Severity per prime 10 vittime nel 2022*

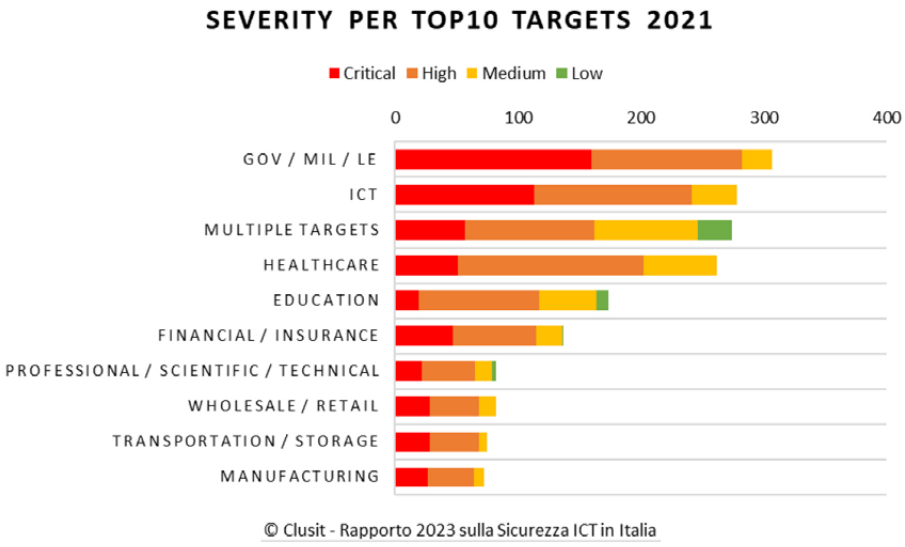


Fig. 20: *Distribuzione della Severity per prime 10 vittime 2021*

Severity per tecniche di attacco

Sconsolante. Non viene alla mente una parola diversa per descrivere il confronto tra gli impatti causati dalle diverse tecniche di attacco.

Al netto della categoria "Unknown", inevitabilmente presente vista la metodologia di analisi, non solo le tecniche sono le medesime di oltre 30 anni fa, ma i danni che riescono a provocare con queste tecniche, spesso banali ed obsolete, sono in netto aumento.

Questo trend, una volta di più, suggerisce la necessità di applicare le best practice conosciute da anni, prima di iniziare a pensare a soluzioni bleeding edge per la maggioranza delle aziende. Quanto a PMI e PAL probabilmente si tratta di adottare una maggior stringente governance dei propri fornitori, dotandosi delle competenze necessarie per farlo. Quanto alle organizzazioni più mature, come suggerito più sopra, probabilmente si tratta in molti casi di adottare un approccio più integrato, con un cambio di passo, mentalità e strategia importante rispetto al passato.

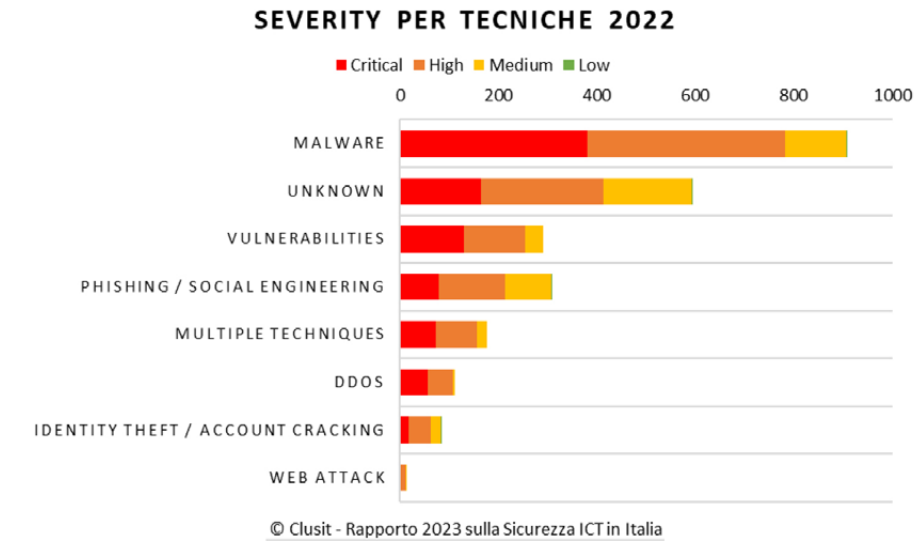


Fig. 21: *Distribuzione della Severity per tecniche di attacco nel 2022*

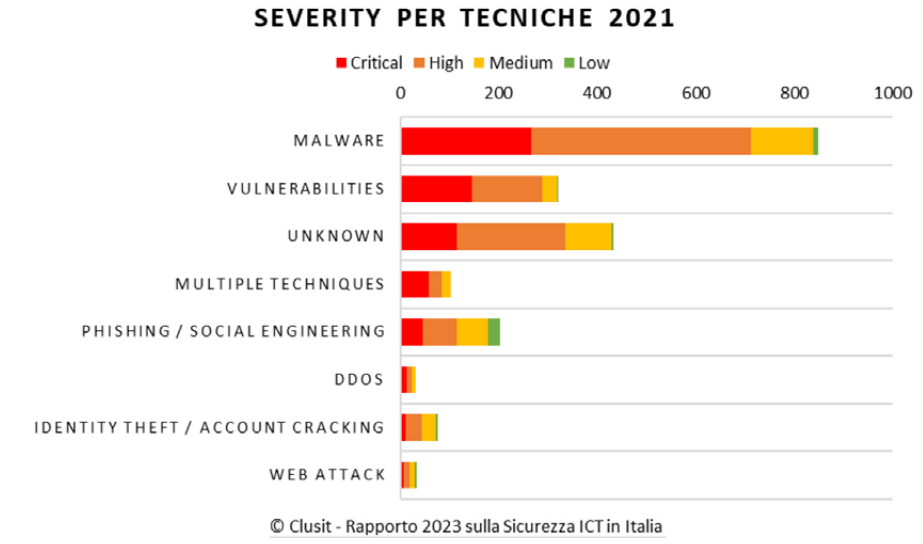


Fig. 22: *Distribuzione della Severity per tecniche di attacco nel 2021*

Analisi degli attacchi in Italia

In questa sezione, per la prima volta, offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti nell'anno precedente.
Tra il 2018 e il 2022 il campione ha incluso **373** attacchi noti di particolare gravità che hanno coinvolto realtà italiane.
Come è possibile vedere nel prossimo grafico (Fig. 23), in cui il dato del 2022 supera la linea di tendenza degli ultimi anni, lo scorso anno il numero di incidenti rilevati è cresciuto significativamente, con un aumento del **527%**.

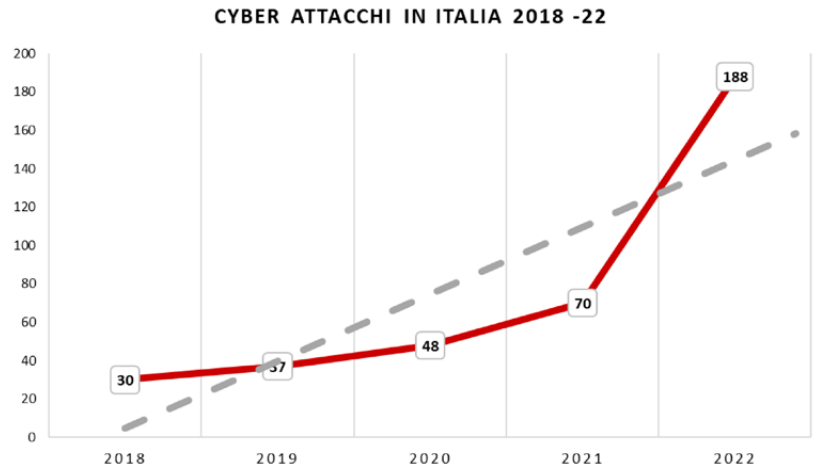


Fig. 23: *Distribuzione dei cyber attacchi in Italia nel periodo 2018-2022*

Tra questi, più del 50% (188 incidenti) sono avvenuti solo nell'ultimo anno preso in esame, andando (purtroppo) a costituire una base di analisi statistica ormai consistente e affidabile per fornire degli indicatori significativi.

La situazione nazionale diventa ancora più preoccupante se confrontata, in termini di percentuali di crescita, rispetto al dato globale, come è possibile vedere nel prossimo grafico (Fig. 24): la consistenza di tale picco di crescita è ampiamente giustificata dal fatto che più del 50% (188) degli incidenti considerati complessivamente sono avvenuti solo nell'ultimo anno preso in esame, andando (purtroppo) a costituire una base di analisi statistica ormai consistente e affidabile per fornire degli indicatori significativi per questo Rapporto.

Fig. 24: *Crescita percentuale degli attacchi Italia vs. global - 2018-2022*

Sempre in relazione al dato globale, significativa non è solo la crescita in termini percentuali, quanto il fatto che **nel 2022 il dato italiano rappresenta il 7,6%** del totale del campione complessivo considerato a livello globale.
D'altro canto, anche dalla Ricerca 2022 dell'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano emerge che:

- il 67% delle grandi imprese ha subito un aumento dei tentativi di attacco rispetto all'anno precedente;
- il 14% delle grandi imprese dichiara di aver subito attacchi con conseguenze concrete.

È possibile, sulla base di queste informazioni, sostenere che il nostro paese stia osservando una particolare recrudescenza e attenzione da parte degli attaccanti, rispetto al resto del mondo?

Distribuzione degli attaccanti per tipologia (2018 – 2022)

Per provare a dare una risposta, analizziamo innanzitutto la tipologia di attaccanti, indicativa delle finalità e propedeutica a capire quali fenomeni prevalenti dobbiamo tenere sotto attenzione.
Tra quelli avvenuti In Italia, la stragrande maggioranza degli attacchi noti si riferisce alla categoria **"Cybercrime"**, che rappresenta il **93%** del totale, **+11%** rispetto al resto del mondo (dove la percentuale è pari all'**82%**).

Seguono con il **7%** gli incidenti classificati come **"Hacktivism"**, mentre non rilevano in modo significativo gli attacchi nelle categorie "Espionage / Sabotage" o "Information Warfare".

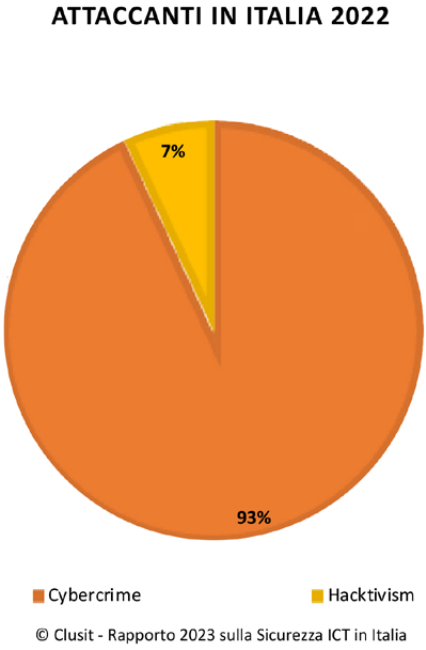


Fig. 25: *Attaccanti in Italia nel 2022*

Sebbene diminuisca il peso percentuale del Cybercrime (nel 2021 rappresentava il 100% degli attacchi), in termini assoluti anche in Italia nel 2022 questa categoria ha fatto registrare il numero di attacchi più elevato mai rilevato. Rispetto al 2021, la crescita è pari al **150%**, passando da 70 a 175 attacchi rilevati.

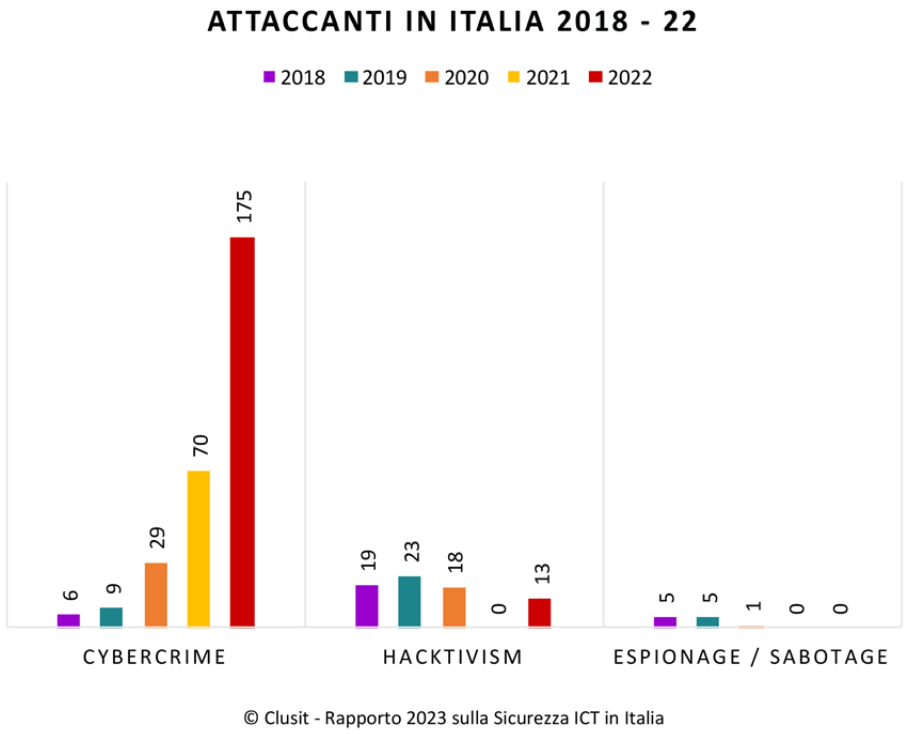


Fig. 26: *Attaccanti in Italia nel periodo 2018-2022*

Distribuzione delle vittime per categoria (2018 – 2022)

Guardando alla distribuzione delle vittime, la categoria merceologica per cui si rileva un maggior numero di attacchi è **"Government"** (**20%** del totale), seguita a breve distanza da **"Manufacturing"** (**19%**).

La ripartizione è significativamente diversa rispetto a quella del campione a livello mondiale, in cui le due categorie raccolgono rispettivamente il 12% e il 5% degli attacchi (terza e settima posizione).

Gli incidenti rivolti al "Manufacturing" rilevati in Italia, in particolare, rappresentano il 27% del totale degli attacchi censiti a livello globale nei confronti di questo settore.

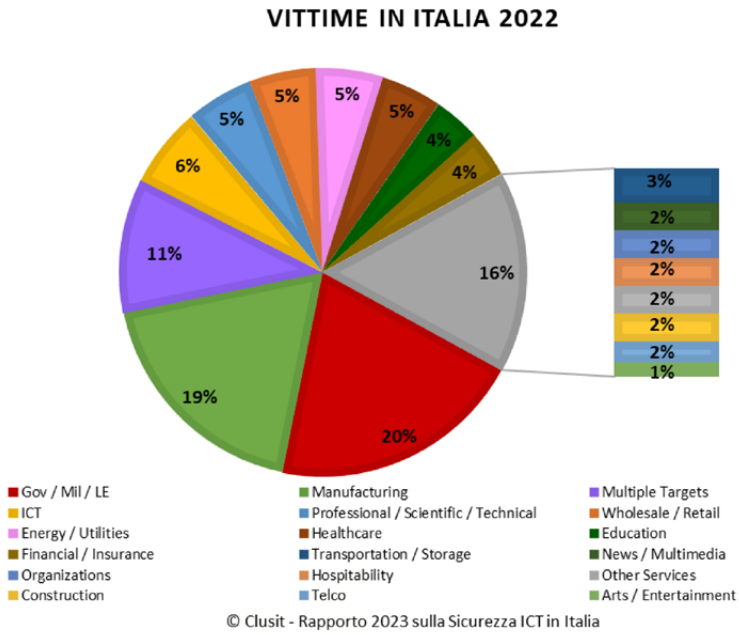


Fig. 27: *Distribuzione delle vittime in Italia nel 2022*

Se non è possibile sostenere, semplicemente guardando i dati, che i criminali guardino al nostro paese con maggiore interesse rispetto ad altri, è tuttavia evidente che la percentuale di successo delle loro attività in Italia sia ascrivibile tanto alle peculiarità del tessuto economico e sociale del Bel Paese, quanto ai fattori che influenzano l'evoluzione della digitalizzazione delle imprese e delle pubbliche amministrazioni.
L'accelerazione verso il digitale, forte dell'impulso dato dalla pandemia, ha infatti coinvolto mai come in questi ultimi tre anni le piccole e medie imprese italiane, che da questi dati risultano evidentemente impreparate a sostenere la crescente pressione dei cyber-attack.
A conferma di questo fatto, rispetto al 2021, si rileva un aumento del numero degli attacchi per tutte le aree merceologiche prese in esame, come dimostra una sempre più uniforme distribuzione del grafico a torta. Anche in questo caso, è d'obbligo sottolineare come **la magnitudine delle conseguenze per le vittime non sia correlata alla complessità degli attacchi stessi**.
Infatti, in coerenza con quanto avviene a livello globale, si ha la maggiore crescita percentuale anno su anno per la categoria "Multiple Targets" (**+900%**): si tratta di attacchi non mirati, campagne generalizzate che in Italia continuano a causare effetti consistenti.
Se guardiamo agli altri settori che più crescono in termini di incidenti anno su anno, ciò sembra riflettere quanto potremmo aspettarci dal grado di maturità tecnologica negli spe-

cifici ambiti: "Professional / Scientific / Technical" vede un incremento del **+233,3%** di incidenti gravi, "Manufacturing" **+191,7%**. Essendo tra le più colpite, è rilevante anche la crescita per le organizzazioni "ICT" (**+100%**) e "Gov / Mil / LE" (**+65,2%**).

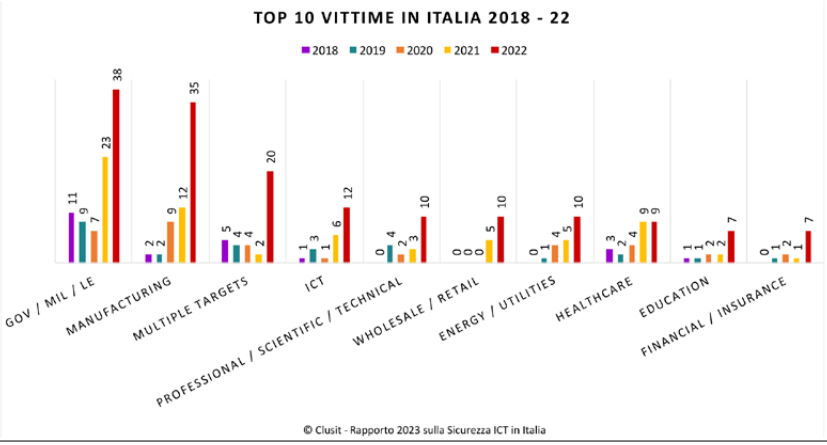


Fig. 28: *Top 10 vittime in Italia nel periodo 2018-2022*

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.

Il malware, come nel mondo, la fa da padrone, ma in Italia in modo decisamente più consistente (**53%, +6% rispetto al dato globale**). Si tratta di tecniche quasi sempre standardizzate, ormai frutto dell'*industria del cyber-crime* che, come abbiamo visto, è la matrice prevalente delle attività malevole nel nostro Paese. Ciò in parte conferma l'ipotesi precedentemente espressa per cui l'aumento degli attacchi in Italia sia con-causato da forti limiti nella capacità di difesa delle vittime. L'ulteriore conferma arriva dalla pressoché assenza in Italia della categoria *Multiple Techniques,* che da qualche anno nel nostro campione include gli attacchi più avanzati.
Rassicura solo in parte (poiché non può che confermare quanto detto sopra) il dato degli attacchi di tipo phishing e di ingegneria sociale, che in Italia risulta incidere in maniera minore rispetto al resto del mondo (**8% sul 12% globale**), mentre resta preoccupante la percentuale di incidenti basati su vulnerabilità note, se non altro perché, come diciamo ormai da anni, questa categoria potrebbe facilmente scomparire dal campione se le organizzazioni si dotassero di efficaci processi di gestione delle vulnerabilità e degli aggiornamenti di sicurezza. Non va comunque male come nel resto del mondo, in quanto nello stivale il dato si attesta percentualmente alla metà (**6% rispetto al 12% globale**).

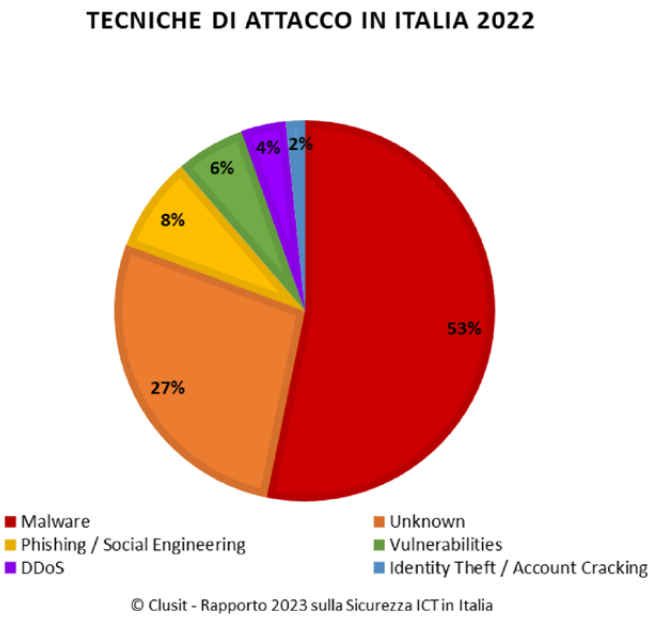


Fig. 29: *Tecniche di attacco in Italia nel 2022*

I DDoS crescono in misura minore e si mantengono pressoché stabili rispetto agli anni precedenti (**4% in linea con il dato globale, vs. 6% dell'anno precedente**), come confermato anche dai dati Italiani presenti in altri contributi del Rapporto (analisi Fastweb). Siamo diventati più bravi a proteggerci da questa tecnica? Chi ha le capacità economiche, le competenze per farlo, i razionali di business e i driver normativi, certamente sì. Resta, tuttavia, vero che sono gli stessi criminali a preferire ormai altre tecniche di attacco che consentono un minor impegno "pro-capite" per fare abbondanti raccolte di riscatti, come per l'appunto le campagne malware.
Residuale è il furto di identità **(2% vs. 3% del dato globale)** che evidentemente non costituisce più un elemento preferenziale di innesco delle azioni di hacking, di nuovo in linea con la considerazione che gli attacchi gravi che rientrano nel nostro campione siano per lo più frutto di attività criminali *industrializzate* e fortemente *automatizzate*. Non possiamo dire che il fenomeno del furto di identità e di credenziali non sia rilevante nel nostro paese: come testimoniano altre fonti[1], 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.

[1] https://barbaraganz.blog.ilsole24ore.com/2023/02/16/piccole-imprese-e-attacchi-informatici-colpite-4-su-10-le-contromisure/

Infine, di particolare rilievo è l'assenza, rispetto al dato globale, di un numero statisticamente rilevante di "web based attack". Sempre tenendo conto l'elevata quantità di situazioni dove non è possibile identificare la tecnica primaria dell'attacco (**Unknown, 27%** rispetto al 24% nel mondo), tali attacchi sono certamente presenti, ma ancora in quantità limitata. 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

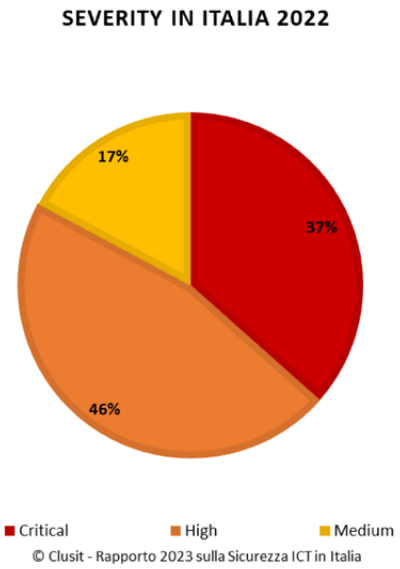


Fig. 30: *Severity degli attacchi in Italia nel 2022*

Dal punto di vista della severity degli attacchi, il dato italiano è sostanzialmente allineato a quello internazionale.

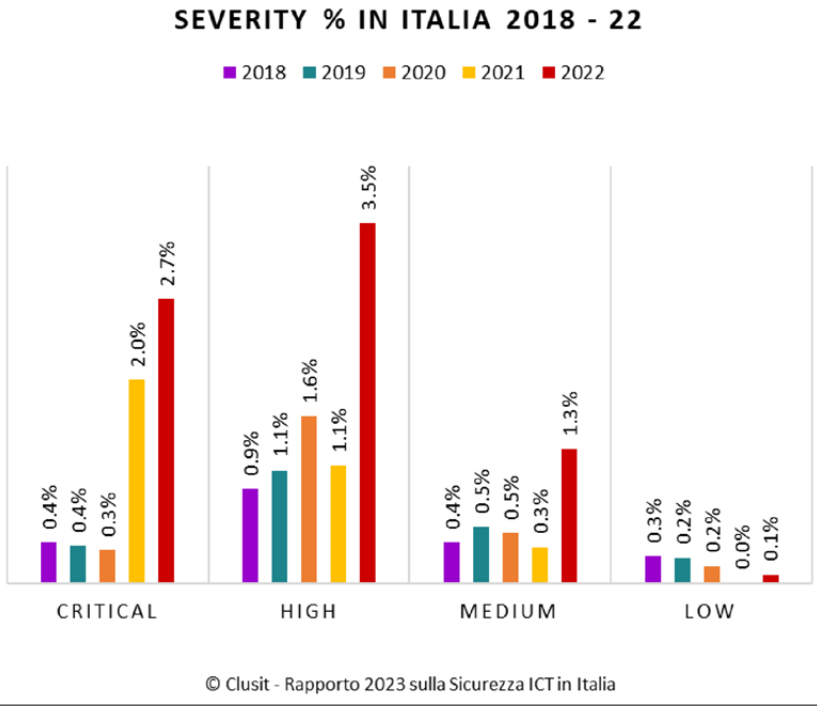


Fig. 31: *Severity degli attacchi in Italia nel periodo2018-2022*

Guardando alla progressione storica, è possibile notare un progressivo aumento della Severity degli attacchi, (+2,7% di attacchi Critical, +2,4% High, +1% attacchi Medium) rispetto al 2021. La serie storica italiana resta in ogni caso peggiore rispetto al dato globale, dove si registra un numero maggiore di attacchi con severità media e bassa.
Considerando che in molti casi gli attacchi non differiscono dal punto di vista tecnico o sono realizzati dagli stessi gruppi di cybercriminali, la vittima italiana sembra subire mediamente conseguenze più consistenti rispetto al resto del mondo.
Possiamo sperare che la crescita sul mercato dei servizi di SOC e l'attenzione apportata dalle istituzioni, in primis l'Agenzia per la Cybersicurezza Nazionale, al tema della gestione degli incidenti e delle crisi, stiano sostenendo il riallineamento del dato italiano a quello internazionale. D'altro canto, gli eventi a maggiore gravità costituiscono ancora una percentuale troppo elevata (81% complessiva tra le Severity Critical e High) per dire che questo percorso sia stato portato a compimento.

Analisi degli attacchi alle organizzazioni governative e alle pubbliche amministrazioni

"La digitalizzazione aumenta nel suo complesso il livello di vulnerabilità della società da minacce cyber, su tutti i fronti (ad es. frodi, ricatti informatici, attacchi terroristici, ecc.). Inoltre, la crescente dipendenza da servizi "software" (e la conseguente esposizione alle intenzioni degli sviluppatori/proprietari degli stessi) e l'aumento di interdipendenza delle "catene del valore digitali" (PA, aziende controllate dallo Stato, privati) pongono ulteriore enfasi sulla significatività del rischio in gioco e sull'esigenza, quindi, di una risposta forte."

Quello che precede è un estratto dal Piano Nazionale di Ripresa e Resilienza[2], la cui implementazione è ancora, nel 2022, alle fasi iniziali. Per questo motivo, abbiamo ritenuto importante introdurre per quest'anno un'analisi verticale della situazione globale del settore delle organizzazioni governative e delle pubbliche amministrazioni sia centrali che locali (escluso il comparto difesa) sperando che una fotografia in tal senso della situazione attuale possa essere da sprone per il rapido indirizzo degli investimenti che, come vedremo, hanno ormai carattere di urgenza.

Analisi dei principali cyber attacchi noti a livello globale del 2018-2021 e del 2022

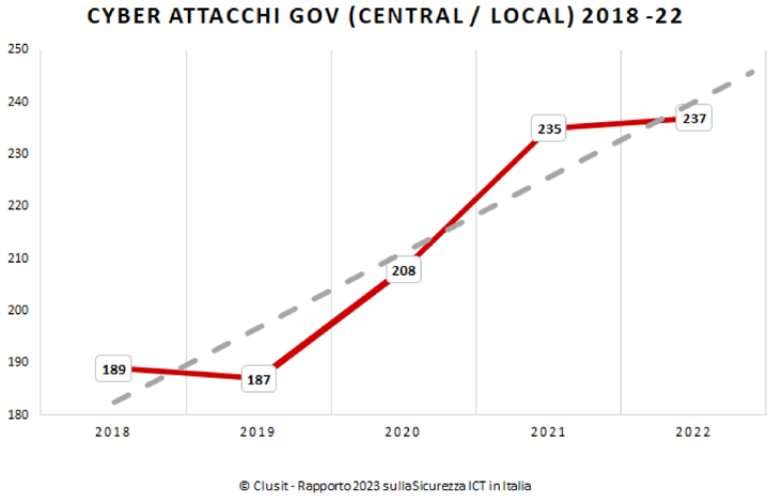


Fig. 32: *Attacchi al settore GOV (CENTRAL/LOCAL) nel periodo 2018-2022*

[2] https://www.italiadomani.gov.it/content/dam/sogei-ng/documenti/PNRR%20Aggiornato.pdf

Tra il 2018 e il 2022 il campione ha incluso 1.056 attacchi noti di particolare gravità che hanno coinvolto realtà governative nel mondo. Dopo una crescita particolarmente significativa fra il 2019 e il 2021, il numero di attacchi gravi è rimasto pressoché costante nel 2022. Nell'arco dei cinque anni si è comunque passati dai 189 attacchi del 2018 ai 237 del 2022, con un incremento complessivo del 25%.

Distribuzione degli attaccanti per tipologia

La stragrande maggioranza degli attacchi condotti verso il settore pubblico, ben due terzi, è relativa alla categoria **"Cybercrime"**, con il 67% degli attacchi; seguono, molto distaccati ma quasi a pari merito **"Espionage/Sabotage"** e **"Hacktivism"**, rispettivamente al 13% e 12%, e infine **"Information Warfare"** al 8%.

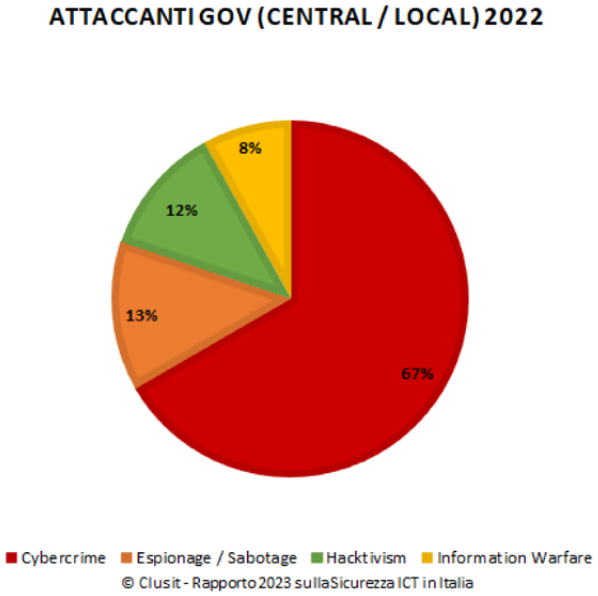


Fig. 33: *Distribuzione degli attaccanti al settore GOV (CENTRAL/LOCAL) nel 2022*

Il dettaglio dell'evoluzione negli ultimi anni degli attacchi verso il settore pubblico ci mostra uno spaccato interessante: nel 2022 infatti gli attacchi di matrice criminale sono significativamente diminuiti rispetto al 2021 (-21%) mentre sono cresciuti quelli riconducibili a tutte le altre tipologie di attaccanti; addirittura, gli attacchi di matrice ideologica (Hacktivism) di gravità tale da rientrare nel nostro campione, sono passati da uno solo del 2021 a ben 28 del 2022. Questo andamento in apparente controtendenza è evidentemente conseguenza della situazione sorta attorno al conflitto tra Russia e Ucraina, che ha spinto molti attivisti a

colpire le organizzazioni governative, anche quelle di Paesi non direttamente coinvolti nella guerra, con attacchi dimostrativi e di supporto verso l'una o l'altra parte.

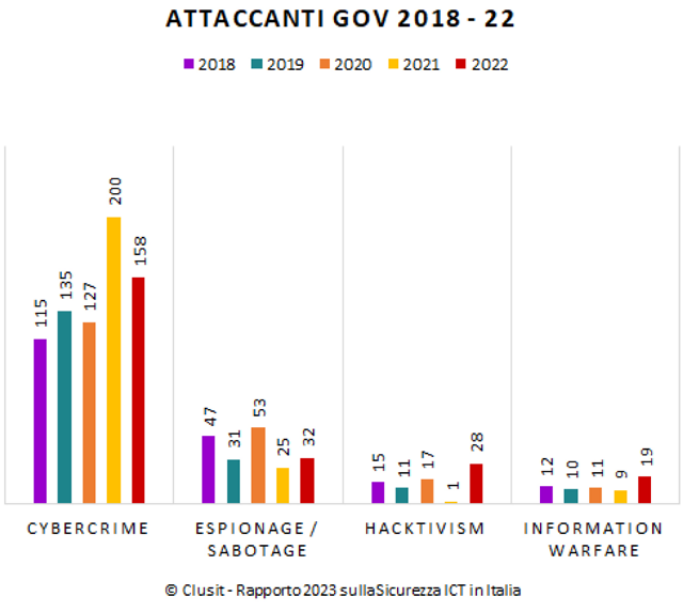


Fig. 34: *Distribuzione degli attaccanti per il settore GOV (CENTRAL / LOCAL) nel periodo 2018-22*

Distribuzione generale delle vittime per area geografica

La distribuzione geografica delle vittime vede l'Europa e il continente americano perfettamente in parità, una situazione del tutto inedita perché storicamente la distribuzione era sempre stata sbilanciata verso l'altro lato dell'oceano. Nel 2022 invece sia il vecchio che il nuovo continente subiscono ciascuno il 43% degli attacchi globali diretti verso il settore governativo, con l'Asia distaccatissima all'11%, l'Oceania al 2% e un rimanente 1% costituito da attacchi diretti verso bersagli multipli.

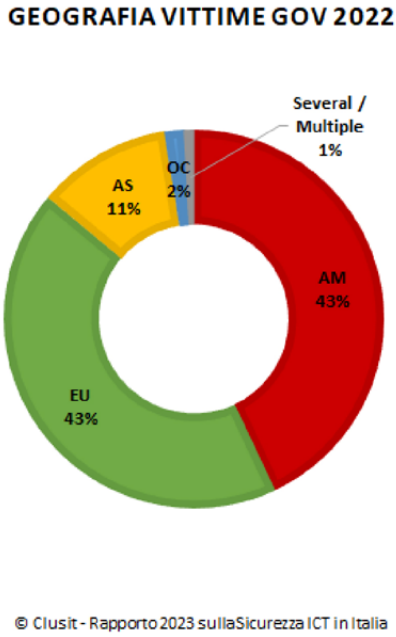


Fig. 35: *Distribuzione geografica delle vittime nel settore GOV (CENTRAL / LOCAL) nel 2022*

È interessante notare, come si vede dal grafico successivo, che questo ribilanciamento nella distribuzione geografica delle vittime è avvenuto nel corso degli ultimi tre anni: quindi, almeno per quanto concerne le organizzazioni governative e le pubbliche amministrazioni, lo spostamento degli attacchi in Europa non è solo frutto del recente conflitto rosso-ucraino ma è un fenomeno iniziato da tempo.

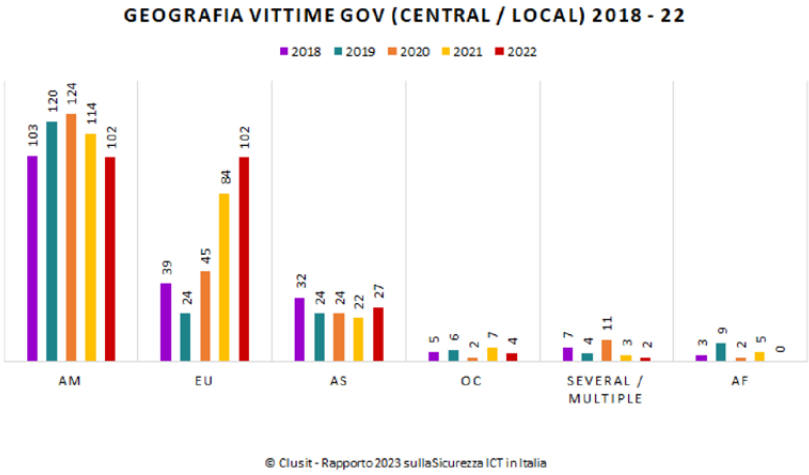


Fig. 36: *Distribuzione geografica delle vittime nel settore GOV (CENTRAL / LOCAL) nel periodo 2018-22*

Distribuzione delle tecniche di attacco

Per quanto riguarda le tecniche utilizzate, oltre un terzo degli attacchi (**34%**) è basato su malware, ma per più di un quarto (**27%**) la modalità non è nota o non è stata accertata; molto distaccati risultano gli attacchi basati sul Distributed Denial of Service (**12%**), sullo sfruttamento di vulnerabilità tecniche note (**9%**) e sul social engineering (**5%**).
Confrontando questi dati con quelli di tutti gli attacchi globali notiamo una assai minore incidenza del social engineering, segno forse che le organizzazioni governative stanno diventando più attente rispetto alla media, ed invece una maggiore incidenza del DDoS che è lo strumento tipico degli attacchi dimostrativi/ideologici quali sono quelli tipicamente condotti verso le organizzazioni governative.

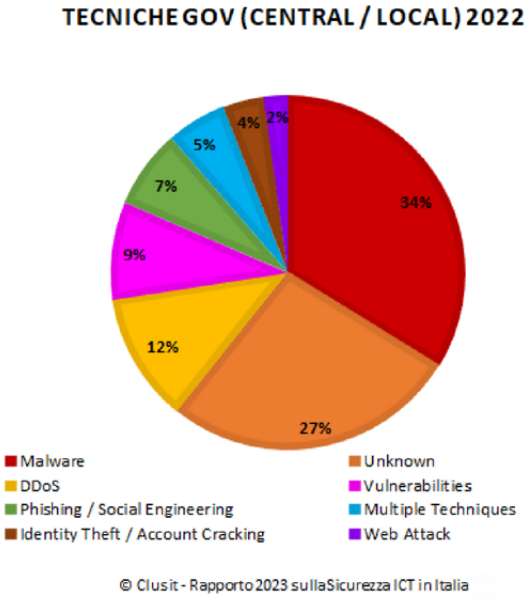


Fig. 37: *Distribuzione delle tecniche di attacco nel settore GOV (CENTRAL / LOCAL) nel 2022*

Il dato più caratteristico che si nota esaminando l'evoluzione nel tempo delle tecniche d'attacco è la notevole crescita del DDoS in questo ultimo anno: si è infatti passati dai soli 7 attacchi significativi nel 2021 ai ben 28 del 2022. Ciò si inquadra perfettamente nel contesto geopolitico dell"ultimo anno, nel quale il conflitto russo-ucraino ha provocato un'ondata di attacchi ideologici condotti verso le organizzazioni governative mediante lo strumento del Denial of Service, tra i più efficaci per generare conseguenze mediaticamente rilevanti tramite l'interruzione di servizi di pubblica utilità. Contestualmente sono diminuiti gli attacchi basati su malware e sullo sfruttamento delle vulnerabilità, mentre le altre tipologie di attacco sono rimaste sostanzialmente costanti.

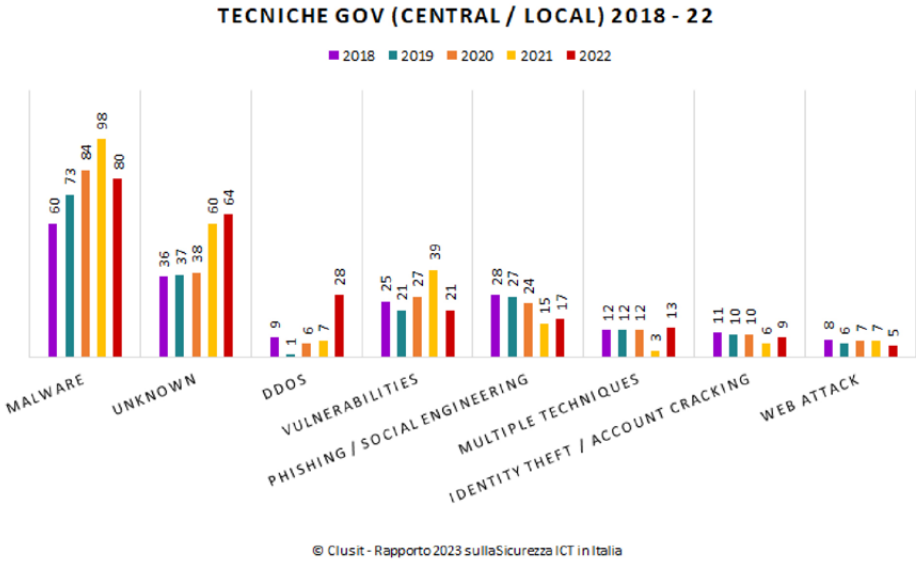


Fig. 38: *Distribuzione delle tecniche di attacco nel settore GOV (CENTRAL / LOCAL) nel periodo 2018-22*

Analisi della "Severity" degli attacchi

Gli attacchi condotti verso il settore pubblico, come si vede dal grafico, sono caratterizzati da una Severity assai maggiore rispetto all'insieme di tutti gli attacchi: ben il 56% è infatti classificato come **critico**, contro il 36% del dato globale, e il 36% è classificato **alto** contro il 44% del dato globale. Sembra quindi che chi attacca il settore pubblico sia assai più preparato, motivato ed efficace nelle sue azioni, puntando ad ottenere impatti decisamente più elevati della media: di fatto solo il 5% degli attacchi condotti con successo ha impatto basso, mentre il 95% lo ha alto o critico, un dato davvero preoccupante.

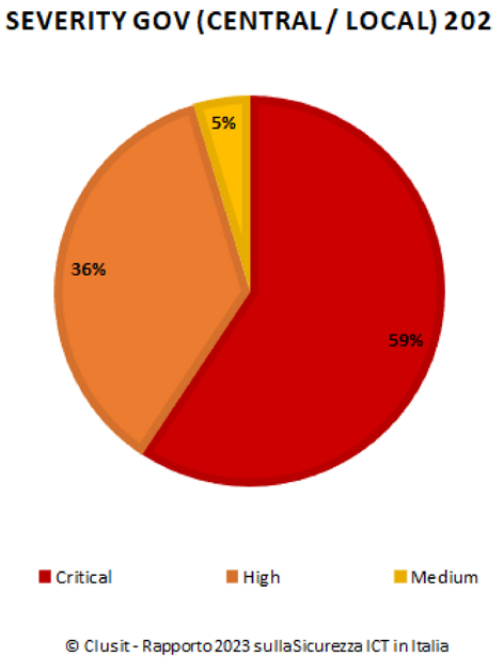


Fig. 39: *Distribuzione della Severity degli attacchi nel settore GOV (CENTRAL / LOCAL) nel 2022*

Il grafico evolutivo ci mostra che negli ultimi anni la Severity degli attacchi verso il settore pubblico è andata fortemente aumentando: nel solo 2022 gli attacchi critici sono aumentati del 31% passando da 107 a 140, mentre quelli ad alto impatto sono diminuiti del 21% passando da 108 a 85; conseguentemente, quelli a basso impatto sono diminuiti del 45% passando da 20 a 11. Anche in questo caso è interessante notare come tale tendenza non sia specifica dell'ultimo anno ma sia iniziata già due anni fa, nel passaggio dal 2020 al 2021, probabilmente a causa dell'impennata dell'utilizzo di tecnologie digitali a seguito della pandemia.

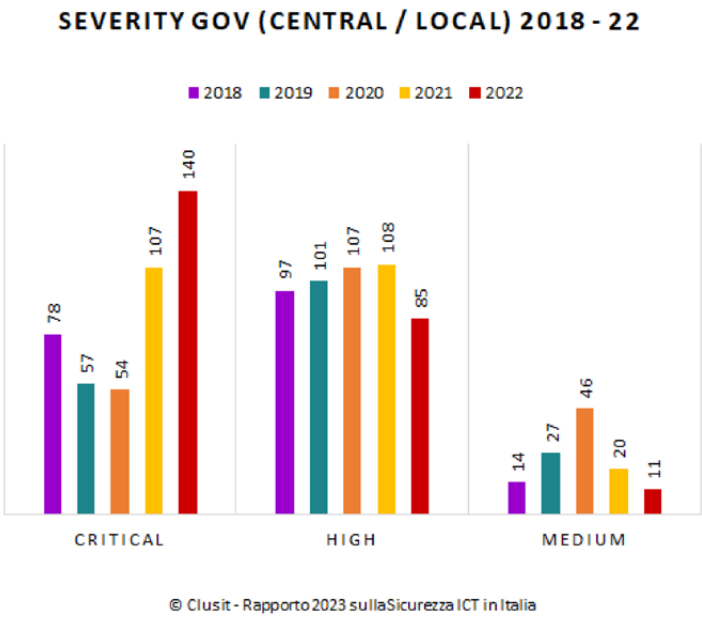


Fig. 40: *Distribuzione della Severity degli attacchi nel settore GOV (CENTRAL / LOCAL) nel periodo 2018-22*

Dall'analisi alla sintesi: dai trend alla strategia

L'obiettivo delle attività di analisi e raccolta dei dati che, come Clusit, facciamo all'interno di questo Rapporto, non è certo confermare anno su anno uno scenario a tinte fosche, quanto 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 fondamentale rafforzare la **governance dei processi di patch & vulnerability management**. Non è credibile immaginare uno sviluppo consistente della digitalizzazione, che passa attraverso la fiducia in particolare verso le infrastrutture governative, le pubbliche amministrazioni ed i servizi digitali ai cittadini, e allo stesso tempo assistere ad allarmi internazionali per campagne di attacco basate su vulnerabilità per le quali esistono aggiornamenti da oltre un anno[3].

[3] https://www.agendadigitale.eu/sicurezza/attacco-hacker-globale-forse-eccesso-di-allarme-ma-la-minaccia-cyber-resta-seria/

I penetration test triennali o annuali non sono più sufficienti in molti casi per sostenere di presidiare la tematica delle vulnerabilità tecniche. È necessario **ragionare in ottica di Continuous Vulnerability Management** (anche con soluzioni di PTaaS) supportate da processi **di patch management sempre più efficaci** ed a processi di reale **presidio 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 assimilabili al SOC nell'ambito delle applicazioni** su ogni elemento (servizi esposti, front end, middleware, applicazioni mobili, IoT).
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, e non solo nelle fasi di realizzazione, quando molte scelte sono state fatte e le possibilità di intervento si riducono. Questo approccio deve valere, ovviamente, per tutte le iniziative, da quelle architetturali a quelli di sviluppo o adozione di soluzioni, 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.

Allo stesso modo, la creazione e protezione delle copie di sicurezza dei dati è un requisito imprescindibile. 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 un'inadeguata gestione dei backup, strumento che esiste praticamente da quando esistono i computer.

Come poi è stato rilevato dall'analisi della Severity degli attacchi, ormai da anni assistiamo ad una crescita continua e per gradini periodici di quelli più gravi, nonostante anche in Italia (secondo i dati dell'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano) gli investimenti in sicurezza stiano crescendo.

Da un lato, probabilmente ciò può essere spiegato con il fatto che non basta aumentare in modo cieco gli investimenti. Molti sforzi andrebbero razionalizzati e, soprattutto in Italia, **andrebbe ridotta la micro-frammentazione di infrastrutture e servizi**.

Allo stesso modo, dobbiamo domandarci se i cambiamenti e le evoluzioni della rete (diffusione, utilizzo, consapevolezza) possano influenzare questi fenomeni, evitando di puntare l'attenzione solo su fattori che sono al di fuori del nostro controllo, come la continua evoluzione e crescita delle organizzazioni criminali. In questa ottica si ritengono estremamente significative iniziative come quella del Polo Strategico Nazionale e della strategia Cyber Nazionale. **Serve una governance più efficace, maggiore automazione e colmare lo skill gap di cui, in questo momento, il nostro mercato sta enormemente soffrendo**.

In tal senso, per il nostro Paese è altresì fondamentale che **siano colte le opportunità di investimento del PNRR, dando adeguata priorità agli aspetti di cybersecurity**, quanto meno contestualmente alle altre iniziative della c.d. Componente 1 della Missione di Digitalizzazione e Innovazione della PA, perché siano realizzate in modo sicuro *by design*.

Prioritario, in tale ambito, deve essere un cambio di passo non solo sulle iniziative tecnologiche e di governo: come individuato tra i *Flagship Program* del piano Next Generation EU della Commissione Europea, deve essere incentivato lo sviluppo del pillar "*Reskill and upskill*" con riguardo alle **competenze STEM** nell'ambito dell'Istruzione Tecnica Superiore e Universitaria.

Inoltre, considerato che in Italia l'80% degli attacchi si concentra nei due livelli più elevati di Severity, Critical e High, le iniziative istituzionali dovranno essere sostenute anche dalle singole imprese e pubbliche amministrazioni, tramite la **costituzione / evoluzione di processi adeguati di monitoraggio della sicurezza, incident management, crisis management, e servizi SOC**, tra gli altri.

Nell'ambito delle imprese, tali iniziative dovranno interessare in modo più esteso rispetto al passato tutti i settori merceologici, non solo quelli su cui si osserva la maggiore crescita della pressione dei cyber-attack (sebbene in questi si ritrovi un numero consistente delle aziende del *Made in Italy* , come "Manufactoring" e "Professional / Scientific / Technical" per citarne alcune, alla base della nostra economia).
Non importa infatti la singola percentuale, quanto il fatto che non ci sia settore o compartimento che si possa ritenere esente rispetto al problema. In un mondo in cui, nel 2023, alcune organizzazioni hanno rispetto alla cyber security ancora un approccio basato sul "per quel che faccio io chi vuoi che mi attacchi", è un dato fondamentale per comprendere come ogni organizzazione debba avere la sua specifica strategia di contrasto agli attacchi e di contenimento degli incidenti. È necessario pertanto un cambio di passo nell'approccio alla cybersecurity, **guidato non più (solo) da driver normativi, ma da processi di valutazione e gestione del rischio per il business,** atti a calibrare adeguatamente gli investimenti sulla base delle reali necessità; Non può essere un caso che in Italia, **i settori in cui maggiormente crescono gli attacchi, siano quelli che ad oggi sono meno impattati da normative generali e settoriali contenenti prescrizioni sulla sicurezza delle informazioni**.

Infine, in riferimento al dato nazionale, esiste poi un fitto sottobosco di situazioni ben approfondite nelle analisi dei successivi capitoli del Rapporto, come, ad esempio, il contributo della Polizia Postale e delle Comunicazioni a cui si rimanda la lettura. Si tratta di tutti quegli eventi che interessano i singoli cittadini e le PMI; sebbene siano incidenti che, presi singolarmente, non possono avere il carattere di pubblicità ed evidenza mediatica tale da rientrare nelle statistiche della presente analisi, il fenomeno sta tuttavia assumendo un

grado di estensione che diventa sempre più preoccupante: solo nella provincia di Milano, nel 2022, il numero di denunce per truffe e frodi informatiche per numero di abitanti è secondo solo a quelle relative ai furti tradizionali[4]. 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**.

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. Per valutare il valore dei dati raccolti e delle analisi effettuate, è necessario chiedersi prima di tutto quali siano le modalità di raccolta e di analisi, e quali quindi i limiti dei risultati ottenuti.

I dati riportati si riferiscono ad incidenti riportati in fonti di informazione pubbliche. Da quando, nel 2012, 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.

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

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

Nel campione di questa analisi sono certamente meglio rappresentati gli attacchi realizzati per finalità cyber criminali o di hacktivism rispetto a quelli derivanti da attività di cyber espionage, che tendono ad essere condotti con grande cautela e pertanto emergono più difficilmente. Questo può essere un limite importante da considerare: gli attacchi che colpiscono la riservatezza dei dati sono sicuramente sottorappresentati perché, a meno che gli attaccanti per qualche motivo pubblichino l'informazione, le stesse organizzazioni colpite potrebbero non averne evidenza. Si tratta di *known unknown* rispetto ai quali è difficile avere dati statisticamente significativi. Anche venendone a conoscenza, le organizzazioni colpite potrebbero avere interesse a non darne evidenza a nessuno. Un tema analogo è legato alle attività di information warfare, che possono essere condotte con altrettanta cautela, anche per non esporre gli strumenti utilizzati[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 per la maggior parte degli attacchi di grandi dimensioni, con una sottostima difficile da quantifi-

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

care 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.

L'analisi Fastweb della situazione italiana in materia di Cyber-Crime

Introduzione

Fastweb conferma il proprio impegno nel contribuire a fotografare la situazione del cybercrime in Italia attraverso un'analisi puntuale dei principali trend, elaborata dal proprio Security Operation Center (SOC) attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica. Grazie al recente ampliamento dell'operatività del SOC, con l'espansione delle attività di sicurezza informatica anche presso la sede di Bari, Fastweb offre un monitoraggio sempre più dettagliato dei fenomeni cyber oltre ad un supporto continuativo su tutte le reti dei clienti.
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 oltre 56 milioni di eventi di sicurezza, un aumento del 25% rispetto agli eventi rilevati nel Report 2021.

In generale, i fenomeni e gli effetti legati al cybercrime osservati nel 2022 sono, per la maggior parte, in continuità con quanto visto nel 2021. Si continua ad osservare come, all'avanzare degli attacchi informatici si contrappone una sempre maggiore efficacia delle misure di difesa, grazie anche ad una progressiva consapevolezza da parte delle aziende rispetto ai rischi informatici e i conseguenti investimenti indirizzati verso tecnologie e servizi nell'area Security. Infatti, nonostante l'intensificarsi degli eventi di sicurezza e l'elevata diversificazione delle tecniche di attacco, nel 2022 le rilevazioni rispetto agli effetti dannosi di questi eventi sono rimaste pressoché invariate. A dimostrazione di ciò, sono state rilevate significative diminuzioni nel numero di attacchi Ddos (-25% degli eventi ad alto impatto rispetto al 2021), dei servizi critici esposti su internet (-9%) e del numero di malware (-4%). Quest'ultimo dato, in particolare, è legato al rafforzamento del livello di cyber-resilienza delle aziende, in quanto, nonostante un deciso aumento delle famiglie di malware (+22%), si registra un numero inferiore di attacchi.

La sempre più ampia diffusione di forme di lavoro flessibile e il maggior utilizzo di strumenti digitali ha messo le imprese e la pubblica amministrazione di fronte alla necessità di gestire con attenzione la sicurezza dei propri sistemi informativi, a cui i dipendenti accedono sempre più in maniera remota e distribuita. Questa maggiore attenzione è stata sostenuta dalla diffusione di programmi strutturati di formazione e awareness, a cui la stessa Fastweb ha contribuito nel panorama italiano con i corsi erogati dalla Fastweb Digital Academy (FDA) e con nuove soluzioni per la formazione e l'identity management dei dipendenti delle aziende con i servizi FastCoach e Fast Security VPN.
Entrando più nel dettaglio dei trend 2022 della cybersecurity, sul fronte degli attacchi DDoS (Distributed Denial of Service) sono stati rilevati circa 1.800 eventi significativi e circa 20.000 anomalie riconducibili a possibili attacchi diretti contro i clienti Fastweb.

Il dato mostra una decisa diminuzione rispetto al 2021 (-25%); si riconferma, quindi, il trend visto l'anno precedente di diminuzione degli attacchi DDoS dopo i picchi gestiti nel 2020. I settori più colpiti sono ancora Finance/Insurance e Pubblica Amministrazione, che insieme costituiscono oltre il 55% dei casi. L'aumento più significativo è quello del settore dei Service Provider, cresciuto dal 3% del 2021 a quasi il 16% del 2022.
Inoltre, nel 2022 sono stati rilevati più di 41.000 server e device privi di livelli minimi di protezione e quindi esposti a rischi in rete. Il numero è in costante diminuzione ormai dal 2019, con un trend in decrescita tra 2022 e 2021 pari al 9%.

Infine, si osserva una lieve flessione nel volume di malware e botnet (-3% rispetto al 2021) con, al tempo stesso, un deciso incremento delle famiglie di software malevoli (+22% rispetto all'anno precedente). Tra queste minacce, prioritaria risulta "downadup" con il 33% delle rilevazioni totali: questi virus sfruttano falle di Windows per prendere il controllo della macchina e rubare informazioni e credenziali agli utenti ignari. Significativa la diminuzione della quantità di famiglie di malware e botnet sconosciute (-49% rispetto al 2021), a riprova di una maggiore resistenza degli strumenti di difesa sul mercato.
In assoluta continuità rispetto all'anno precedente risulta la distribuzione geografica dei centri di controllo dei malware, con infezioni controllate da server ospitati in Europa sempre più numerosi rispetto a quelli dislocati negli Stati Uniti.
Per quanto riguarda la vista sui tentativi di attacco applicativo, cioè ai software dei dispositivi e diretti contro i clienti Enterprise Fastweb (grandi aziende e pubblica amministrazione), nel 2022 SQL Injection rimane il primo in termini di utilizzo. Questa tipologia di attacco è diretta ad avere accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database. Si osserva, una netta diminuzione delle attività di information gathering, anche per l'implementazione di blocchi su base geografica, contromisura che è stata applicata in maniera massiccia dalle aziende, subito a valle degli eventi che hanno indirizzato i nuovi equilibri geopolitici in Est Europa.

In continuità con il report 2021, Fastweb ha monitorato anche le minacce afferenti ai servizi Mail che, anche nel 2022, sono cresciute in termini di volume. Il fattore principale utilizzato per veicolare attacchi rimane l'utilizzo di URL malevoli (92% dei casi, +5% rispetto al 2021). Tra le nuove tecniche utilizzate dai cybercriminali, il whaling phishing (attività relativa a campagne fraudolente ai danni di figure apicali di grandi aziende) risulta tra le preferite dai cyber-criminali. Il panorama di minacce è cambiato rispetto al 2021: le rilevazioni mostrano come malware che erano minoritari nel 2021 sono aumentati a tal punto da risultare prioritari nel 2022; questo dimostra una forte dinamicità da parte del mondo del cybercrime, che tenta di sorprendere le vittime con un parco di attacchi sempre diverso (come i threat actor Mummy Spider e Hastur). Tra le diverse minacce alcune iniziano a utilizzare l'intelligenza artificiale e il machine learning per aumentare i danni degli attacchi, rendendoli sempre più efficaci.

Per quanto concerne i fenomeni fraudolenti che sfruttano il servizio gli SMS, il cosiddetto fenomeno dello smishing, nel 2022 sono in forte aumento gli attacchi che comportano una potenziale perdita di dati per gli utenti. Come nel 2021, si riscontrano tra i principali fenomeni di frodi, la sottoscrizione con furto di identità e il PBX hacking (legato alle vulnerabilità dei centralini per la generazione di traffico verso numerazioni ad alto costo).
In conclusione, le rilevazioni di Fastweb del 2022 hanno rilevato in continuità con il 2021 un aumento generalizzato degli attacchi informatici e la forte consapevolezza del tema della sicurezza cibernetica, anche legata alla situazione geopolitica attuale, che ha portato ad un innalzamento della soglia di attenzione da parte di aziende e utenti. Il trend osservato dopo la pandemia, quindi, continua anche quest'anno, diventando strutturale. Significativi aumenti di investimenti in ambito Security portano ad una dimostrata riduzione delle conseguenze più dannose degli attacchi.
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 2022 è rimasto pressoché stabile rispetto all'anno precedente, con una leggera flessione del -2,5%. Al contrario, quest'anno, le famiglie di software malevoli individuate rispetto allo scorso anno è cresciuto notevolmente, invertendo il trend registrato nel 2021: 208 famiglie rispetto alle 163 del 2021 (+21,6%), in linea con il dato del 2020 (220 categorie).

Come si può vedere nel grafico di **Fig. 1**, a differenza del 2021, dove si è registrato un trend di rilevazione crescente del numero di dispositivi infetti durante l'anno (linea grigia), nel 2022 le rilevazioni hanno mostrato un'inversione di tendenza (linea arancio).

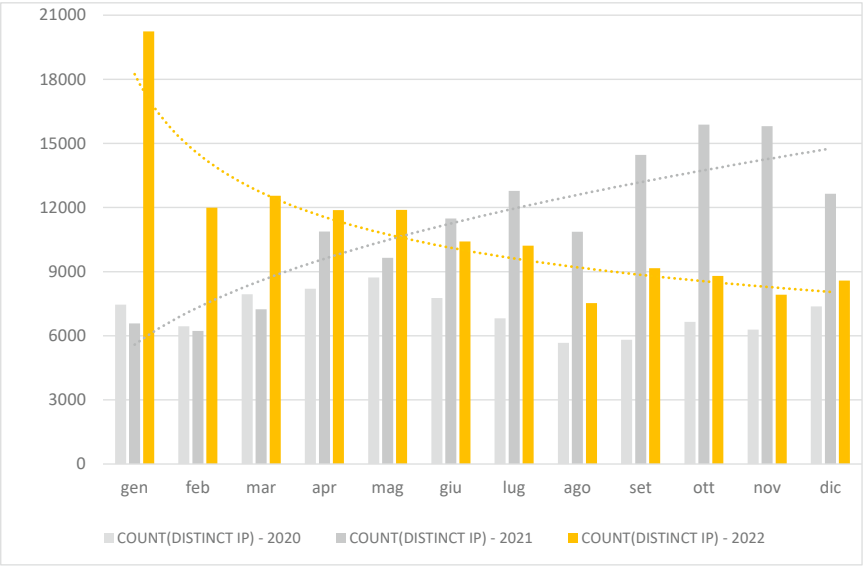


Figura 1: *Distribuzione temporale del numero di infezioni rilevate (Dati Fastweb relativi agli anni 2020, 2021 e 2022)*

La famiglia di malware "downadup" (conosciuta anche come "conficker") nel 2022 supera in valore assoluto quella di avalanche-andromeda, con rilevazioni pari al 33% 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. Passa al secondo posto 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 marzo ritorna in maniera significativa QSnatch. Questo malware ha iniziato ad essere presente a fine 2019 e durante tutto il 2020; sparito a fine 2021, ha avuto un forte impatto raggiungendo addirittura il 10% delle minacce riscontrate. Il malware, diffondendosi sulle unità NAS (network-attached storage), prende il controllo completo del dispositivo ed è in grado di bloccare patch e aggiornamenti software.

Continua il trend positivo di diminuzione delle infezioni causate da malware appartenenti a famiglie sconosciute, con una diminuzione rispetto al 2021 di circa la metà, a sottolineare una maggiore capacità di rilevazione da parte dei vendor di tecnologia di sicurezza e degli esperti del settore.

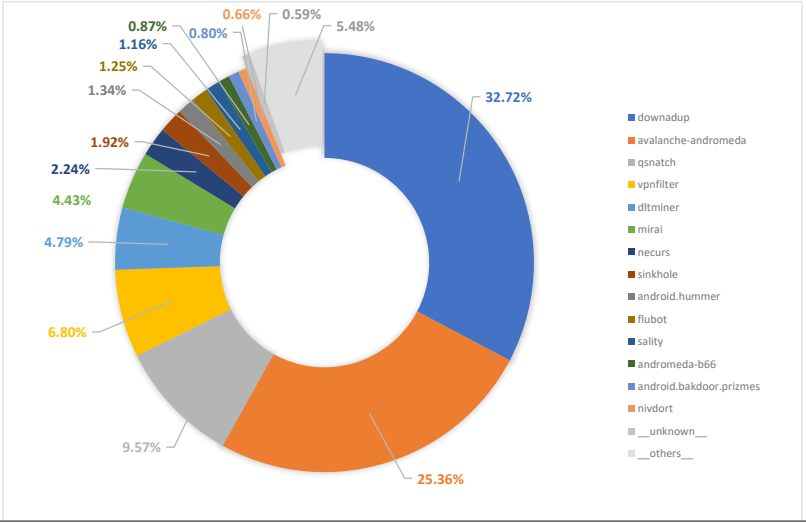


Figura 2: *Analisi delle infezioni rilevate (Dati Fastweb relativi all'anno 2022)*

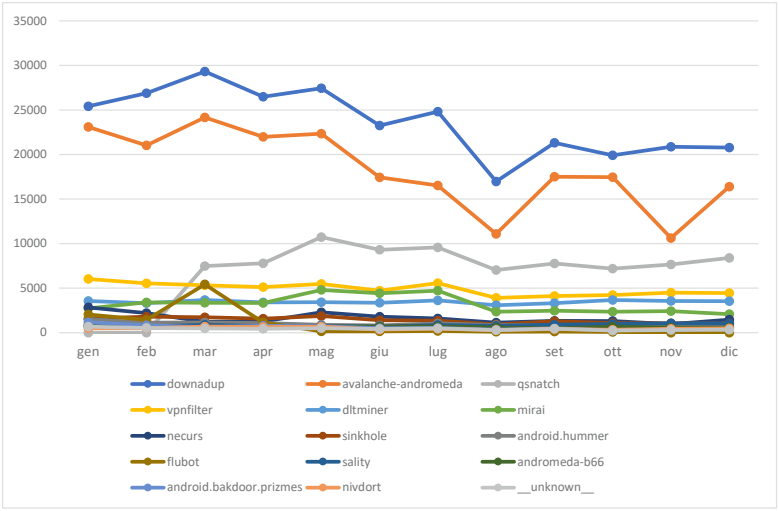


Figura 3: *Rilevazione mensile dei Malware (Dati Fastweb relativi all'anno 2022)*

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 2022 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 2021, la distribuzione geografica è rimasta pressoché invariata.

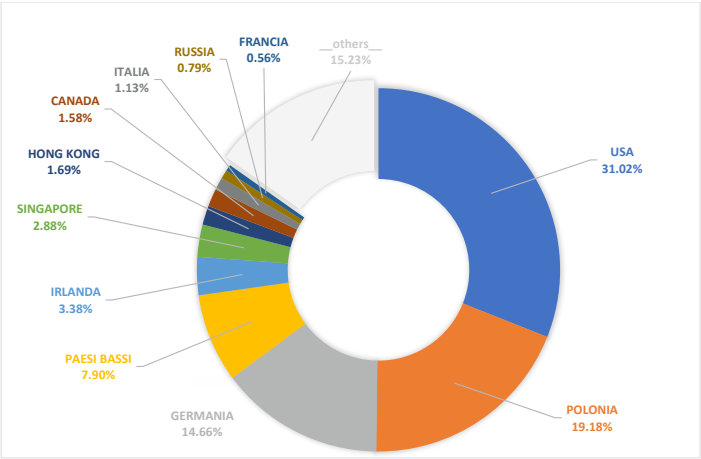


Figura 4: *Dislocazione dei centri di Comando e Controllo (Dati Fastweb relativi all'anno 2022)*

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 5-10$ mese per botnet in grado di erogare un attacco di 5-10 minuti ad oltre 100Gbps.
Durante tutto l'anno 2022 sono stati rilevati circa di 1.800 eventi di impatto importante e 20.000 anomalie riconducibili a possibili attacchi DDoS diretti verso i clienti Fastweb. Questa distinzione si basa sulla probabilità di causare un effetto negativo rilevante all'organizzazione target dell'attacco.
A livello di numerosità dei casi significativi, prosegue il trend discendente, dopo l'aumento registrato nel 2020 a seguito dei forti cambiamenti nel mondo del digitale introdotti dalla pandemia: rispetto al 2021, si registra un -25,4%. In controtendenza le anomalie a basso impatto, che sono cresciute del 11% rispetto al 2021, che rimangono comunque estremamente più basse in totale rispetto al dato del 2020 (circa 36.300 anomalie rilevate).

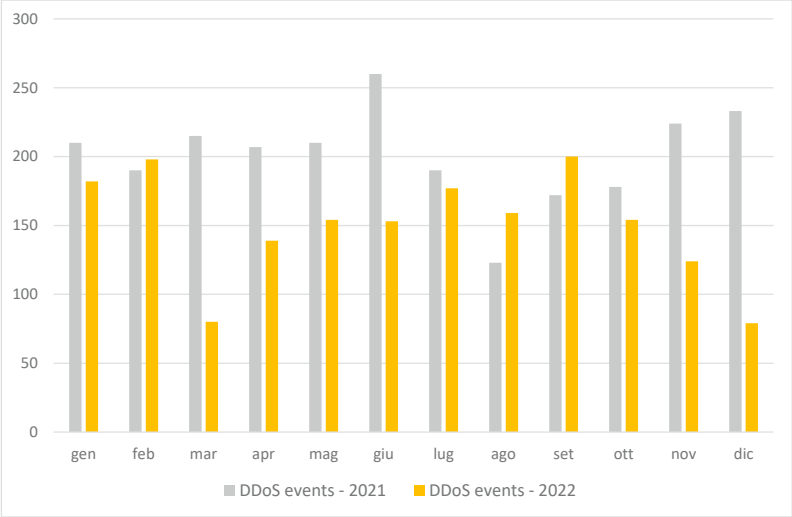


Figura 5: *Distribuzione mensile delle anomalie DDoS (Dati Fastweb relativi agli anni 2021 e 2022)*

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, 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 55% dei casi, con un aumento significativo rispetto al 2021 (dove entrambe le categorie superavano di poco il 50%). Dato interessante riguarda il settore dei service provider, cresciuto dal 2,7% del 2021 a quasi il 16% nel 2022, con un aumento che lo porta al terzo posto. I settori gambling e retail cambiano tendenza rispetto al 2021, nel quale erano cresciute significativamente, per tornare a livelli più simili al 2020.

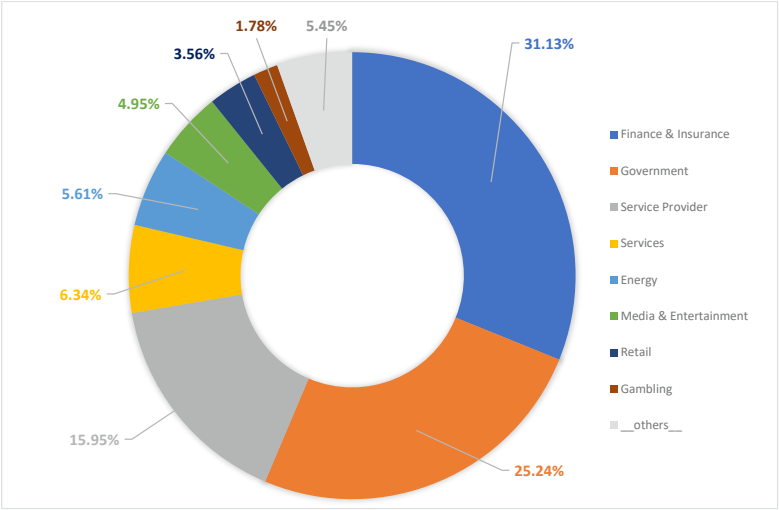


Figura 6: *Target di possibili attacchi DDoS (Dati Fastweb relativi all'anno 2022)*

Di seguito viene riportata la distribuzione della banda media in Gbps di un attacco DDoS nel 2022.

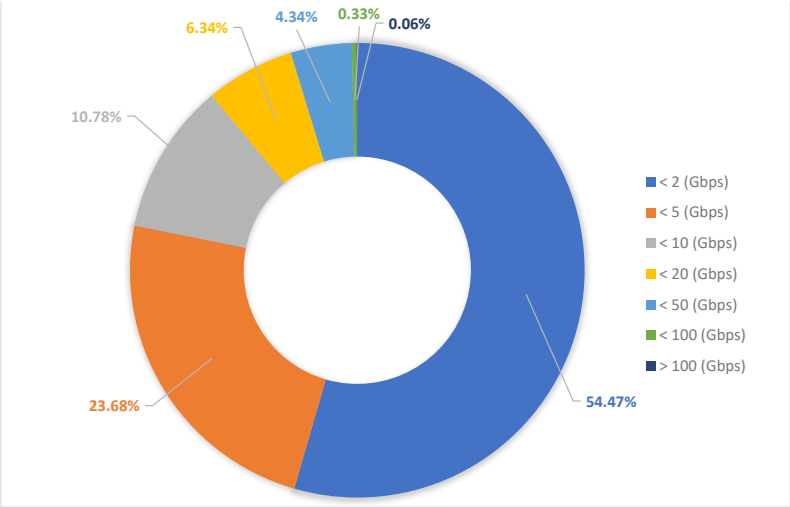


Figura 7: *Distribuzione della dimensione di un attacco DDoS (Dati Fastweb relativi all'anno 2022)*

Nel corso degli anni, l'aumento di consapevolezza rispetto alle tematiche di cybersecurity, unito alla maggiore efficacia delle tecniche di difesa, hanno portato ad una diminuzione significativa della durata degli attacchi. Anche quest'anno il trend continua, dimostrando come ad una crescente consapevolezza da parte delle vittime degli attacchi si leghino maggiori investimenti per garantire alla propria azienda la protezione da attacchi di tipo DDoS. Nel 2022, si è osservato che quasi il 93% degli attacchi è durato meno di 1 ora, con un forte miglioramento rispetto al 2021, dove il 97% degli attacchi durava quasi 3 ore. I rimanenti casi sono principalmente riconducibili a diversi tentativi effettuati in sequenza ravvicinata. È importante evidenziare che solo una parte minoritaria degli attacchi (1,07%) ha una durata di oltre 24 ore consecutive.

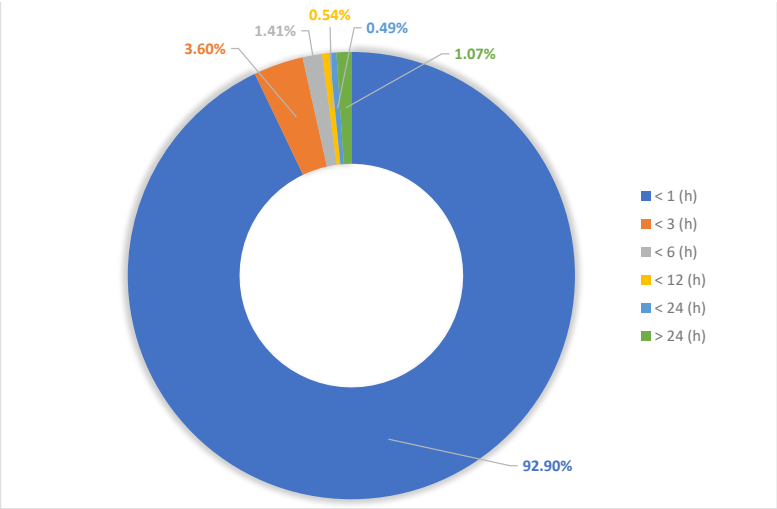


Figura 8: *Durata dei possibili attacchi DDoS (Dati Fastweb relativi all'anno 2022)*

Nel 2022 le tre principali tipologie di attacco DDoS, che sono anche le più critiche per le aziende, si confermano essere "NTP amplification", che sale dal 26,7% al 28,9%, DNS amplification" (dal 8,9% al 14,73%) e "IP Fragmentation" (dal 10,2% al 3,1%).
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.

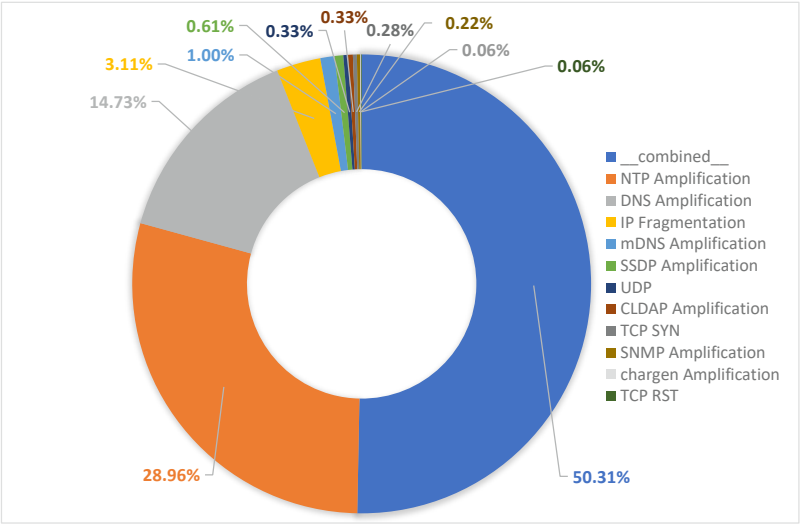


Figura 9: *Tipologie di attacchi DDoS (Dati Fastweb relativi all'anno 2022)*

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. Nel 2022 sono stati rilevati oltre 41.000 server e device che espongono impropriamente protocolli a rischio in rete, un numero in diminuzione rispetto a quanto visto in passato. 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.

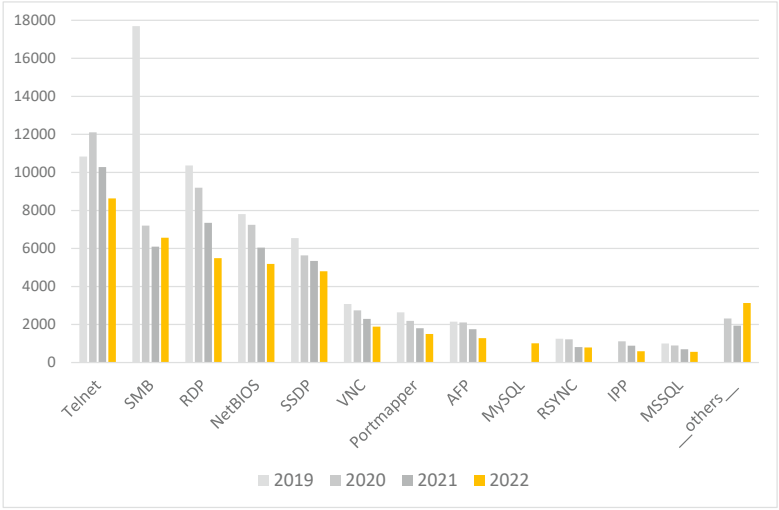


Figura 10: *Servizi critici esposti su Internet (Dati Fastweb relativi agli anni 2019, 2020, 2021 e 2022)*

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 una diminuzione del 16% rispetto alle rilevazioni del 2021. In controtendenza rispetto agli anni precedenti, aumentano significativamente i 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. Scende al terzo posto l'RDP (-25% rispetto al 2021), utilizzato per la connessione remota ad un PC e che permette di prendere il controllo completo di un apparato se sfruttato dall'esterno.

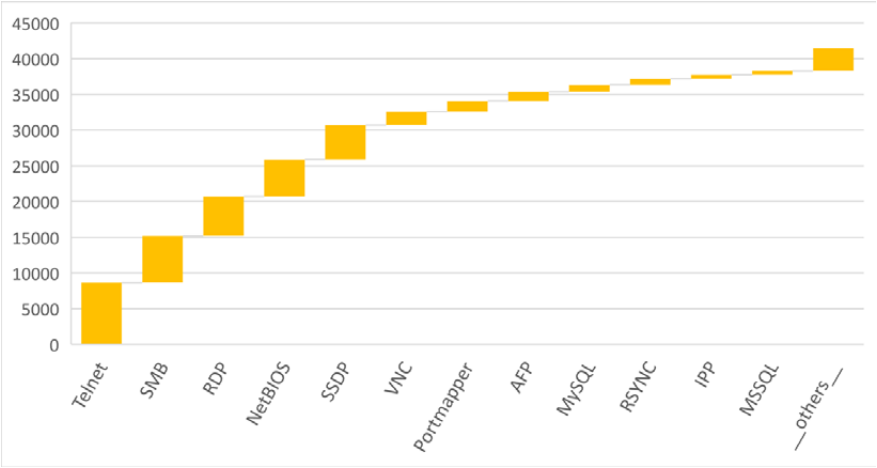


Figura 11: *Servizi esposti direttamente su Internet (Dati Fastweb relativi all'anno 2022)*

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 2022, le rilevazioni effettuate mostrano che oltre 3.400 IP sono stati inseriti almeno una volta nelle blocklist. Il dato nel 2022 (-35.4%) è in netto calo rispetto al 2021, dove si erano registrati circa 5.300 azioni di blocklisting. La rilevazione indica un'inversione di tendenza, in quanto si registra per la prima volta una diminuzione percentuale così elevata. 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.

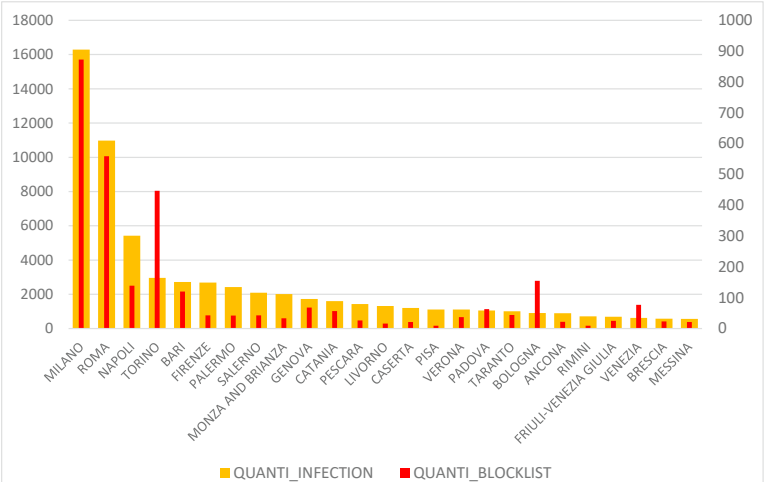


Figura 12: *Dispositivi in Blocklist e infezioni per città (Dati Fastweb relativi all'anno 2022)*

A livello nazionale, si rileva che le regioni del nord Italia hanno registrato quasi il 60% delle infezioni totali (+11% rispetto al 2021).

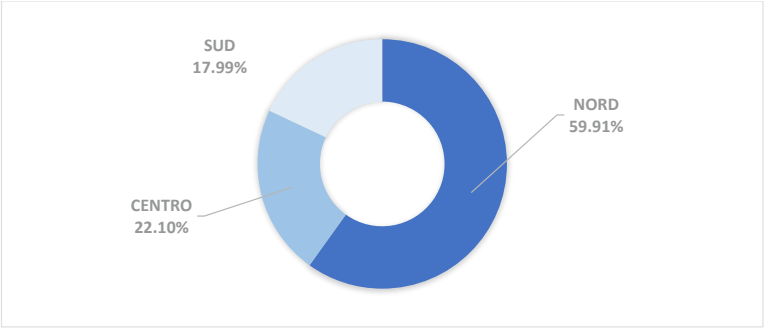


Figura 13: *Distribuzione geografica dei server in blacklist (Dati Fastweb relativi all'anno 2022)*

Sicurezza applicativa Web

Di seguito un'analisi sul mondo delle vulnerabilità e degli attacchi indirizzati ai software e ai sistemi applicativi delle aziende del settore Enterprise e della Pubblica Amministrazione rilevati sulla rete di Fastweb attraverso tecnologie di tipo Web Application Firewall e bloccati dai servizi di cyber sicurezza attivi. Dalle rilevazioni raccolte nel campione analizzato del 2022, a differenza dell'anno precedente, si evidenziano eventi cyber di tipologia *SQL*

Injection (attacco diretto ad avere accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database). Le attività di information gathering risultano notevolmente ridotte rispetto agli anni passati: la spiegazione è da ricondurre agli sviluppi che nel 2022 hanno caratterizzato lo scenario geopolitico internazionale. Il primo effetto, registrato dai giorni immediatamente successivi all'invasione delle truppe russe in territorio ucraino (24 febbraio 2022), è stato una richiesta massiccia di implementazione di blocchi su base geografica. La maggior parte delle aziende e delle istituzioni nazionali, infatti, ha provveduto a limitare le esposizioni dei propri servizi non solo a sorgenti provenienti dalle nazioni coinvolte nel conflitto in maniera diretta ma anche a tutte le sorgenti delle aree geografiche non direttamente di interesse per il loro business.
A seguire, nelle tipologie di tecniche di attacco applicativo, ritroviamo: *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 che costringe l'utente a eseguire azioni non volute) e *Directory Traversal* (attacco utile ad avere accesso a file in directory in cui non si è autorizzati ad accedere). 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 Attack* sono state raggruppate tutte quelle tipologie di attacchi che sfruttano exploit comuni ma non rientrano nelle categorie precedenti.

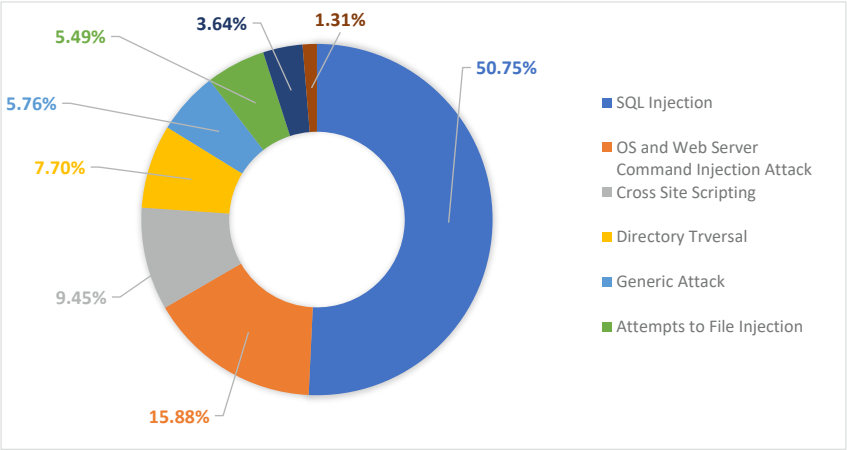


Figura 14: *Tecniche di attacco applicativo rilevate dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2022)*

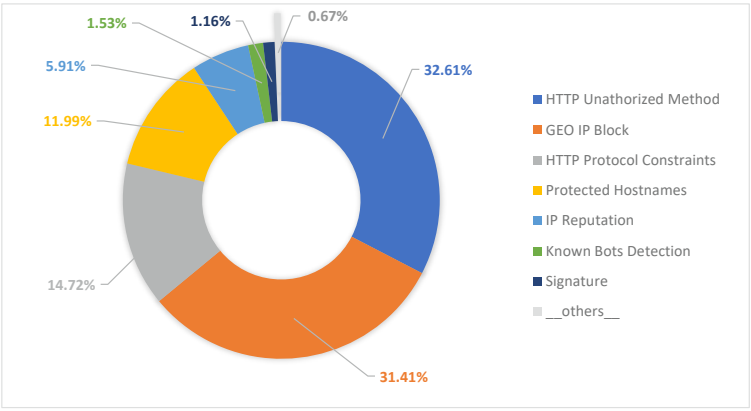


Figura 15: *Tipologie di contromisure maggiormente intervenute a protezione degli attacchi applicativi (Dati Fastweb relativi all'anno 2022)*

La rilevazione delle sorgenti di attacco applicativo rilevate dai WAF, gestiti dal Security Operation Center di Fastweb, mostrano anche quest'anno gli Stati Uniti al primo posto. A partire dall'ultimo trimestre c'è stato un aumento di attacchi provenienti dalla Germania, che ha superato anche quanto rilevato dagli Stati Uniti. Al terzo posto si piazza la Federazione Russa, seguita da Italia e Bulgaria, che entra per la prima volta in classifica. Rispetto al 2021, l'Italia perde una posizione ma rimane tra le aeree geografiche da cui partono la maggior parte dei tentativi di connessione malevola: questo sottolinea quanto contromisure basate sulla provenienza geografica perdano di valore e sia sempre più importante introdurre sistemi di protezione basati su tecnologie all'avanguardia e affidarsi a centri di competenza specifici come Cyber Defense Center e personale specializzato.

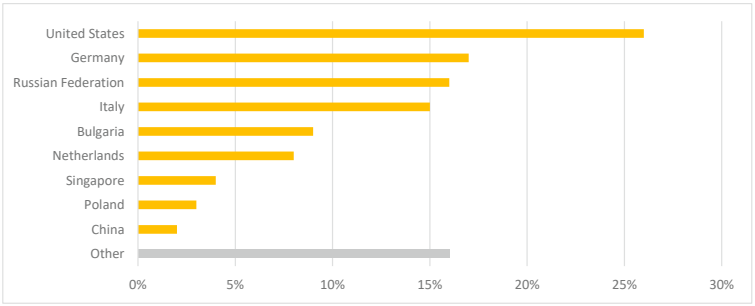


Figura 16: *Dislocazione delle sorgenti di attacco applicativo rilevate dai WAF del segmento Enterprise (Dati Fastweb relativi all'anno 2022)*

Trend e minacce in ambito Mail

In questa sezione vengono riportati i principali trend del 2022 rilevati da Fastweb nell'ambito Mail Security.

Il fattore dominante utilizzato per veicolare attacchi tramite e-mail è rappresentato dall'utilizzo di URL malevoli, come illustrato nel grafico sottostante. Considerando l'andamento annuo, in aumento del 100% rispetto al precedente, la presenza diretta di allegati malevoli all'interno delle e-mail, appare in diminuzione. Il dato è in controtendenza rispetto al trend,delle compromissioni malware e ransomware. Una spiegazione del fenomeno può essere data dal fatto che la minaccia inviata tramite URL all'interno di una e-mail potrebbe condurre l'utente a scaricare file malevoli in un secondo momento.. –

Gli attacchi veicolati tramite messaggi di posta elettronica sono sempre più spesso organizzati tramite campagne dedicate, dove il fattor comune è il tema oggetto della comunicazione e/o l'identità dei soggetti da colpire.

Resta comunque significativa, anche se in diminuzione rispetto all'anno precedente, un'importante percentuale (pari al 73,30%) relativa alle «Minacce Individuali» inviate tramite e-mail. Con questo termine s'identificano le minacce mail per le quali non è stato possibile determinare elementi in comune a campagne note, a causa delle insufficienti informazioni per attribuirla ad uno specifico attaccante.

Le tipologie di minacce sono in continua crescita, sintomo che gli attaccanti escogitano sempre nuove modalità per eludere i sistemi di monitoraggio.

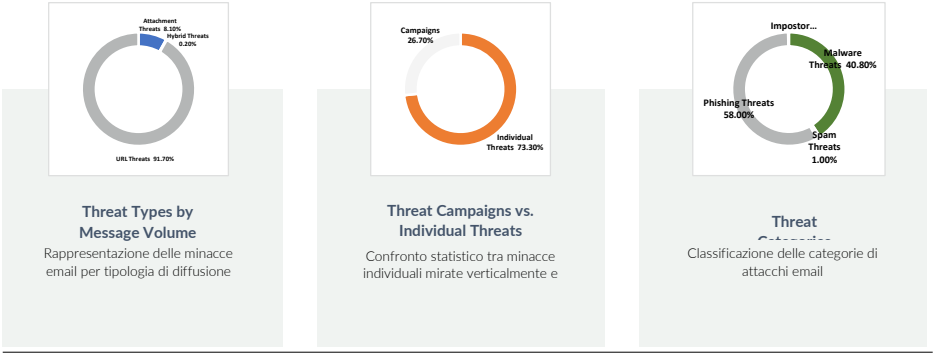


Figura 17: *KPI Minacce Mail 2022*

Ad eccezione del trojan bancario Emotet (utilizzato nel 2022 principalmente come sistema di distribuzione di ransomware) e di Cobalt Strike, la distribuzione delle restanti tipologie di malware è relativa a quelle forme di codice malevolo che hanno come finalità l'esfiltrazione di informazioni e dati delle vittime (minacce di tipo «info-stealer»). Come è possibile vedere dall'immagine sottostante, nel 2022 lo scenario dei malware più impattanti a livello di volume è molto diverso da quanto visto nel 2021: le rilevazioni hanno registrato aumenti significativi per tutte le categorie, portando malware che erano minori nel 2021 ad essere i

più frequenti. Si precisa che il malware FormBook è l'unico presente nella top 5 di entrambi gli anni, riconfermando il trend di crescita a volume.

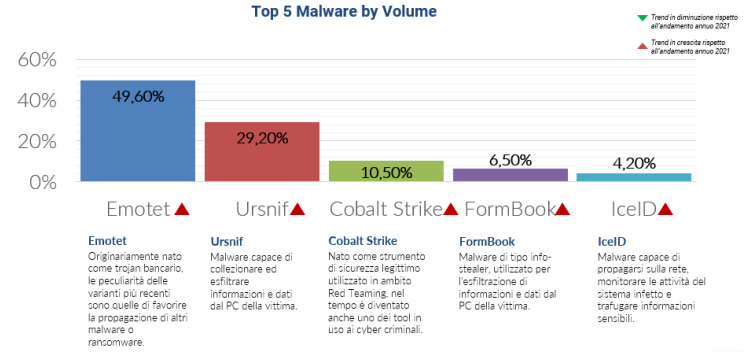


Figura 18: *Top 5 Malware per volume 2022*

A livello di tecniche utilizzate dai cybercriminali nel veicolare le minacce via e-mail, si registra un aumento delle campagne fraudolente ai danni delle figure apicali di grandi aziende italiane e non solo (il cosiddetto whaling phishing). Si tratta di una particolare frode che utilizza le modalità del phishing per l'operatività delle e-mail malevole e quelle del social engineering per rendere credibile il raggiro che, solitamente, culmina con perdite economiche anche rilevanti per le aziende prese di mira.

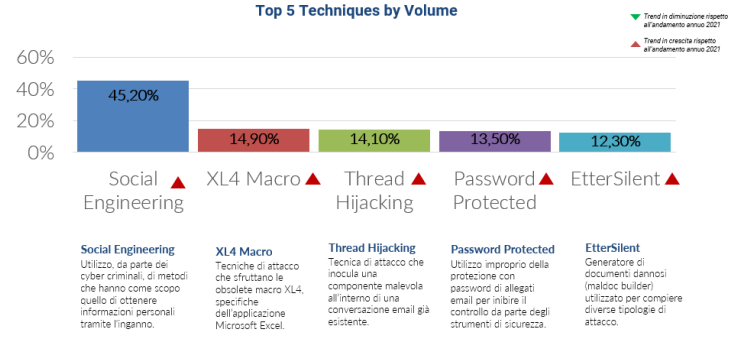


Figura 19: *Top 5 tecniche per volume 2022*

Il grafico precedente mostra, anche in questo caso, una tendenza crescente rispetto al 2021, con un aumento nei volumi registrati per ognuna delle tecniche più comuni. Da sottolineare come il social engineering, l'insieme delle tecniche utilizzate per veicolare attacchi volti ad estorcere dati personali da utenti ignari, abbia registrato l'aumento più significativo, con una crescita del 460%.

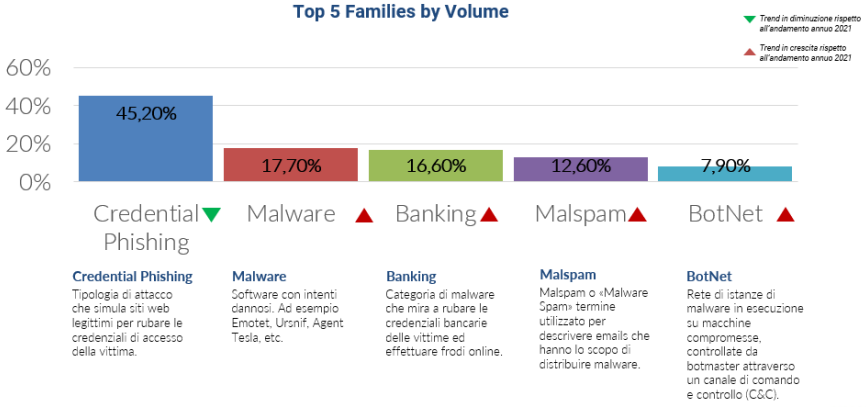


Figura 20: *Top 5 famiglie di minacce per volume 2022*

L'immagine sopra rappresenta una classificazione delle minacce e-mail le cui modalità di attacco variano dall'installazione di software malevolo al furto dei dati personali degli utenti. Il dato sul «Credential Phishing», nonostante presenti un Trend in lieve decrescita nell'anno 2022, rappresenta comunque la modalità di attacco più utilizzata. Tutte le altre famiglie di minacce, invece, sono aumentate in termini di volume rispetto al 2021.
Il team Fastweb CSIRT&SOC, nel corso dell'anno 2022, tramite i sistemi di monitoraggio del presidio e-mail, ha attenzionato un volume di messaggi malevoli afferenti a diversi threat actor. Come è possibile osservare dal grafico sottostante, i principali sono stati:
TA542 (Mummy Spider)
TA542 (alias Mummy Spider) è un gruppo di tipo Cyber Crime legato prevalentemente allo sviluppo del malware Emotet.
Osservato per la prima volta a metà del 2014, questo gruppo ha rapidamente sviluppato le capacità di Emotet, facendolo evolvere da trojan bancario ad una più sofisticata minaccia utilizzata per veicolare altre tipologie di malware o ransomware.
TA542 è noto tipicamente per distribuire campagne email malevole ad alto volume, composte da centinaia di migliaia di messaggi di posta rivolti verso target di diversi settori e su scala internazionale.
TA544 (Hastur)
TA544 (alias Hastur) 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. Si segnala come queste tipologie di minacce, così come il social en-

gineering, si basano sull'intelligenza artificiale, tecnica sempre più utilizzata dai cyber-criminali per affinare la qualità dei loro attacchi e ingannare più utenti possibile. Infatti, l'uso del machine learning permette di raccogliere informazioni sui target e addestrare l'intelligenza artificiale per provocare conseguenze sempre più impattanti.

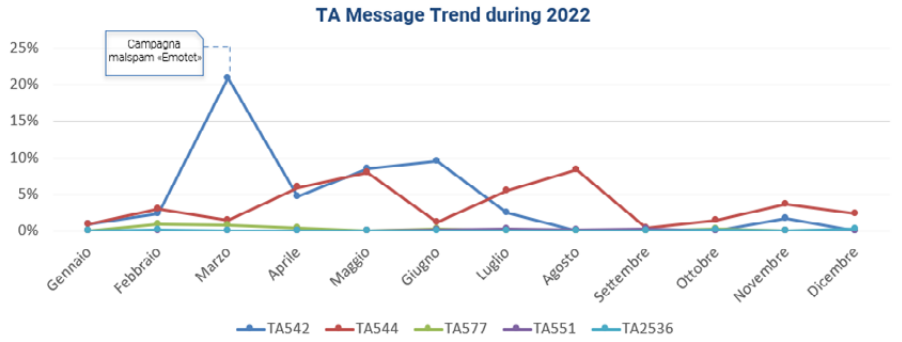


Figura 21: *Threat Actor durante il 2022*

Trend e nuovi fenomeni in ambito Frodi

Nel 2022 Fastweb ha rilevato una crescita di fenomeni legati al cosiddetto "CLI spoofing", ossia la manipolazione del numero chiamante per camuffare la reale provenienza della chiamata. Questo fenomeno è associato in modo importante al telemarketing "aggressivo" e al "robocalling", ossia il fenomeno delle chiamate automatiche.

Il CLI spoofing è spesso utilizzato per chiamate ingannevoli nei confronti degli utenti, che vengono spinti a cambiare operatore con scuse del tutto inventate quali il raddoppio del canone o disservizi prolungati anche fino a 60 giorni.

L'introduzione a luglio 2022 del registro delle opposizioni anche per i numeri mobili non ha finora sortito gli effetti sperati. È infatti esperienza purtroppo comune a molti cittadini italiani essere contattati tutti i giorni, a qualsiasi ora, da numeri di telefono sconosciuti per la proposizione dei più svariati servizi, spesso tramite risponditore automatico. E questo accade anche dopo l'iscrizione al registro delle opposizioni.

Restano sempre diffusi e pericolosi i fenomeni fraudolenti che sfruttano il servizio SMS. In particolare, la diffusione di malware, veicolati attraverso lo smishing, cioè il phishing via SMS che avviene solitamente inducendo la persona a cliccare su link malevoli inseriti all'interno del testo dell'SMS Questi malware, oltre a comportare potenziale perdita di dati per gli utenti, si possono propagare inviando nuovi SMS agli indirizzi che trovano nella rubrica dell'utente e a numerazioni decise da "command & control". Lo smishing spesso si verifica anche associato allo spoofing del mittente, ossia alla falsificazione del mittente, specie se alfanumerico (alias). Il risultato è che l'utente viene ingannato da un SMS malevolo che risulta inviato da un mittente a lui noto, come ad esempio la sua banca.

Una versione di smishing ad alto costo per l'utente ma a minor rischio di violazione, è quella dei messaggi che invitano a chiamare numerazioni a pagamento (es 899). Fastweb ha da anni adottato una politica di protezione per i propri clienti, limitando la possibilità di chiamare le numerazioni ad alto costo.
Per sensibilizzare gli utenti a riconoscere ed evitare queste minacce, sempre più aggressive e frequenti, Fastweb invia comunicazioni multicanale ai propri clienti e pubblica periodicamente informazioni sul proprio sito istituzionale nella sezione "Sicurezza in rete" e sulle sue properties.
Tra i fenomeni sempre attuali è bene ricordare:
Le frodi da sottoscrizione con furto d'identità, che diventano sempre più sofisticate e costose, quando scoperte. Il fenomeno è presente anche per le Partita IVA, oltre per il segmento residenziale.
Questi fenomeni, possono essere correlati a "frodi dealer", ossia frodi che hanno come obiettivo quello di massimizzare i guadagni di un rivenditore a scapito del titolare dell'identità e con danno economico e di immagine dell'operatore suo malgrado coinvolto.
Il "PBX hacking", in cui i truffatori sfruttano le vulnerabilità dei centralini stessi o l'esposizione di servizi in rete per "attaccarsi" al centralino di un cliente di tipo business, per generare traffico verso numerazioni ad alto costo. Il fenomeno affligge sia i centralini fisici, sia i centralini virtuali. Il fenomeno interessa anche le PA. Tuttavia, si riducono i costi associati al fenomeno, soprattutto per la maggiore reattività degli strumenti e dei team antifrode su un fenomeno noto.
Tra le direttrici internazionali maggiormente sfruttate, si confermano alcuni Paesi dell'Africa e Paesi dell'Europa orientale, come da mappa sotto rappresentata.

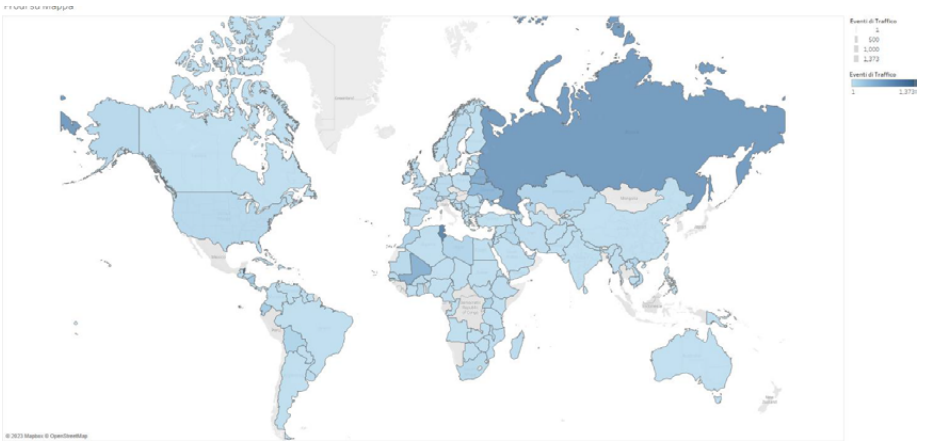


Figura 22: *Distribuzione geografica degli eventi di frodi*

Attività e segnalazioni della Polizia Postale e delle Comunicazioni nel 2022

Si illustrano di seguito i risultati conseguiti dalla Polizia Postale e delle Comunicazioni a livello nazionale nell'attività di prevenzione e contrasto dei reati informatici, riferiti all'anno 2022, confrontato con il biennio precedente.
Nel 2022 si è assistito ad un incremento generale degli attacchi nel nostro Paese, così come nel resto del mondo, a causa soprattutto del turbamento degli equilibri geopolitici legati al conflitto russo-ucraino e alla concatenata crisi finanziaria ed energetica. Ad essere colpite soprattutto aziende e infrastrutture strategiche italiane, con un incremento che, come vedremo nei paragrafi successivi, ha fatto registrare un +138% rispetto al 2021 ed un +220% rispetto al 2020.
Per un altro verso la fine dell'emergenza sanitaria e la progressiva ripresa delle normali attività, con una contestuale riduzione dell'isolamento sociale, hanno fatto registrare, nel 2022, dati sostanzialmente in linea con l'anno precedente, con una lieve flessione per alcune tipologie di reati, che analizzeremo più approfonditamente di seguito.

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

La tecnologia è diventata parte integrante del vivere quotidiano, ogni attività viene organizzata, gestita e vissuta con il supporto del mezzo informatico, questo comporta un coinvolgimento, sempre più frequente, della rete anche nelle attività illecite. Vittime della criminalità on-line spesso sono i minori che hanno raggiunto livelli di confidenza elevatissimi con gli strumenti informatici.
Nel 2022 il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) ha confermato il suo ruolo di punto di riferimento e di coordinamento nazionale dei Centri Operativi Sicurezza Cibernetica – COSC della Polizia Postale nella lotta alla pedofilia e pornografia minorile online, nonché al contrasto di tutti i fenomeni che coinvolgono i minori.
I dati analizzati nel corso dell'anno hanno fatto riscontrare una lieve flessione dei casi trattati, nonché la diminuzione delle segnalazioni provenienti da organismi internazionali attivi nella protezione dei minori in rete, evidenziando, di contro, l'impegno profuso dalla Specialità nel reprimere episodi di particolare gravità, elemento rilevabile dal maggior numero di responsabili sottoposti a pene detentive.
La fine dell'emergenza sanitaria, con la progressiva ripresa delle attività nella direzione di un recupero della normalità, potrebbe aver contribuito a ridurre l'isolamento sociale, facendo rilevare nel 2022 una riduzione della circolazione globale di materiale pedopornografico su circuiti internazionali, che non ha però inciso sull'attività di contrasto. Infatti, è stato registrato un aumento dei soggetti individuati e deferiti all'Autorità giudiziaria per violazioni connesse ad abusi in danno di minori.
In particolare, nell'ambito dell'attività di contrasto coordinata dal Centro sono stati trattati complessivamente 4.618 casi, che hanno consentito di indagare 1.466 soggetti, di cui 149

tratti in arresto per reati connessi alla materia degli abusi tecnomediati in danno di minori, con un aumento di persone tratte in arresto di circa il +7% rispetto all'anno precedente.
Nell'ambito dell'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati visionati 25.896 siti, di cui 2.622 inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	2021	2022	Variazione percentuale
Persone indagate	1.421	1.466	+3%
Siti in Black List	2.543	2.622	+3%

Adescamento online

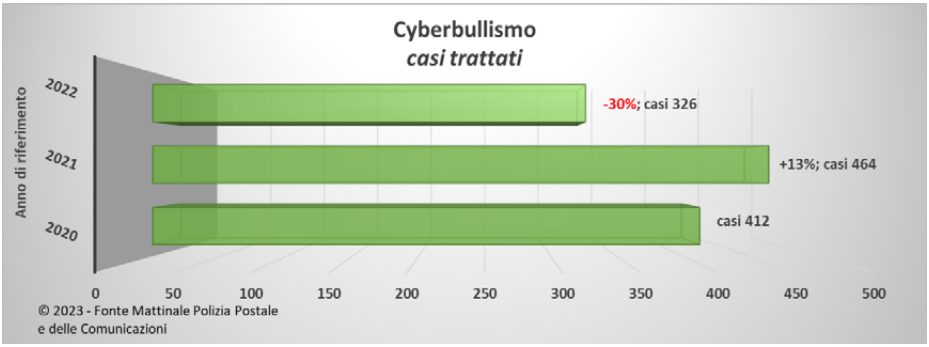
Nel periodo di riferimento sono stati trattati 430 casi per adescamento online: anche quest'anno la fascia dei preadolescenti (età 10-13 anni) è quella più coinvolta in interazioni sessuali tecnomediate, 231 rispetto al totale.
Un dato che impone maggior attenzione e quello rilevato nella fascia di età 0-9 anni, infatti il lento incremento dei casi relativi a bambini adescati di età inferiore ai 9 anni è diventato più consistente a partire dalla pandemia. Social network e videogiochi online sono i luoghi di contatto tra minori e adulti più frequentemente teatro delle interazioni nocive, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

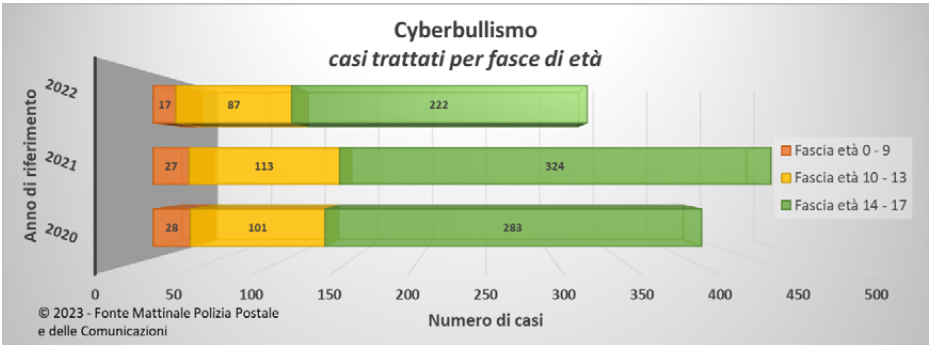
Cyberbullismo

Anche per quanto riguarda gli episodi di cyberbullismo è stata riscontrata una leggera flessione che può essere interpretata come effetto della normalizzazione delle abitudini dei ragazzi: non si può escludere che il ritorno ad una vita sociale priva di restrizioni abbia avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costanza dell'opera di sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete.
Nel periodo di riferimento sono stati trattati 326 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 2020	412	+13%	28	-4%	101	+12%	283	+14%
Anno 2021	464	-30%	27	-37%	113	-23%	324	-31%
Anno 2022	326		17		87		222	

CYBERBULLISMO Minori indagati	TOTALE
Anno 2020	118
Anno 2021	136
Anno 2022	129





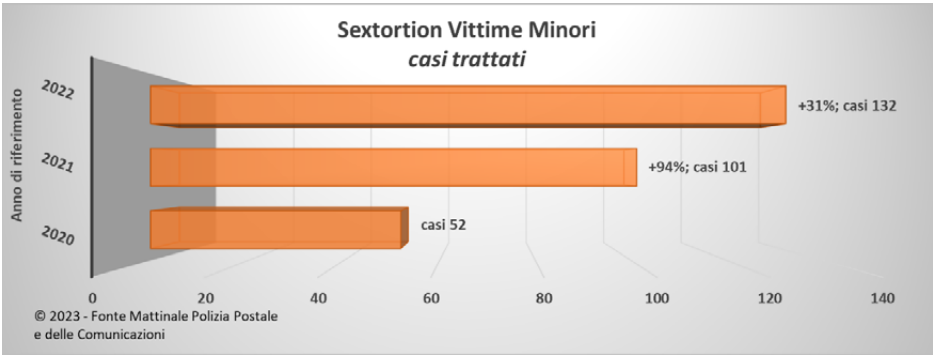
Sextortion

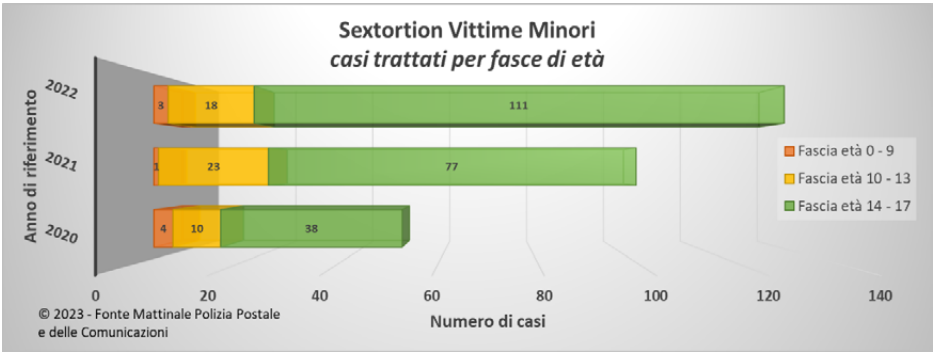
È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo, fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

Recentemente le sextortion stanno interessando sempre più spesso vittime minorenni, nel corso dell'anno sono stati trattati 132 casi, la maggior parte dei quali nella fascia 14-17 anni, più spesso in danno di vittime maschili 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 di aver ceduto e di essersi fidati di perfetti e "avvenenti" sconosciuti.

La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste.

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 2020	52	+94%	4	-75%	10	+130%	38	+103%
Anno 2021	101	+31%	1	+200%	23	-22%	77	+44%
Anno 2022	132		3		18		111	





C.N.C.P.O. – ATTIVITÀ DI POLIZIA GIUDIZIARIA

Si riportano di seguito, le attività investigative di maggior rilievo coordinate dal Centro Nazionale per il Contrasto alla Pedopornografia online:

OPERAZIONE *"MEET UP"*: condotta in modalità sotto copertura dal personale del Centro Operativo Sicurezza Cibernetica della Polizia Postale Piemonte e Valle D'Aosta, all'interno di canali Telegram dedicati alla diffusione, anche mediante sottoscrizione di abbonamenti a pagamento, di contenuti realizzati mediante sfruttamento sessuale di minori. Gli investigatori, interagendo direttamente in chat con gli utenti responsabili della diffusione, anche grazie alla capitalizzazione delle tracce informatiche e finanziarie enucleate, hanno potuto identificare gli utilizzatori dei nicknames destinatari dei 26 decreti di perquisizione emessi dall'A.G. procedente, che hanno consentito di indagare 26 persone, 3 delle quali tratte in arresto.

OPERAZIONE *"GREEN OCEAN"*: svolta in modalità sotto copertura dal Centro Operativo Sicurezza Cibernetica della Polizia Postale di Palermo su piattaforme di file sharing e di messaggistica utilizzate per la diffusione di contenuti di pornografia minorile. All'esito dell'indagine sono state eseguite, su tutto il territorio nazionale, coordinate dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, 32 perquisizioni nei confronti di altrettanti indagati, che hanno consentito di trarre in arresto 13 persone per detenzione di ingente quantità di materiale pedopornografico. In un caso, la perquisizione informatica effettuata sui dispositivi ha messo in luce l'esistenza di abusi fisici in danno di due minori, all'epoca dei fatti dell'età di 2 e 3 anni.

L'attività in argomento ha consentito, inoltre, di individuare centinaia di account riconducibili a utenti esteri, per i quali sono stati interessati i relativi collaterali.

OPERAZIONE *"FAMIGLIE DA ABUSI"*: svolta in modalità sotto copertura nell'ambito del contrasto alla pedopornografia online sul gruppo Telegram "Famiglie da Abusi" e condotta dai Centri Operativi Sicurezza Cibernetica di Roma, Bologna, Milano, Napoli e Catania, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di arrestare 5 persone ritenute responsabili di diffusione e detenzione di

materiale di sfruttamento sessuale di minori online.

In particolare, gli indagati appartenevano a una comunità ristretta dedita allo scambio di materiale pedopornografico, anche autoprodotto dagli stessi partecipanti.

OPERAZIONE "*REVELATUM*": condotta dal Centro Operativo Sicurezza Cibernetica della Polizia Postale della Puglia nell'ambito del contrasto alla pedopornografia online, ha visto coinvolti 72 indagati, destinatari di altrettanti decreti di perquisizione su tutto il territorio nazionale, emessi dall'A.G. procedente.

L'indagine, avviata alla fine del 2020, ha preso le mosse dall'analisi delle tracce informatiche collegate a un link afferente a un cloud attestato sulla piattaforma di file hosting "Mega.nz".

Gli Uffici territoriali della Polizia Postale, coinvolti nella fase esecutiva dell'operazione e coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, hanno denunciato 59 persone per detenzione e diffusione di materiale pedopornografico e altre 7 sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante sfruttamento dei minori degli anni 18.

OPERAZIONE "*LUNA*": avviata dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale del Friuli Venezia Giulia sulla scorta delle risultanze emerse a seguito dell'analisi forense eseguita sui supporti informatici sequestrati a un indagato nell'ambito di altra operazione di polizia giudiziaria, si è conclusa con la denuncia di 25 persone, 7 delle quali minorenni e una tratta in arresto. L'attività, che ha coinvolto tutti gli Uffici territoriali della Specialità, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di indagare 25 soggetti, di cui uno in stato di arresto.

OPERAZIONE "*ESTOTE PARATI*": l'attività di indagine del Centro Operativo Sicurezza Cibernetica della Polizia Postale di Palermo trae origine dalla più ampia Operazione "DICTUM", avviata a seguito di una segnalazione pervenuta nell'ambito della cooperazione internazionale di polizia, che ha condotto all'individuazione di numerosi soggetti responsabili di aver condiviso in rete materiale pedopornografico tramite la piattaforma Mega.nz.

L'analisi del materiale detenuto in cloud, ha consentito la denuncia di 27 persone, 3 delle quali sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante lo sfruttamento sessuale di minori.

OPERAZIONE "*AREA PEDONALE*": avviata in modalità sotto copertura dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale Piemonte e Valle D'Aosta, con il coordinamento di questo Servizio, sulla piattaforma di messaggistica istantanea Telegram, sotto la direzione della Procura della Repubblica di Torino. Sono state eseguite contestualmente 12 perquisizioni su tutto il territorio nazionale, ad esito delle quali sono stati denunciati in stato di libertà 9 utenti per diffusione e detenzione di materiale pedopornografico, mentre altri 3 sono stati tratti in arresto in flagranza di reato.

OPERAZIONE "*BLACK ROOM*": condotta in modalità sotto copertura dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Napoli all'interno di canali Telegram, ha consentito la denuncia di 21 persone e l'arresto di altrettante 5, tra cui figu-

ra l'amministratore della pagina, creatore di un bot ad hoc per la condivisione automatica di materiale a fronte del pagamento di corrispettivi in denaro.

OPERAZIONE *"COCITO"*: il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Milano ha arrestato un trentatreenne romano per violenza sessuale aggravata ai danni della propria figlia, per detenzione, produzione e cessione di materiale pedopornografico e per adescamento di minorenne. L'attività è stata condotta in modalità sotto copertura all'interno di un canale Telegram, ove era avvenuta la condivisione del materiale multimediale inerente agli abusi, a cura degli operatori sul territorio con il costante coordinamento e supporto del C.N.C.P.O.

OPERAZIONE *"DICTUM III"*: l'attività di indagine del Centro Operativo Sicurezza Cibernetica della Polizia Postale per la Toscana trae origine dalla più ampia Operazione "DICTUM", avviata a seguito di una segnalazione pervenuta nell'ambito della cooperazione internazionale di polizia, che ha condotto all'individuazione di numerosi soggetti responsabili di aver condiviso in rete materiale pedopornografico tramite la piattaforma Mega.nz.

All'esito delle attività, sono state denunciate 30 persone accusate di aver condiviso materiale pedopornografico tramite la citata piattaforma di cloud, di cui 5 sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante lo sfruttamento sessuale di minori.

OPERAZIONE *"POISON"*: condotta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Pescara, è scaturita su impulso del CNCPO a seguito di una segnalazione del Servizio Emergenza Infanzia 114, relativa alla condivisione, su gruppi social, oltre che di contenuti pedopornografici, anche di carattere zoofilo, necrofilo, scat, splatter, nonché di violenza estrema, apologia del nazismo/fascismo, atti sessuali estremi e mutilazioni, atti di crudeltà verso essere umani e animali, che ha interessato, nella fase esecutiva, diverse articolazioni territoriali della Specialità.

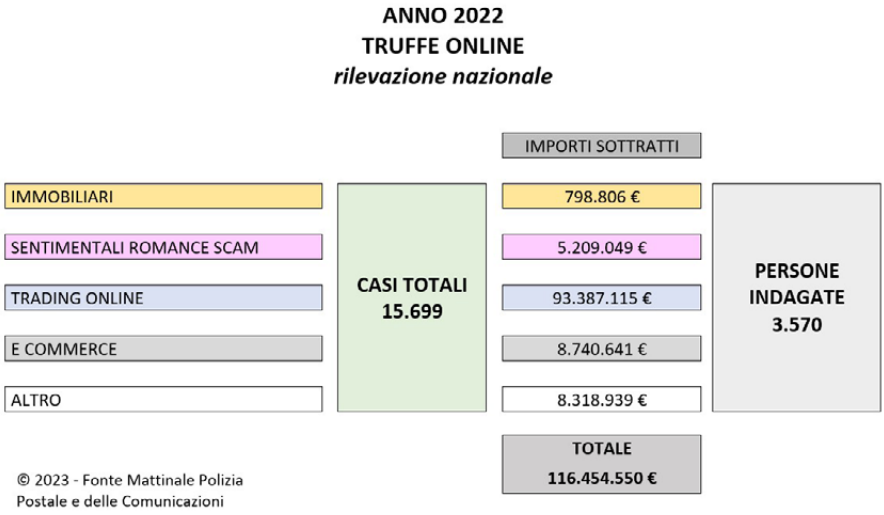
All'esito delle attività sono stati denunciati in stato di libertà 7 minori per diffusione e detenzione di materiale pedopornografico.

ARRESTO FIRENZE: personale del Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Firenze ha tratto in arresto un cittadino statunitense trovato in possesso di ingente quantitativo di materiale pedopornografico realizzato utilizzando minori di anni diciotto. La vicenda trae origine da una segnalazione che il CNCPO ha ricevuto dal collaterale statunitense.

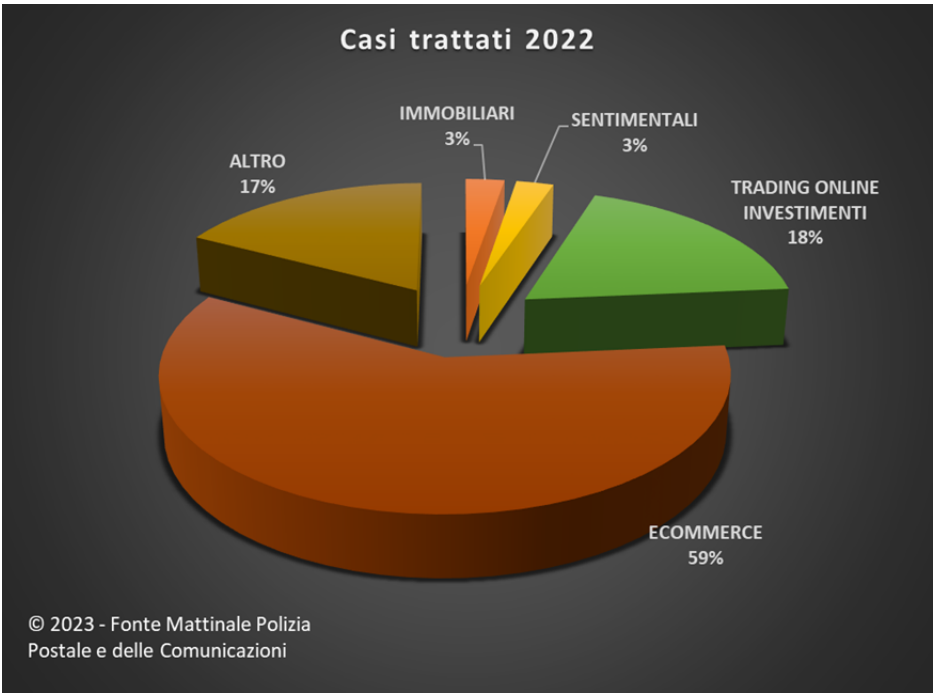
SEZIONE OPERATIVA

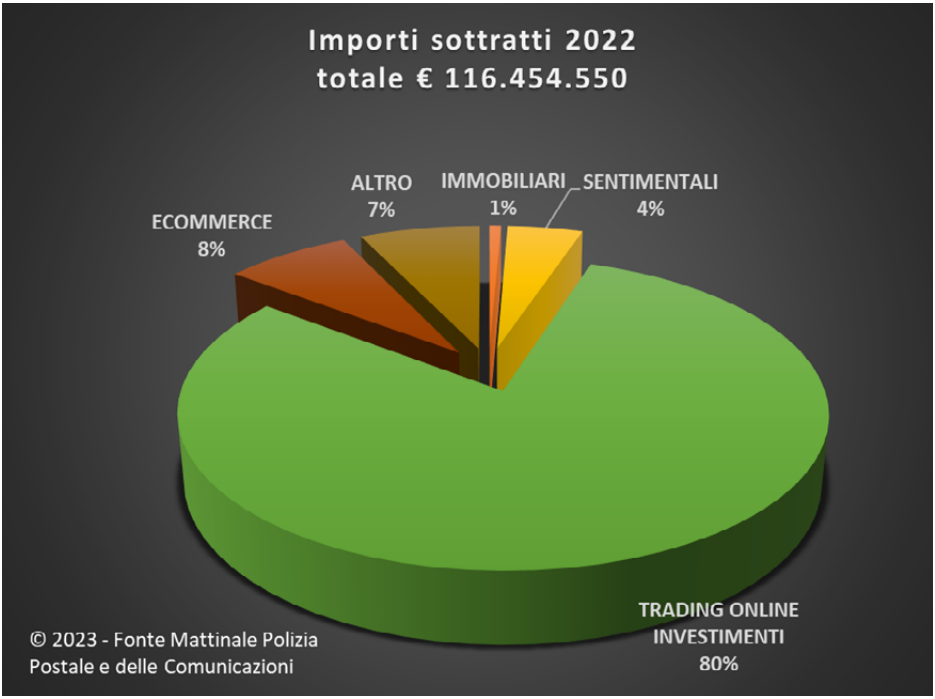
Nell'ambito delle competenze della Polizia Postale si segnala il rafforzamento dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle truffe online con 3541 persone deferite all'Autorità Giudiziaria, in particolare nel settore dell'e-commerce e market place.

Truffe OnLine	2021	2022	Variazione percentuale
Casi trattati	15.250	15.699	+3%
Persone indagate	3.441	3.570	+4%
Somme sottratte	€ 73.245.740	€ 116.454.550	+59%



Nell'ambito delle truffe sul web anche nel corso del 2022, importante l'incremento degli illeciti legati al fenomeno del trading online (3.057 i casi trattati e 131 le persone indagate), con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, e l'utilizzo di tecniche di *social engineering* sofisticate per individuare e contattare le vittime. L'attività investigativa, proprio per la caratterizzazione transnazionale del reato, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia con la richiesta del blocco urgente delle somme versate e l'espletamento di accertamenti sui flussi finanziari normalmente destinati all'estero.





Proprio per dare maggior impulso alle indagini che vedono coinvolti cittadini stranieri, la Sezione Operativa della Polizia Postale, nel corso dell'anno 2022, ha attivato 260 richieste di cooperazione internazionale attraverso i canali Europol e Interpol che, in più di un'occasione, si sono rivelate determinanti per l'individuazione degli autori dei reati investigati. Particolare attenzione è rivolta inoltre ai fenomeni del revenge porn, con 245 casi trattati (di cui 34 in danno di minori) e 72 persone denunciate e delle truffe romantiche, con 431 casi trattati (di cui 4 in danno di minori) e 104 persone denunciate, spesso sommersi in quanto caratterizzati da un forte coinvolgimento emotivo che induce la vittima a non denunciare. Sono stati 15 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 OnLine1	2021	2022
Casi trattati	10.412	9.366
Persone indagate	1.712	1.169

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

ANNO 2022
REATI CONTRO LA PERSONA
rilevazione nazionale

	CASI TRATTATI	PERSONE INDAGATE
STALKING	158	66
DIFFAMAZIONE ON LINE	2093	585
MINACCE	769	137
REVENGE PORN	245	72
MOLESTIE	632	56
SEXTORTION	1074	96
ILLECITO TRATTAMENTO DATI	952	27
SOSTITUZIONE DI PERSONA	3292	105
FENOMENO HATE SPEECH	100	24
PROPOSITI SUICIDARI	51	1
TOTALE	**9.366**	1.169

© 2023 - Fonte Mattinale Polizia Postale e delle Comunicazioni

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).
La Sezione Operativa ha profuso il proprio impegno anche nell'individuazione di proposte di vendita online di prodotti contraffatti o all'utilizzo illecito di segni distintivi dei marchi registrati, anche a tutela del c.d. italian sounding.
Il monitoraggio di siti e spazi web (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente seguita dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.
Nel corso del 2022 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli.
In ultimo, ma comunque di primaria importanza, è stata l'attività rivolta all'individuazione di quelle persone che, sfruttando principalmente la cassa di risonanza che i social media offrono, hanno manifestato intenti suicidari in conseguenza dei quali sono state attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente (64 le segnalazioni veicolate attraverso il Commissariato di P.S. OnLine e 51 gli interventi eseguiti sul territorio dalla Polizia Postale e delle Comunicazioni).

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC

Nell'esercizio della propria missione istituzionale, il Servizio Polizia Postale e delle Comunicazioni garantisce, fra l'altro, ai sensi del DM 15 agosto 2017 - Direttiva sul riordino dei comparti di Specialità delle Forze di Polizia – la protezione delle infrastrutture critiche informatizzate del Paese.
Nell'attuale e particolare contesto internazionale, l'escalation di tensione geopolitica in Ucraina continua ad avere significativi riverberi anche in materia di sicurezza cibernetica. Risultano infatti in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di phishing, diffusione di malware distruttivi (specialmente Ransomware), attacchi Ddos, campagne di disinformazione e leak di database. Inoltre, gruppi di hacker hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico".
In tal senso, come noto, il conflitto russo-ucraino ha comportato una recrudescenza nell'attività di attori ostili, connotati per attacchi ransomware – volti a paralizzare servizi e sistemi

critici mediante la cifratura dei dati contenuti – campagne DDoS, volti a sabotare la funzionalità di risorse online e, soprattutto, attacchi di tipo APT (Advanced Persistent Threat), condotti da attori ostili di elevato expertise tecnico, in grado di penetrare i sistemi più strategici mediante tecniche di social engineering o sfruttamento di vulnerabilità, al fine di garantirsi una persistenza silente all'interno di tali sistemi a scopo di spionaggio o successivo danneggiamento.
La proliferazione di gruppi ostili, si è attuata poi mediante il ricorso a crew hacker di c.d. crime as a service, ordinariamente attive nel fornire supporto tecnlogico ad attori criminali ed oggi sempre più contigue a gruppi di ascendenza statuale.
In riferimento allo specifico scenario e ai rischi collegati al quadro internazionale in dinamica evoluzione, il Servizio Polizia Postale e delle Comunicazioni, Organo del Ministero dell'Interno per la sicurezza delle telecomunicazioni, ha elaborato e condiviso numerosi report di sicurezza informatica recanti evidenze informative relative alle potenziali criticità in ambito cibernetico che depongono per il mantenimento del pi*ù elevato grado di allertamento*.
In particolare, il Servizio ha implementato l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al dark web, attivando canali di diretta interlocuzione dedicati allo scenario in atto, con Europol, oltre che con Interpol e FBI, con l'obiettivo di elevare il livello di attenzione con particolare riguardo al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione state sponsored.
Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), attraverso dedicati alert ha diffuso indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali target di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.
I Centri Operativi per la Sicurezza Cibernetica(COSC) sono stati inoltre sensibilizzati all'innalzamento delle attività di competenza, attraverso un adeguato e precipuo coinvolgimento dei rispettivi Nuclei Operativi di Sicurezza Cibernetica (NOSC), e alla predisposizione di adeguati servizi di monitoraggio e analisi, significando l'esigenza di tempestiva condivisione di ogni evidenza utile in relazione al quadro internazionale in parola.
A partire dal 19 maggio u.s., l'Italia - al pari di altri Paesi con posizioni di sostegno all'Ucraina - è stata interessata da una vasta mole di attacchi informatici, operati da gruppi di dichiarata matrice filorussa, diretti verso le infrastrutture critiche di numerosi paesi atlantisti. alia in particolare, tali attacchi si sono tradotti tra l'altro nella minaccia di danneggiamenti significativi a pubbliche amministrazioni, primari Organi di stampa, Istituti bancari, Porti, Aeroporti, Logistica.

L'attività del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni, oltre ai doverosi approfondimenti investigativi, si è tradotta nell'analisi tecnica della minaccia, volta alla elaborazione di informazioni di sicurezza preventiva, nonché nel supporto operativo alle infrastrutture attaccate, ed hanno consentito il ritorno alla piena operatività di tutti i sistemi informatici colpiti.

Nell'anno 2022, il C.N.A.I.P.I.C. - nell'ambito del complessivo Sistema Informativo Nazionale per il Contrasto al Cyber Crime[1], ha gestito:

- 13.099 attacchi informatici significativi nei confronti di servizi informatici relativi a sistemi istituzionali, infrastrutture critiche informatizzate di interesse nazionale, infrastrutture sensibili di interesse regionale, grandi imprese;

	ANNO 2020	ANNO 2021	ANNO 2022
TOTALE ATTACCHI RILEVATI	4.091	5.509	13.099
Variazione percentuale per anno		+35%	+138%
Variazione percentuale per biennio		+220%	

- ha diramato 113.420 alert di sicurezza riferibili a minacce per sistemi informatici/telematici oggetto di tutela del Centro;

	ANNO 2020	ANNO 2021	ANNO 2022
ALERT DIRAMATI DAL C.N.A.I.P.I.C.	83.416	110.880	113.420
Variazione percentuale per anno		+33%	+2%
Variazione percentuale per biennio		+36%	

- ha ricevuto 77 richieste di cooperazione, gestite dall'Ufficio del punto di contatto HTC Emergency presente all'interno del C.N.A.I.P.I.C. nell'ambito della Rete 24-7 "High Tech Crime" del G7.

[1] Si tratta del più ampio progetto SINC3, che prevede collegati in rete il CNAIPIC, a tutela delle infrastrutture critiche nazionali, ed i Nuclei operativi sicurezza cibernetica – NOSC dei Compartimenti, di prossima istituzione con la riorganizzazione dei presidi territoriali della Specialità, quest'ultimi a tutela dei rispettivi asset cibernetici regionali. Il progetto prevede tra l'altro la formazione degli operatori NOSC e la creazione di una piattaforma informatica per la gestione degli eventi e per la condivisione delle informazioni di sicurezza finanziata con fondi ISF, che, oramai avviata la fase sperimentale, potrà essere inaugurata il prossimo anno.

	ANNO 2020	ANNO 2021	ANNO 2022
Richieste di cooperazione HTC (High Tech Crime) 24/7	69	60	77
Variazione percentuale per anno		-13%	+28%
Variazione percentuale per biennio		+12%	

Le attività investigative avviate dal Centro e dai COSC, hanno portato al deferimento di complessive 334 persone per accesso abusivo e danneggiamento di sistemi informatici afferenti sistemi critici ovvero servizi essenziali, diffusione di mallware, trattamento illecito di dati su larga scala.

	ANNO 2020	ANNO 2021	ANNO 2022
Persone indagate	294	201	304
Variazione percentuale per anno		-32%	+66%
Variazione percentuale per biennio		+13%	

Di seguito, le principali attività svolte nel settore della protezione delle infrastrutture critiche nazionali nell'anno in corso.

Assistenza al Vicariato di Roma per la gestione della sicurezza informatica del X Incontro Mondiale delle Famiglie

Il 26 giugno 2022 si è concluso il X Incontro Mondiale delle Famiglie, tenutosi in forma "multicentrica e diffusa", a cui hanno partecipato i delegati delle Conferenze episcopali di tutto il mondo, nonché i rappresentanti dei movimenti internazionali impegnati nella pastorale familiare.

Il Servizio Polizia Postale e delle Comunicazioni ha assicurato un complessivo supporto tecnico-operativo finalizzato alla prevenzione ed al contenimento di eventuali attività ostili ai danni dell'infrastruttura informatica predisposta per l'iniziativa.

In particolare, il presidio di sicurezza si è articolato, da un lato, in una mirata attività di prevenzione, assicurata h24 dalla sala operativa del CNAIPIC, e dall'altro nell'invio di un team di supporto tecnico, direttamente presso la sede dell'evento.

Le evidenze raccolte in sede di monitoraggio, protrattosi per tutte le giornate dell'evento, sono state partecipate, in tempo reale, attraverso un canale operativo di comunicazione attivo 24/7 con i tecnici informatici presenti nel corso della manifestazione.

L'aliquota di personale specializzato del CNAIPIC presente in loco per tutta la durata

dell'Incontro, allocato presso una postazione dedicata nell'Aula Paolo VI della Città del Vaticano, ha garantito altresì diretta collaborazione e supporto ai referenti informatici del Vicariato anche attraverso la condivisione di tutte le informazioni di sicurezza informatica disponibili che hanno consentito di predisporre le adeguate misure di protezione dei sistemi e, quindi, il regolare svolgimento dell'evento.

72° Festival della Canzone Italiana di Sanremo

Il Servizio Polizia Postale e delle Comunicazioni, in collaborazione con la struttura di sicurezza cibernetica della RAI, infrastruttura critica convenzionata con il CNAIPIC, ha espletato un dedicato servizio di sicurezza informatica a tutela del 72° Festival della Canzone Italiana di Sanremo.
In particolare, come in occasione di importanti eventi nazionali, personale del CNAIPIC di questo Servizio e del Centro Operativo per la Sicurezza Cibernetica "Liguria", in stretto raccordo con la Questura di Imperia, ha garantito un dispositivo attivo h24 presso una sala operativa dedicata allestita dalla RAI in Sanremo per la diretta tutela dei sistemi e dei servizi informatici che hanno supportato l'intera produzione.
Durante l'attività svolta, il personale tecnico della Specialità ha individuato e segnalato due dispositivi affetti da numerose vulnerabilità, di cui due gravi, consentendo così alla struttura di sicurezza RAI di approntare le opportune e tempestive attività di rimedio, al fine di evitare possibili attacchi informatici.
È stato assicurato inoltre un monitoraggio costante degli account social (Twitter, Facebook ed Instagram) attivati per la manifestazione canora, esteso anche al sistema di tv streaming presente su www.raiplay.it, al fine di rilevare e neutralizzare in tempo reale minacce e interferenze ostili.

Attacco Ddos Parlamento Europeo

Una specifica campagna di attacchi informatici di tipo DDOS, tecnica volta a dirigere ingenti quantità di connessioni e richieste verso siti internet allo scopo di determinarne il malfunzionamento o la paralisi, è stata condotta nei confronti del sito del Parlamento Europeo (www.europarl.europa.eu) dal collettivo hacker "KillNet", associato ad ambienti filorussi e rivendicata attraverso i propri canali Telegram.
Il CNAIPIC ha investito la Sala Operativa Internazionale del Servizio per la Cooperazione Internazionale di Polizia per l'attivazione dei canali di cooperazione finalizzati alla condivisione con gli organi unionali delle informazioni di sicurezza informatica disponibili.
In particolare, gli indicatori di compromissione, elaborati dal Centro, sono stati al contempo direttamente anticipati, per una tempestiva azione di mitigazione, all'Ufficio di Collegamento presso l'Unione Europea.

Elezioni del Senato della Repubblica e della Camera dei Deputati

Il Servizio Polizia Postale e delle Comunicazioni, in collaborazione con il Dipartimento per gli Affari Interni e Territoriali (DAIT), ha espletato un dedicato servizio di sicurezza

informatica, a tutela del regolare svolgimento delle operazioni elettorali in occasione delle elezioni, tenutesi il 25 settembre u.s., per il rinnovo del Senato della Repubblica e della Camera dei Deputati.
È stato assicurato un complessivo supporto tecnico-operativo finalizzato alla prevenzione ed al contenimento di eventuali attività ostili ai danni dell'infrastruttura informatica predisposta per l'iniziativa.
In particolare, il presidio di sicurezza si è articolato in una mirata attività di prevenzione, assicurata h24 dalla sala operativa del CNAIPIC, nonché nell'impiego di un *team* di supporto tecnico di pronto intervento, operativo per tutta la durata delle operazioni elettorali e di scrutinio.
Le evidenze raccolte in sede di monitoraggio nonché tutte le informazioni di sicurezza disponibili sono state partecipate, in tempo reale, attraverso un canale operativo di comunicazione attivo 24/7 con i tecnici informatici del DAIT, consentendo di predisporre le adeguate misure di protezione dei sistemi a garanzia del corretto svolgimento dell'evento elettorale.

79^ Mostra Internazionale d'Arte Cinematografica presso la Biennale di Venezia

Il Servizio Polizia Postale e delle Comunicazioni ha espletato un dedicato servizio di sicurezza informatica a tutela della 79^ Mostra del Cinema presso la Biennale di Venezia, assicurando un complessivo supporto tecnico-operativo finalizzato alla prevenzione ed al contenimento di eventuali attività ostili ai danni dell'infrastruttura informatica predisposta per l'iniziativa.
In particolare, il presidio di sicurezza si è articolato, da un lato, in una mirata attività di prevenzione, assicurata h24 dalla sala operativa del CNAIPIC, e dall'altro nell'invio di un *team* di supporto tecnico, direttamente presso la sede dell'evento.
La sala operativa del CNAIPIC ha svolto più di 1000 ore di monitoraggio con oltre 100 specialisti della Polizia Postale.
Durante le attività sono state eseguite milioni di analisi di dati relativi agli IP di compromissione che hanno consentito di emanare delle procedure, grazie alle quali gli attacchi sono stati mitigati e respinti.
Come in occasione di importanti eventi nazionali, personale del CNAIPIC e del Compartimento Polizia Postale di Venezia ha garantito un dispositivo attivo h24 per la diretta tutela dei sistemi e dei servizi informatici che hanno supportato l'intera produzione.
Durante l'attività svolta, il personale tecnico specializzato della Polizia Postale e delle Comunicazioni, presente in loco presso una postazione dedicata, ha garantito altresì diretta collaborazione e supporto ai referenti informatici della Mostra anche attraverso la condivisione di tutte le informazioni di sicurezza informatica disponibili che hanno consentito di predisporre le adeguate misure di protezione dei sistemi e, quindi, il regolare svolgimento dell'evento.
È stato assicurato inoltre un monitoraggio costante degli account social (Twitter, Facebook ed Instagram) attivati per la manifestazione, nonché di quelli antagonisti orbitanti nell'am-

bito “no grandi navi” e “climate change” al fine di rilevare e neutralizzare in tempo reale minacce e interferenze ostili.

EUROVISION 2022

Una specifica campagna di tentativi di attacchi informatici di tipo DDOS, è stata condotta ai danni dei siti internet dell’evento internazionale Eurovision Song Contest 2022.
Per garantire la sicurezza durante lo svolgimento della manifestazione di carattere internazionale si è consolida la collaborazione e la partnership tra Polizia di Stato e Rai.
L’attivazione di una sala operativa dedicata all’evento di Eurovision nella quale tecnici e poliziotti specialisti del CNAIPIC (Centro Nazionale Anticrimine Informatico Protezione Infrastrutture Critiche) della Polizia Postale hanno lavorato fianco a fianco h24, ha permesso la neutralizzazione di minacce cibernetiche all’iniziativa.
L’attività info-preventiva condotta dal personale del CNAIPIC della Polizia Postale sulla base dell’analisi delle informazioni tratte anche nel darkweb, ha consentito altresì di desumere importanti informazioni di sicurezza, già condivise con la RAI per la prevenzione di ulteriori eventi critici.
La sala operativa del CNAIPIC ha svolto più di 1000 ore di monitoraggio con oltre 100 specialisti della Polizia Postale
È stata monitorata l’intera rete e analizzato miliardi di dati informatici provenienti anche dalle diverse piattaforme social. Durante le attività sono state eseguite milioni di analisi di dati relativi agli IP di compromissione che hanno consentito di emanare importanti procedure, grazie alle quali gli attacchi sono stati mitigati e respinti.

FINANCIAL CYBERCRIME

Nel corrente anno 2022 si riconferma la tendenza, già evidenziata nell'anno precedente, in base alla quale il financial cybercrime si afferma sempre più come una delle forme più predominanti e preminenti del crimine informatico, sia a livello nazionale che globale.
Questa tipologia di reati pone il vantaggio per la criminalità di fornire un immediato riscontro economico alle attività delittuose.
Sono molteplici ed in continua evoluzione le tecniche utilizzate da organizzazioni criminali, che colpiscono il tessuto economico italiano. La minaccia, spesso rappresentata da organizzazioni a carattere transnazionale, è fronteggiata puntualmente attraverso la specializzazione di unità della Polizia Postale che si occupano della materia. Il monitoraggio costante della rete è stato esteso anche al dark-web, e l'obiettivo di prevenire i rischi per i cittadini è stato perseguito anche attraverso campagne d'informazione condivise con il sistema bancario italiano e diffuse sui social-network e sulle piattaforme bancarie.
Il coordinamento delle attività investigative e l'azione di contrasto hanno consentito di individuare e fermare organizzazioni criminali specializzate, attraverso l'applicazione di misure precautelari personali e reali, fino al blocco/congelamento e al sequestro delle somme distratte, consentendone la restituzione alle vittime.
In tale scenario, è proprio il dato, l'informazione relativa all'identità, a costituire l'elemento più pregiato e ambito, che si ottiene grazie alle massive campagne di phishing, di social engineering rivolte soprattutto contro aziende piccole, medie e grandi, che costituiscono l'ossatura del sistema Paese.

Nel settore del contrasto al financial cybercrime, il fenomeno dei "money mules" rappresenta senz'altro una delle modalità più frequenti e consolidate per realizzare frodi online: con la funzione di "teste di legno" cibernetiche, personalità di dubbia moralità si prestano ad essere l'ultimo anello della catena attraverso il quale i criminali monetizzano i proventi del reato. La diffusione di questa modalità e il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e rappresentano ormai una realtà criminale quasi endemica in tutto il mondo. Per tale ragione già da diversi anni EUROPOL ha dedicato al contrasto del fenomeno una specifica Azione (EMMA) ad alto impatto che vede il coinvolgimento di oltre 20 nazioni.
Il 2022, inoltre è stato caratterizzato dalla crescita dell'interesse per le Cryptovalute: i cittadini italiani, anche con bassa scolarizzazione informatica, sono sempre più frequentemente attratti dagli investimenti in Cryptovalute, con la speranza di realizzare i facili e veloci guadagni pubblicizzati.

Quello delle Cryptovalute costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. All'interno di questo mondo è possibile effettivamente fare lauti guadagni, ma anche essere truffati da finte piattaforme di trading online o essere oggetto di furti e frodi attraverso attacchi di phishing.
In tale contesto sono realizzate attività investigative finalizzate a fermare i tentativi di phi-

shing: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle Crypto (cd. SEED), in realtà queste consentono ai malfattori di prendere il pieno possesso del Wallet e di impadronirsi del contenuto.
Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in Cryptovalute; sono state infatti coordinate diverse attività investigative dal Servizio Polizia Postale e delle Comunicazioni che hanno visto come oggetto truffe informatiche ad alto contenuto tecnico, conosciute con l'acronimo di BEC, CEO, Vishing, phinshing, con le quali viene tentato di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad exchange di cryptovalute. Tale procedimento consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare cash-out.

Per tale ragione è stata intensificata la collaborazione con le grandi società di Exchange di Crypto, così come è stata intensificata anche l'analisi delle transazioni Crypto con la collaborazione degli specialisti di settore di Europol.
La mancanza di confini geografici in Internet consente sempre più frequentemente anche la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.
Con riferimento al financial cybercrime, in relazione ai fenomeni di phishing, smishing e vishing, tecniche utilizzate per carpire illecitamente dati inerenti le credenziali di accesso ai sistemi di home banking, codici dispositivi, numeri di carte di credito, chiavi private di wallet di cryptovalute, la Polizia Postale e delle comunicazioni ha registrato 9.423 casi nazionali per i quali sono state indagate 867 persone.

Le minacce e gli attacchi al sistema economico del Paese, che già hanno avuto una crescita esponenziale e una forte evoluzione negli ultimi anni, anche nel 2022 si affermano sempre più come una delle forme predominanti e preminenti del crimine informatico, sia a livello nazionale che globale.
Il settore del c.d. *financial cybercrime* è un bacino molto remunerativo ed appetibile sfruttato da molte organizzazioni criminali, anche estere, come veicolo per finanziare le proprie attività illecite, il più delle volte attraverso l'utilizzo di sofisticate tecniche di *social engineering* per manipolare le vittime e indurle a fornire informazioni riservate.
I reati finanziari perpetrati all'interno dello spazio cibernetico, oltre ad offrire ampi margini di guadagno, hanno l'indubbio vantaggio di garantire spazi di impunità, grazie a sofisticate tecniche di anonimizzazione rese disponibili nel *dark web*, ad appannaggio anche di delinquenti comuni non facenti parte di grandi organizzazioni criminali.
Le conseguenze di un attacco informatico portato a compimento possono essere drammatiche ed avere effetti devastanti non solo su singoli utenti o investitori, ma anche con riverberi negativi per ciò che concerne piccole e medie imprese, con ingenti perdite economiche e

danni d'immagine difficilmente quantificabili, che incidono sullo stesso tessuto economico e sociale del Paese.
Solo la specializzazione del personale del Servizio Polizia Postale e delle Comunicazioni, e delle Sezioni operative presenti nei C.O.S.C. territoriali, impiegato per il contrasto al *Financial Cybercrime*, ha consentito di poter contrastare la minaccia spesso rappresentata da evolute tecniche di attacco poste in essere da organizzazioni criminali a carattere transnazionale.

L'a-territorialità che connota il reato informatico grazie alla mancanza di confini geografici dello spazio cibernetico, consente sempre più frequentemente anche la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.
L'esperienza maturata negli anni ha fatto intendere quali sono i principali focus per il contrasto di questa tipologia di crimini, sicuramente è prioritaria la scolarizzazione informatica e la corretta gestione dei *device* da parte dell'utenza che opera nel settore economico, partendo dall'assunto che l'errore umano è alla base di ogni tipologia di attacco.
L'obiettivo della prevenzione deve necessariamente essere perseguito attraverso campagne d'informazione della Polizia di Stato condivise con tutti i principali attori del sistema economico anche attraverso la diffusione sui social-network e sulle piattaforme finanziarie e bancarie.
All'obiettivo primario della prevenzione deve seguire una forte azione di contrasto finalizzata in *primis* al congelamento delle somme sottratte mediante il blocco bancario a cui far seguire il sequestro delle somme distratte, consentendone la restituzione alle vittime.
Il coordinamento delle attività investigative e l'azione di contrasto hanno consentito di individuare e fermare organizzazioni criminali specializzate soprattutto nella sottrazione e vendita del dato personale (i.e. l'identità, nr. di c/c, nr. telefonico, nr. carta di credito, documenti personali etc.).
E proprio il "dato personale" in tutte le sue sfaccettature, costituisce l'elemento più pregiato ed ambito, che si ottiene grazie alle massive campagne di *phishing* e di *social engineering* rivolte soprattutto contro aziende piccole, medie e grandi, che costituiscono l'ossatura del sistema Paese.
Una delle costanti nel sistema criminale che opera in questo settore è data dalla presenza dei "*money mules*", tipologia di soggetti di dubbia moralità che rappresentano l'elemento costante utilizzato ai fini della monetizzazione delle frodi.
Difatti questo ultimo anello della catena rappresenta anche la prima tappa della lunga marcia investigativa che occorre seguire per individuare gli ideatori delle truffe.
La diffusione di questa modalità ed il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e descrivono ormai una realtà criminale quasi endemica in tutto il mondo. Per tale ragione già da diversi anni EUROPOL ha dedicato al contrasto del fenomeno una specifica Azione ad alto impatto (EMMA) che vede il coinvolgimento di oltre 20 nazioni.

Nel 2022, le *Cryptovalute*, anche a causa degli eventi bellici, hanno avuto una flessione sia nel loro valore esponenziale che nel volume degli scambi. Non la stessa cosa può dirsi per le frodi perpetrate con il sistema del *fake trading on line* che hanno coinvolto moltissimi soggetti.

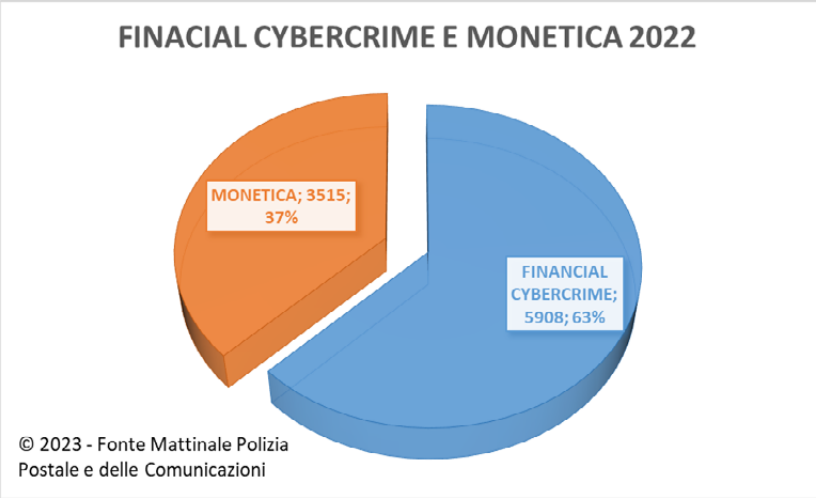
Quello delle *Cryptovalute* costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. All'interno di questo mondo è possibile effettivamente fare lauti guadagni, ma anche essere truffati da finte piattaforme di trading online o essere oggetto di furti e frodi attraverso attacchi di *phishing*.

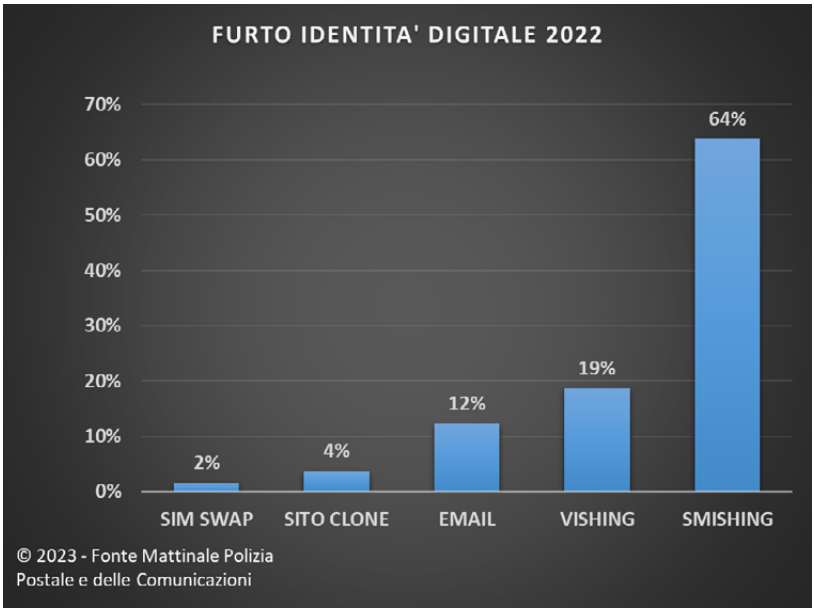
In tale contesto sono realizzate attività investigative finalizzate a fermare i tentativi di *phishing*: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle *Crypto* (cd. *SEED*), in realtà queste consentono ai malfattori di prendere il pieno possesso del *Wallet* e di impadronirsi del contenuto.

Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in *Cryptovalute*; infatti il Servizio Polizia Postale e delle Comunicazioni ha coordinato numerose attività investigative, che hanno visto come oggetto truffe informatiche ad alto contenuto tecnico, conosciute con l'acronimo di *BEC*, *CEO Fraud*, *Vishing*, *phinshing*, con le quali viene tentato di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad *exchange* di *cryptovalute*. Tale procedimento consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare *cash-out*.

Per tale ragione è stata intensificata la collaborazione con le grandi società di *Exchange* di *Crypto*, così come è stata intensificata anche l'analisi delle transazioni *Crypto* con la collaborazione degli specialisti di settore di Europol.

Con riferimento al *financial cybercrime*, in relazione ai fenomeni di *phishing*, *smishing* e *vishing*, tecniche utilizzate per carpire illecitamente dati inerenti le credenziali di accesso ai sistemi di *home banking*, codici dispositivi, numeri di carte di credito, chiavi private di *wallet* di *cryptovalute*, **la Polizia Postale e delle comunicazioni ha registrato 9.423 casi nazionali per i quali sono state indagate 867 persone.**


FINACIAL CYBERCRIME E MONETICA 2022
MONETICA; 3515; 37%
FINANCIAL CYBERCRIME; 5908; 63%
© 2023 - Fonte Mattinale Polizia Postale e delle Comunicazioni


FURTO IDENTITA' DIGITALE 2022
70%
60%
50%
40%
30%
20%
10%
0%
2%
4%
12%
19%
64%
SIM SWAP
SITO CLONE
EMAIL
VISHING
SMISHING
© 2023 - Fonte Mattinale Polizia Postale e delle Comunicazioni

Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, dirottate soprattutto verso Paesi extraeuropei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma OF2CEN (*On line fraud cyber centre and expert network*) per l'analisi e il contrasto avanzato delle frodi del settore, **la Specialità ha potuto bloccare e recuperare alla fonte 4.673.074,58 euro, su una movimentazione di 20.502.112,79, frutto di B.E.C.** (Business Email Compromise) **e** C.E.O**.** fraud (Chief Executive Officer fraud) **in danno di 156 grandi e medie imprese nazionali.** Sono in corso attività di cooperazione internazionale finalizzate al recupero delle restanti somme.

B.E.C. E CEO FRAUD IN DANNO DI GRANDI E MEDIE IMPRESE INVESTIGATE DAL SETTORE FINANCIAL CYBER CRIME DEL SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI

	2021	2022	%
Casi Trattati	131	156	+19%
Movimento totale frodi	20.784.572 €	20.502.112 €	
Somme recuperate	7.653.158 €	4.673.074 €	

A seguito dell'adesione a campagne internazionali ad alto impatto come EMMA 8 (*European Money Mule Action*), coordinata a livello nazionale dal Servizio Polizia Postale e delle Comunicazioni con la collaborazione di 24 paesi europei e di Europol, sono state identificate **653** persone in Europa e indagati **209** soggetti nel territorio nazionale. Le **transazioni fraudolente** sono state **838**, per un totale di circa **16 milioni di euro**, di cui oltre **5 milioni bloccati e/o recuperati**.

Attività di rilievo dell'anno 2022

Operazione "*FIDEL SCAM*"

Nella giornata del 17 novembre, personale della Polizia di Stato ha eseguito 7 decreti di perquisizione locale di perquisizione personale, locale e informatica contestuali alla misura cautelare dell'obbligo di dimora e presentazione alla P.G. emessi dalla Procura della Repubblica di Brescia, nei confronti di soggetti appartenenti ad un'associazione per delinquere finalizzata alla commissione di una serie di truffe, tentate o consumate, ai danni di piccole medie imprese nazionali.

In particolare, nell'ambito delle indagini, emergeva che le società bersaglio venivano contattate mediante PEC contenenti proposte di falsi finanziamenti, apparentemente erogati da importanti istituti bancari, garantiti da Cassa Depositi e Prestiti e concessi alla sola condizione della sottoscrizione di una polizza assicurativa fittizia che veniva incassata dal sodalizio criminale.

La Sezione Operativa per la Sicurezza Cibernetica di Crotone, coadiuvata per il coordinamento dal Servizio della Polizia Postale e delle Comunicazioni, è riuscita a porre sotto sequestro 15 dispositivi elettronici, 2 *hard disk*, 15 utenze telefoniche, 6 account email, 4 *tera byte* di dati, 10 carte di pagamento elettroniche e 19.960 euro in contanti, interrompendo così l'attività del sodalizio criminoso**.**

Operazione "*GHOTA*"

Il Centro Operativo Sicurezza Cibernetica per la Sicilia Orientale, con il coordinamento del Servizio della Polizia Postale e delle Comunicazioni, è riuscito ad individuare una serie di centrali di distribuzione del segnale pirata dislocate in particolare in Sicilia, Puglia e nelle Marche.

Nella mattinata del 10 novembre personale della Polizia di Stato ha eseguito 52 decreti di perquisizione personale, domiciliare e informatica emessi dalla Procura della Repubblica di Catania, a carico di altrettanti soggetti residenti in Italia e all'estero, facenti parte di un'associazione a delinquere a carattere transnazionale, strutturata secondo un modello organizzativo di tipo verticistico con l'aggravante del metodo mafioso, finalizzata al compimento di diversi reati tra i quali la diffusione di palinsesti televisivi ad accesso condizionato, attraverso le cosiddette IPTV (*Internet Protocol Television*),

Il complesso apparato organizzativo, impiantato dagli indagati, prevedeva di acquisire il segnale digitale proveniente da una serie di abbonamenti legittimamente acquisiti - successivamente inviato ad una struttura – e veniva convertivo in dato informatico (IP), attraverso specifiche apparecchiature dette "encoder". Una volta convertito veniva trasmesso in via informatica dalla sorgente ad uno o più server, allo scopo di renderne possibile la fruizione dei relativi contenuti audio e video presso migliaia di utenti finali dietro un corrispettivo di pagamento.

Dal 2016 l'attività illegale degli indagati, ha generato un volume di affari accertato di circa 10 milioni di euro, creando un mancato profitto alle società che forniscono il servizio di "Pay Tv".

Operazione "*PERUGIA 1*"

Il Centro Operativo per la sicurezza Cibernetica per l'Umbria, sotto la direzione del Servizio Polizia Postale in collaborazione con i C.O.S.C. di Milano, Napoli, Bologna e Ancona, ha dato esecuzione a 5 ordinanze di applicazione della misura cautelare degli arresti domiciliari, emesse dalla Procura della Repubblica di Perugia, nei confronti di alcuni cittadini italiani e stranieri originari del Marocco e della Costa d'Avorio per il reato di truffa attraverso dei raggiri effettuati mediante l'impiego di messaggi telefonici o di chiamate.

La tecnica utilizzata era sostanzialmente quella di carpire informazioni riservate dal punto di vista economico attraverso messaggi via cellulare: gli indagati, dopo aver individuato le ignare vittime ed aver accertato in capo a questi ultimi la titolarità di conti correnti, inviavano un SMS che, apparentemente proveniente dall'Istituto di Credito, anticipata una chiamata telefonica motivata da un accesso abusivo all'home banking da parte di ignari malfattori.

Dopo pochi minuti l'utente riceveva realmente una chiamata - da un finto operatore - nel

corso della quale veniva comunicata la presenza di un virus installato sul dispositivo mobile; a quel a quel punto il finto l'operatore, seguendo una procedura ormai ampiamente consolidata, chiedeva alla "vittima" di spegnere e riaccendere il dispositivo al fine di formattare il sistema e ripristinare le normali funzioni dell'apparato.

Tale operazione consentiva però l'installazione sull'applicazione bancaria del dispositivo - telefono o computer - di un dispositivo elettronico per mezzo del quale si rendeva possibile l'accesso al conto corrente della vittima.

I soldi prelevati venivano poi fatti confluire dagli indagati su carte di debito in modo da averne una immediata disponibilità. Attraverso questa tecnica è stato stimato un danno causato di circa 50mila euro.

Nel corso dell'esecuzione delle misure sono stati recuperati e sottoposti a sequestro circa 16mila euro di cui 8mila in contanti di vario taglio, unitamente a carte di credito e dispositivi informatici che saranno sottoposti a successiva analisi tecnica.

Operazione "*PERUGIA 2*"

In data 27 luglio 2022 questa Specialità, unitamente all'Arma dei Carabinieri, ha dato esecuzione a 11 Ordinanze di Custodia Cautelare suddivise in 4 carcere, 3 domiciliare e 4 con obbligo di presentazione alla P.G e altrettanti decreti di perquisizione locale e personale con contestuale sequestro, eseguite nelle città di Napoli, Padova e Perugia.

La complessa e articolata attività di indagine svolta ha permesso di evidenziare la sussistenza di un nutrito gruppo criminale composto da soggetti residenti nell'area campana ed umbra, con ramificazioni nel Nord Italia, dedito alla realizzazione di una pluralità di reati perpetrati con il seguente *modus operandi*:

- Truffe alle finanziarie ed agli Istituti di Credito finalizzate ad ottenere prestiti personali di denaro attraverso l'esibizione di documentazione fiscale e d'identità falsa e/o artatamente alterata, da destinare prevalentemente all'acquisto di veicoli di alta gamma per la successiva rivendita in virtù di una fitta rete di soggetti compiacenti. Nello specifico, il sodalizio dopo aver reclutato una persona solitamente priva di reddito o con reddito molto basso, mette a disposizione, oltre alla documentazione in questione, un copione con le istruzioni da seguire prima di recarsi presso l'ente finanziario. Dopo di che, ottenuto il prestito, l'organizzazione distribuisce la somma tra i sodali ed effettua solamente il pagamento delle prime tre rate del debito.
- Frodi informatiche perpetrate attraverso "*Smishing*" e "*Vishing*", nonché indebito utilizzo di sistemi di pagamento elettronico. Il gruppo campano realizza le frodi informatiche avvalendosi della rete di *money mules* presenti anche nel territorio umbro.

Operazione "*DREAM EARNINGS*"

Gli investigatori del Centro Operativo per la sicurezza Cibernetica della Polizia Postale del Friuli Venezia Giulia e della Squadra Mobile di Pordenone, con il coordinamento del Servizio Centrale Operativo, del Servizio Polizia Postale e delle Comunicazioni di Roma e la collaborazione del Servizio per la Cooperazione Internazionale di Polizia, unitamente all' Unità Crimini Informatici della Polizia albanese hanno disarticolato un'organizzazione dedita alle truffe perpetrate per mezzo del falso trading online.

Complesse tecniche d'indagine tradizionali e cibernetiche hanno portato alla luce uno schema criminale particolarmente complesso, che vedeva effettuare il riciclaggio delle somme sottratte in diversi Paesi membri U.E., fra i quali Cipro, Lituania, Estonia, Olanda e Germania, e la loro conversione in *criptovalute*. Le misure cautelari e i decreti di perquisizione sono state eseguite nei confronti di cittadini albanesi, tutti residenti a Tirana e facenti parte di un'organizzazione che si stima abbia truffato diverse centinaia di cittadini italiani.

L'ammontare della frode è di svariati milioni di euro ma questa potrebbe essere solo la punta dell'iceberg; solo all'esito dell'analisi dei sistemi informatici sequestrati sarà possibile determinare gli importi reali.

Nel corso di più di 42.000 intercettazioni telefoniche effettuate dagli investigatori italiani, è infatti emerso quanto i truffatori fossero abili nell'utilizzo di vere e proprie tecniche di persuasione e plagio, al punto da convincere le vittime a indebitarsi e versare, nel tempo, svariate centinaia di migliaia di euro.

Operazione "*KAFKA*"

La Polizia di Stato, a conclusione di una delicata attività d'indagine condotta dal Servizio Polizia Postale e delle Comunicazioni, ha eseguito 16 decreti di perquisizione personale e domiciliare, emessi dalle Procure della Repubblica di Brescia e Vicenza, con l'ausilio dei Compartimenti di Polizia Postale di Milano, Torino, Pescara, Trieste, Venezia e Roma.

Proprio come nel libro "Il processo" dello scrittore boemo, ignari utenti della rete si sono visti accusati, processati e condannati per delitti mai commessi; infatti l'indagine trae spunto dall'invio massivo di mail estorsive, apparentemente provenienti da Autorità istituzionali, contenenti una falsa citazione in Tribunale per fatti afferenti alla pedopornografia. Solo nel periodo di circa 2 mesi i proventi illeciti sono stati oltre di mezzo milione di euro.

La corrispondenza telematica oggetto di indagine riproduce un falso documento governativo e presenta nell'intestazione falsi loghi di Forze di polizia e di Ministeri italiani, tra i quali il Ministero dell'Interno e il Ministero della Difesa - affiancati a quelli di Agenzie internazionali quali Europol ed Interpol.

Il falso documento a firma di vertici di Istituzioni statuali quali il Capo della Polizia Lamberto Giannini, piuttosto che del Comandante Generale dell'Arma dei Carabinieri, Teo Luzi, dal Direttore del Servizio Polizia Postale, pro tempore, Nunzia Ciardi e dall'attuale Supplente del Direttore del Servizio Polizia Postale, Ivano Gabrielli.

L'atto fraudolento contesta all'utente violazioni gravissime, commesse attraverso la rete Internet, legate a condotte penalmente rilevanti riferite a delitti di molestie sessuali su minori.

Il documento minaccia di inoltrare le prove ad un non meglio specificato "Procuratore" ed ai media, invitando a fornire giustificazioni entro 72 ore.

Il passo successivo è una richiesta di denaro per far "decadere" le accuse e l'indicazione delle coordinate bancarie verso le quali corrispondere le somme estorte.

Il fenomeno che ha una rilevanza europea, colpisce in particolare Francia, Austria, Spagna, Belgio e Italia. Sono in corso i rituali accertamenti tecnici sul materiale informatico oggetto di perquisizione, al fine di delineare le responsabilità dei soggetti indagati nell'at-

tività delittuosa e la rete dei contatti coinvolti nell'invio delle mail estorsive con particolare attenzione ai collegamenti con l'estero.

Operazione "*MOSCOW MULE 2*"

Gli investigatori del Centro Operativo per la Sicurezza Cibernetica per la Liguria, coordinati dalla locale Procura della Repubblica, hanno ottenuto l'aggravamento degli arresti domiciliari e hanno arrestato nuovamente M.N., 40enne cittadina russa.

La donna era già stata arrestata nel capoluogo ligure nel mese di ottobre 2021. Nella vita di tutti i giorni si nascondeva dietro alla parvenza di una tranquilla madre di famiglia, in realtà si tratta di un'avvenente esperta hacker: un ingegnere informatico con la passione per il crimine e le *cryptovalute*.

Il Tribunale di Genova, nel mese di marzo 2022, aveva concesso alla donna gli arresti domiciliari presso un'associazione di volontariato del centro genovese impegnata nel recupero dei detenuti.

Le particolari attitudini, l'alto profilo criminale, hanno indotto gli investigatori della Polizia Postale a pianificare stretti contatti con la struttura presso la quale "l'ingegnere" era stata posta agli arresti domiciliari. Le continue richieste della donna di poter utilizzare un telefono o un computer hanno ulteriormente insospettito gli investigatori, che hanno predisposto delle attività tecniche di intercettazione ambientali e telematiche.

Da queste si è potuto avere la certezza che la donna, nonostante fosse agli arresti domiciliari aveva da subito cercato di riorganizzarsi, iniziando nuovamente a commettere frodi informatiche a danno di ignari cittadini.

L'hacker ha oltremodo dimostrato la propria capacità criminale avvedendosi dell'intercettazione telematica procedendo ripetutamente in continui tentativi di eludere le investigazioni e di cancellare le prove a proprio carico.

Nel corso della perquisizione domiciliare, gli esperti della Sezione *Financial Cybercrime* della Polizia Postale hanno sequestrato numeroso materiale, tra l'altro reperito dalla donna durante la detenzione domiciliare, che è tuttora sottoposto ad esame per ulteriori risvolti investigativi.

Operazione "*SIM SWAP*"

Nella giornata del 22 marzo 2022 personale della Specialità ha eseguito 2 provvedimenti di custodia cautelare degli arresti domiciliari, emessi dal Tribunale di Bologna, nei confronti di 2 soggetti italiani, operanti sul territorio nazionale, dediti alla frode informatica effettuata attraverso la tecnica c.d. "*SIM SWAP*".

L'attività nasce dalla denuncia di una vittima del ravennate, alla quale, i due soggetti hanno sottratto la somma di circa 75.000 euro. Tale somma è stata distolta con diversi bonifici a favore di conti correnti aperti presso banche italiane ma soprattutto estere.

Le attività di perquisizione eseguite contestualmente ai sopra citati provvedimenti hanno permesso di confermare, oltre al *modus operandi*, come l'attività criminale posta in essere fosse attuale e ancora in corso in quanto gli indagati sono stati trovati in possesso oltre all'attrezzatura informatica, di migliaia di dati relativi alle credenziali di accesso a conti correnti con la relativa indicazione dell'Istituto di Credito.

Operazione "*BOLTON*"

Al termine di un'accurata attività investigativa in materia di abusivismo finanziario effettuato promuovendo la compravendita di strumenti finanziari dietro la promessa di profitti elevati, il Centro operativo per la sicurezza cibernetica di Cagliari unitamente a personale della Guardia di Finanza, in data 16 aprile 2022 ha dato seguito a misure cautelari personali e patrimoniali disposte dal Giudice per le indagini preliminari del Tribunale di Cagliari nei confronti di 6 persone gravemente indiziate, unitamente ad altri 4 indagati denunciati a piede libero.

L'indagine che trae origine da numerose denunce per frode, ha consentito di ricostruire lo schema illecito utilizzato (c.d. schema Ponzi) e la rete posta in essere dai sodali.

Gli indagati, per i delitti di associazione per delinquere finalizzata, alla truffa, al riciclaggio e autoriciclaggio, avevano costituito un reticolo di società finanziarie, anche di diritto estero, strumentali al procacciamento di clienti.

Nel corso dell'operazione sono stati eseguiti sequestri preventivi, finalizzati alla confisca anche per equivalente, di beni e disponibilità finanziarie per un importo complessivo di oltre 4.500.000 euro. Tra i beni sequestrati vi sono disponibilità finanziarie, quote societarie ed una struttura alberghiera ubicata dell'hinterland cagliaritano, del valore stimato di circa 1.500.000 euro, la cui acquisizione da parte del *dominus* dell'associazione criminale è avvenuta mediante il coinvolgimento di un prestanome.

Cyberterrorismo

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista, sia di formazioni di estrema destra (neonazismo, neofascismo, tifoserie strutturate, suprematismo), nonché di estrema sinistra (movimenti di lotta armata, anarchici, insurrezionalisti, antagonisti).

In tale ambito, la Polizia Postale garantisce sia 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 dei contenuti illeciti, sia 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.

Trattandosi, in particolare, di un fenomeno di carattere transnazionale, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.

Cyberterrorismo	2021	2022
Casi trattati	1.339	1.197
Persone indagate	82	66
Spazi virtuali monitorati	128.409	175.572

1- Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico

In ambito europeo, proprio al fine di garantire la cooperazione internazionale, il Servizio Polizia Postale e delle Comunicazioni rappresenta il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti terroristici diffusi in rete e di orientarne l'attività.
In tale ambito, l'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare in primis come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento qualitativo, determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente dell'Intelligenza Artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.
Sul punto, tra le attività effettuate dalla Specialità si segnala quella effettuata dal Centro Operativo per la Sicurezza Cibernetica e dalla DIGOS di Perugia, all'esito della quale un cittadino marocchino di 54 anni è stato espulso dal territorio nazionale, in quanto autore di una prolifica attività propagandistica sul social network Facebook realizzata attraverso numerosi post e commenti a sostegno dei "fratelli musulmani" e del Jihad, specificamente della Palestina contro Israele, nel corso della quale si è definito un "mujahidin" pronto ad aiutare la causa.
In analogia a quanto sin qui evidenziato con riferimento alla propaganda jihadista, anche nell'ambito dei fenomeni di radicalizzazione online legati all'ideologia neofascista e xenofo/razziale, il web si conferma lo strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, nonché per il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.
Appare opportuno evidenziare come il movimento "suprematista bianco" si basi su una importante attività di propaganda di dottrine ideologiche come il neonazismo, il razzismo, l'identitarismo e l'etnocentrismo, che avviene soprattutto all'interno di piattaforme di comunicazione online "riservate", diverse dai principali social network.
La costante attività di monitoraggio informativo ed investigativo ha permesso di accertare come nel corso degli ultimi mesi si sia stato registrato un notevole incremento dei trend e delle discussioni all'interno di chat in diverse piattaforme; si passa dai tradizionali gruppi Facebook (molti dei quali risultano essere già stati bloccati) a social meno noti, come Reddit, fino a piattaforme come 8chan, vk.com (Vkontakte), nonché Telegram, privilegiando tutte quelle piattaforme che per la propria policy garantiscono l'anonimato e rendono più

complicata l'identificazione degli autori dei messaggi.
Alla luce di quanto premesso, appare opportuno evidenziare come gli operatori della Specialità abbiano intensificato le attività di monitoraggio proprio in tali contesti e, in raccordo con la Direzione Centrale della Polizia di Prevenzione, abbiano avviato numerose attività investigative, con il deferimento alle competenti Autorità Giudiziarie dei soggetti identificati – anche attraverso attività sotto copertura e perquisizioni – quali autori dei messaggi connotati dalla discriminazione razziale, etnica e religiosa.
Tra le numerose attività d'indagine, a titolo esemplificativo, merita di essere menzionata quella avviata dal C.O.S.C. e dalla D.I.G.O.S. di Torino che ha permesso di individuare un gruppo di matrice nazi-fascista, attestato sulla piattaforma Telegram, sul canale "Brudershaft thule" ("Fratellanza di Thule") e sul connesso gruppo di discussione "Meine Ehre Heiβt Treue" ("Il mio onore si chiama lealtà"), partecipato da militanti stanziati su tutto il territorio nazionale e anche all'estero, in Germania, tutti denunciati per riorganizzazione del disciolto partito fascista e propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa.
Tra le numerose attività investigative effettuate nella tematica in argomento, si segnala anche quella avviata dal Centro Operativo per la Sicurezza Cibernetica di Bari e dalla DIGOS di Lecce, che ha permesso di identificare e deferire alla competente A.G. l'autore dell'intrusione informatica nella seduta del Consiglio Comunale di Trieste, tenutasi online nel mese di febbraio 2022 mediante la piattaforma "GoToMeeting", diffondendo immagini di soggetti (non visibili in volto) che esibivano delle magliette con il noto logo del movimento di protesta "V_V", nonché frasi provocatorie e diffamatorie di chiaro orientamento "No-vax" e "no grenn-pass", rendendo di fatto impossibile la prosecuzione della seduta del Consiglio Comunale.
Degna di essere menzionata risulta essere l'attività investigativa che ha portato in data 30/11 u.s., all'esecuzione di perquisizione a carico di sei soggetti, tre maggiorenni e tre minorenni, anche per il reato di propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604 bis c.p.).
L'indagine è stata avviata nell'ambito del monitoraggio del gruppo Telegram "Blocco Est Europa" nel quale venivano condivisi contenuti violenti riconducibili a materiale diffuso da gruppi terroristici islamisti di matrice jihadista, messaggi e post inerenti alla pornografia minorile, uccisioni brutali, stragi terroristiche, razzismo, misoginia, "school shooting" e violenza in genere con esplicite dichiarazioni di propaganda dell'odio razziale accompagnate dall'istigazione al compimento di atti di violenza di matrice discriminatoria e attentati contro le istituzioni a livello nazionale.
Il canale - creato il 23 gennaio 2022 e sospeso dal provider il successivo 2 aprile - è stato utilizzato per divulgare messaggi basati sull'odio antisemita e nei confronti delle persone di colore, attestazioni di stima per Hitler e le teorie naziste accompagnate dal disprezzo per le Istituzioni e le Forze dell'Ordine oltre ad un'accentuata misoginia da cui deriva divertimento per la visione di video di donne, per lo più minorenni, che si suicidano o che vengono violentate o uccise.

Sul gruppo "Blocco Est Europa" sono state inoltre postate immagini relative ad addestramenti con armi ad aria compressa effettuati dagli indagati verso bersagli raffiguranti persone esistenti, tra cui importanti Personalità dello Stato.
Correlato alle predette finalità è anche il progetto di realizzare uno "school shooting" come dimostrato da commenti e fotografie riferite a stragi compiute da giovanissimi nelle scuole.
Sempre mediante il predetto canale, gli indagati hanno inoltre condotto un'intensa attività di propaganda ispirata all'odio razziale e al nazionalsocialismo, alla misoginia e all'intolleranza e alla violenza in generale e condiviso numerosi file dai contenuti pedopornografici.
Proprio quest'ultima circostanza ha determinato per i tre maggiorenni, tutti di 21 anni, l'emissione da parte della competente A.G. di due ordinanze di misura cautelare in carcere ed una ai domiciliari. Mentre i restanti tre minorenni, con età compresa tra i 13 e i 14 anni, sono stati denunciati a piede libero.
Nell'ambito del contenimento e del contrasto della minaccia ibrida, la Polizia Postale sta anche svolgendo dedicati approfondimenti info-investigativi con riferimento al conflitto bellico in atto tra Russia e Ucraina, finalizzati alla prevenzione e al contrasto dei fenomeni criminali nelle materie di competenza, ovvero nel concorso alla corretta gestione dell'ordine e sicurezza pubblica.
Infine, considerando il carattere transnazionale che spesso connota le attività investigative in argomento, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali. In ambito europeo, il Servizio Polizia Postale e delle Comunicazioni è il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda terroristica diffusi in rete e di orientarne l'attività.
Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche appositamente create in ambito IRU a supporto del monitoraggio e delle indagini in materia di terrorismo in Internet.
Proprio nell'ambito della lotta ai crimini ispirati dall'odio, nello scorso mese di aprile, la Polizia Postale ha partecipato alla giornata di azione congiunta a livello dell'U.E., sostenuta da Europol, che, oltre l'Italia, ha coinvolto 10 Paesi (Austria, Bulgaria, Francia, Germania, Lituania, Lussemburgo, Norvegia, Portogallo, Romania e Spagna).
Le attività investigative hanno permesso di identificare in tutta Europa 176 persone in relazione alla diffusione online di messaggi di incitamento all'odio xenofobo-razziale, nonché istigazione alla violenza.
Nella circostanza, le Forze dell'ordine degli Stati membri hanno anche lavorato insieme per far aumentare la consapevolezza di individui e gruppi che Internet non rappresenta un "vuoto giuridico", dando così un chiaro segnale alle persone che diffondono odio violento online che le azioni investigative congiunte saranno sempre più frequenti e consistenti.
Da ultimo, lo scorso 15 dicembre, la Polizia Postale e la D.C.P.P. hanno partecipato ad una seconda giornata congiunta, coordinata dall'European Union Internet Referral Unit (EU

IRU) di Europol, nell'ambito del Referral Action Day (RAD) contro i contenuti violenti dell'estremismo di destra e del terrorismo online. L'attività ha coinvolto anche le Unità specializzate di 14 Paesi, tra cui 13 Stati membri dell'Unione Europea e un Paese non appartenente all' UE.

Le autorità partecipanti sono state coinvolte nell'individuazione e nella segnalazione di contenuti terroristici ai fornitori di servizi online e nel valutare le loro risposte. Le attività hanno portato alla segnalazioni di 831 elementi a 34 piattaforme interessate. Il materiale in questione include contenuti vietati prodotti da organizzazioni estremiste di destra o in favore di queste, nonché contenuti diffusi relativi ad attacchi terroristici motivati dall'estremismo violento.

Tali materiali includono livestream, manifesti, rivendicazioni e celebrazioni di attentati. L'estremismo violento è ancora una preoccupazione crescente dopo i fatti di Bratislava (Slovacchia) e Buffalo (USA).

Gli autori di questi attentati facevano parte di comunità online transnazionali e si sono ispirati ad altri estremisti di destra violenti e terroristi. Nei loro manifesti, i terroristi hanno evidenziato il ruolo centrale della propaganda online nei processi di radicalizzazione. Questo dimostra come l'abuso di internet continui ad essere un aspetto importante per la radicalizzazione e reclutamento della destra violenta.

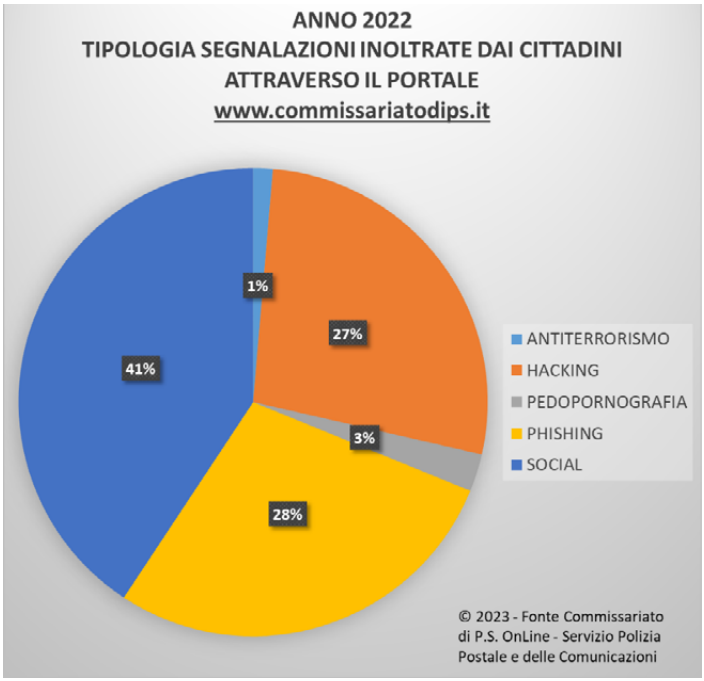
Dal primo Referral Action Day dedicato a questo tipo di contenuti online nel 2021, la minaccia rappresentata dall'estremismo violento e dal terrorismo è ancora in aumento.

I RAD consolidano gli sforzi delle forze dell'ordine per contrastare la creazione e la diffusione di propaganda estremista e terroristica online. Durante le attività coordinate, i partecipanti segnalano i contenuti legati al materiale di propaganda ai fornitori di servizi online invitandoli a valutare e rimuovere i contenuti che violano i loro termini di servizio. Le piattaforme sono invitate a rafforzare i loro protocolli di moderazione per evitare questo tipo di abuso in futuro.

Commissariato di P.S. Online

Per consentire agli utenti del *web* di avere delle risposte in tempo reale su ciò che accade nella rete ed evitare loro di cadere nelle tante insidie della navigazione in Internet, è attivo, ormai da anni, il Commissariato di P.S. Online, portale della Polizia di Stato (raggiungibile attraverso la url www.commissariatodips.it) gestito da investigatori, tecnici ed esperti della Polizia Postale e delle Comunicazioni, che offre agli utenti diversi servizi in materie giuridiche e sociali.

In particolare, il sito è un importante strumento di interazione con i cittadini che, ogni giorno, inviano in media 400 messaggi tra segnalazioni e richieste di informazioni e che allo stesso tempo viene utilizzato per veicolare loro notizie e consigli utili per un uso sicuro, consapevole e responsabile della rete: un dato che offre un chiaro riscontro del sempre alto livello di interazione con gli utenti.
Nell'anno 2022 il Commissariato di P.S. Online ha ricevuto più di 100.000 segnalazioni e 25.792 richieste di informazioni. La popolarità del sito è confermata anche dal numero degli accessi,[2] che sono stati nel periodo di riferimento oltre 42.000.000.



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

Segnalazioni pervenute al Commissariato di P.S. OnLine nel 2022	ANTITERRORISMO	1.364
	HACKING	27.512
	PEDOPORNOGRAFIA	2.615
	PHISHING	28.395
	SOCIAL	41.116
	TOTALE	**101.002**

Informazioni pervenute al Commissariato di P.S. OnLine nel 2022	25.792
Visite al portale web del Commissariato di P.S. OnLine nel 2022	2.597.545
Accessi al portale web del Commissariato di P.S. OnLine nel 2022	42.494.652

Nel portale è presente una sezione dedicata alle "news" in cui vengono pubblicati veri e propri *alert* riguardanti situazioni di pericolo nelle quali si può incorrere navigando sul web e con cui gli utenti vengono informati circa i fenomeni del momento. Nella medesima sezione vengono, inoltre, pubblicati i comunicati stampa relativi alle più importanti operazioni della polizia postale.

Sul sito web sono, altresì, presenti pillole di *cyber hygiene*, cioè tutti quei principi che privati e aziende devono necessariamente seguire per ridurre al minimo i rischi derivanti dall'utilizzo di sistemi informatici.

In tale direzione si rivolge anche l'attività costante di contrasto al fenomeno della disinformazione, agevolato dalla diffusione delle cd. *fake news*, attraverso la predisposizione e diffusione di specifici *alert*, funzionali alla veicolazione delle corrette informazioni.
Il personale del Commissariato di P.S. online si trova spesso ad operare come una vera e propria sala operativa, dal momento che, spesso, giungono sul sito segnalazioni di utenti in pericolo o che minacciano gesti estremi; in considerazione della gravità di tali circostanze, è richiesto un tempestivo e coordinato intervento degli operatori presenti in sala con quelli dislocati presso uffici territoriali delle Questure interessate. Gli interventi finalizzati alla prevenzione di intenti suicidari da parte di utenti dei vari *social network* segnalati nel 2022 attraverso il Commissariato di P.S. online sono stati 64.

Campagne preventive di sensibilizzazione

In considerazione della specificità dei fenomeni di cui si occupa e che incidono in maniera diretta e profonda sulla vita delle persone, soprattutto in ambiti estremamente delicati come la tutela dei minori e delle fasce più esposte della cittadinanza, la Polizia Postale e delle Comunicazioni svolge un'intensa attività di comunicazione, nell'ottica della massima vicinanza al cittadino e di una "educazione al digitale" che consenta a giovani ed adulti un corretto approccio all'uso di internet ed una consapevolezza sempre crescente dei rischi e pericoli del web.

L'attività di prevenzione della Specialità, oltre che nel continuo monitoraggio della rete, si esplica infatti da anni e con un costante ed incessante impegno, attraverso la progettazione e realizzazione di campagne di sensibilizzazione e di educazione al corretto uso delle tecnologie, nel tentativo di far comprendere agli adolescenti, che spesso 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, che vede il coinvolgimento delle scuole di ogni ordine e grado.

Il progetto, arrivato quest'anno alla sua decima edizione, è proseguito anche durante il biennio contrassegnato dalla pandemia con sessioni multimediali online ed ha ripreso la sua attività itinerante in Italia e all'estero attraverso il *truck* simbolo dell'iniziativa al ritorno dei ragazzi in aula.

A bordo del *truck*, che si trasforma in una vera e propria aula multimediale e che raggiunge di volta in volta le città individuate per le tappe, gli operatori della Specialità accolgono le numerose scolaresche e la cittadinanza presente, illustrando loro le più attuali insidie della rete e fornendo utili strumenti per una corretta navigazione.

L'impegno profuso dagli specialisti della Polizia Postale e delle Comunicazioni nell'azione di sensibilizzazione/informazione sull'uso sicuro e responsabile della rete, ha consentito, nel corso dell'anno 2022, di realizzare incontri con 2.500 Istituti scolastici, veicolando contenuti a studenti, docenti, genitori e altre figure di riferimento per i ragazzi.

Queste dirette opportunità di incontro con i giovani acquisiscono particolare rilevanza per l'azione preventiva svolta nei confronti di determinate fenomenologie delittuose, considerato che proprio in queste occasioni spesso emergono episodi o situazioni che permettono quel tempestivo intervento utile ad impedire la consumazione di un reato o l'aggravarsi delle conseguenze di condotte illecite.

Tra queste, un fenomeno che continua a destare grande allarme sociale e nei confronti del quale l'attività di prevenzione della Specialità si rivolge ormai da anni, con costanza e dedizione, è il cyberbullismo. I casi trattati lo scorso anno sono stati 326, con 129 minori indagati.

Una coinvolgente campagna realizzata periodicamente in questa prospettiva dalla Polizia Postale e delle Comunicazioni è il format teatrale #cuoriconnessi dedicato agli studenti delle scuole, con il quale, attraverso uno spettacolo in cui il conduttore concentra l'attenzione del pubblico sull'importanza delle parole in tutte le sue sfumature, con filmati,

letture, musiche e testimonianze dirette, vengono fornite agli spettatori informazioni utili alla corretta navigazione in rete, volte anche a stimolare nei ragazzi una sempre maggiore consapevolezza della gravità delle azioni prodotte online, in relazione all'impatto prodotto nella vita dei loro coetanei.
Per l'anno 2022, la 6^ edizione della citata manifestazione è stata realizzata in concomitanza con il Safer Internet Day, giornata mondiale per la sicurezza in Rete, con un grande evento online, durante il quale la Polizia di Stato si è collegata, attraverso una piattaforma dedicata, con oltre 270 mila studenti.
Il 17 marzo 2022, inoltre, è stato presentato, presso l'Auditorium parco della Musica di Roma, alla presenza del Signor Capo della Polizia Prefetto Lamberto Giannini, il docufilm "Haters e piccoli eroi", con protagonista Valerio Catoia, ragazzo con la sindrome di Down nominato "Alfiere della Repubblica" e "Poliziotto ad Honorem". Il video è stato realizzato dalla Polizia di Stato in collaborazione con l'istituto di cinematografia "Roberto Rossellini" di Roma e narra la storia di questo ragazzo speciale, raccontata da ragazzi come lui, attraverso un linguaggio amato dagli adolescenti, per combattere il cyberbullismo. Valerio è un campione dei Gruppi sportivi paralimpici italiani e, a soli 17 anni, ha salvato da sicuro annegamento una bambina di 10 anni travolta dalle onde del mare. Nonostante il gesto eroico e i riconoscimenti istituzionali conseguiti, è stato oggetto di ripetuti insulti sui canali social. Grazie anche al sostegno della famiglia e all'intervento della Polizia Postale e delle Comunicazioni, Valerio ha trovato la forza di reagire a questa situazione ed è stato il testimonial della campagna della Polizia Postale e delle Comunicazioni per prevenire il fenomeno del cyberbullismo tra gli adolescenti. All'evento hanno assistito oltre 1000 studenti delle scuole di Roma.

La situazione della Email Security in Italia nel 2022

[A cura di Rodolfo Saccani, Libraesva]

Trend generali:
- minori volumi ma maggiore sofisticazione negli attacchi
- crescita degli attacchi basati su link e dell'abuso di servizi cloud
- diffusione di DMARC e crescita della consapevolezza

Ne è passato di tempo dal 1971 quando Ray Tomlinson, un ingegnere informatico, sviluppò il primo sistema di posta elettronica che utilizzava la rete ARPANET, una delle prime reti di computer che sarebbe poi diventata la base di Internet.

Nel 1982, l'Internet Engineering Task Force (IETF) pubblicò la prima versione ufficiale del protocollo SMTP (Simple Mail Transfer Protocol), che definiva come gli host su Internet dovessero scambiarsi email. Questa versione di SMTP consentiva ai server di posta elettronica di inviare e ricevere messaggi utilizzando un formato standardizzato, che è ancora in uso oggi.

Negli anni successivi, SMTP è diventato uno dei pilastri delle comunicazioni su Internet. Con il tempo, sono stati sviluppati molti altri protocolli e tecnologie che hanno migliorato la sicurezza, la privacy e la funzionalità della posta elettronica, ma SMTP è rimasto uno dei principali meccanismi per lo scambio di informazioni su Internet.

In sintesi, la storia di SMTP rappresenta un esempio di come la tecnologia della comunicazione sia continuamente evoluta nel corso del tempo per soddisfare le esigenze degli utenti e delle organizzazioni. Nonostante le sue origini relativamente semplici, SMTP è diventato un componente essenziale della nostra vita digitale e continua a evolversi per soddisfare le nuove esigenze della società.

Nonostante la sua veneranda età, ad oltre 50 anni dal suo concepimento l'email rappresenta il principale mezzo di comunicazione per organizzazioni ed aziende. Ciò rende l'email anche il canale più abusato per condurre attacchi informatici, che sono diventati sempre più sofisticati e mirati. La semplicità d'uso e la diffusione capillare della posta elettronica la rendono un bersaglio ideale per i criminali informatici.

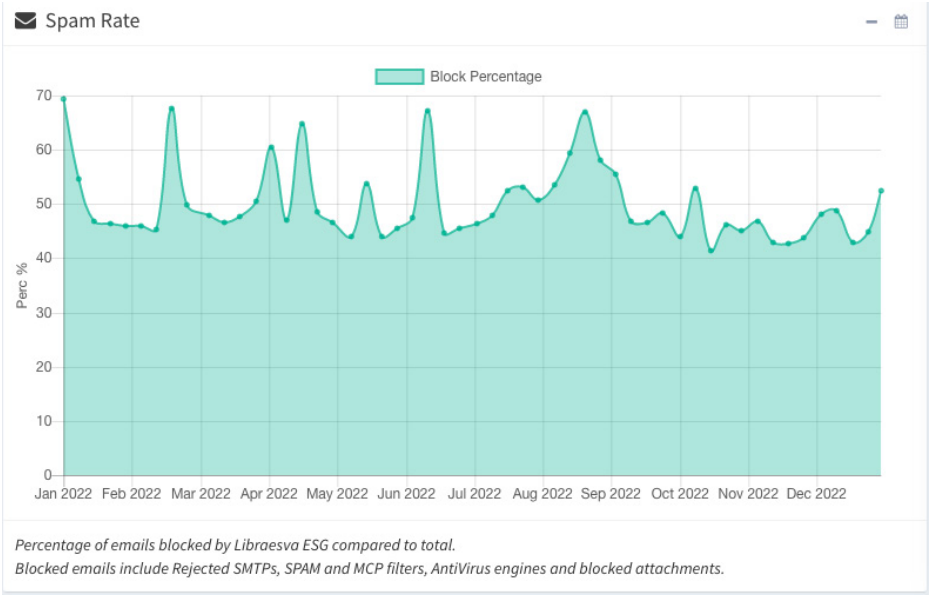


Figura 1: *Percentuale di email bloccate sul totale*

In generale circa la metà dei messaggi inviati o ricevuti dalle organizzazioni sotto monitoraggio nel 2022 sono stati bloccati. La gran parte di questi messaggi (il 35% circa del totale) è stato intercettato dai sistemi di filtraggio a livello di trasporto, che scremano il traffico di più bassa qualità. Tali filtri includono blacklist, SPF (Sender Policy Framework), e altri controlli tecnici sul trasporto fisico delle email. Inoltre, i controlli sul contenuto intercettano circa l'8% del totale dei messaggi in transito.

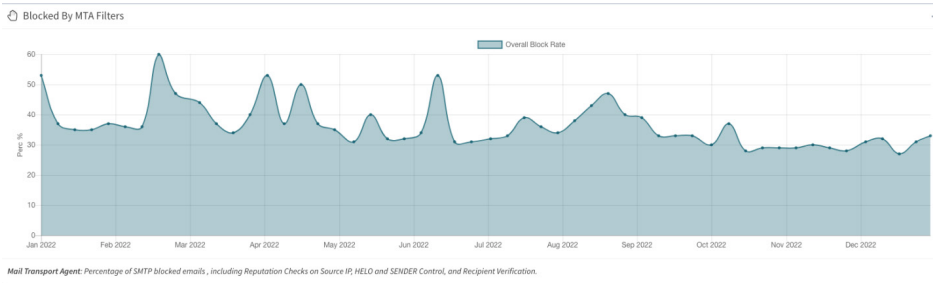


Figura 2: *Percentuale di email bloccate da controlli di trasporto SMTP*

Figura 3: *Percentuale di email bloccate dalle analisi di contenuto*

Se il volume di messaggi malevoli o indesiderati sembra decrescere (ma non è detto che sia una tendenza che verrà mantenuta nel tempo), il livello di sofisticazione degli attacchi sale. Solo l'1,5% degli allegati contenuti nei messaggi di posta appartiene alla categoria degli eseguibili nelle loro varie forme, una forma di attacco sempre meno diffusa ed efficace. Questi tipi di file, quando allegati ad un messaggio di posta, sono virtualmente al 100% pericolosi. La tecnica di nasconderli all'interno di archivi, talvolta cifrati, è ormai obsoleta e poco efficace in quanto i sistemi di sicurezza hanno sviluppato tecnologie per rilevare e bloccare questo tipo di attacchi.

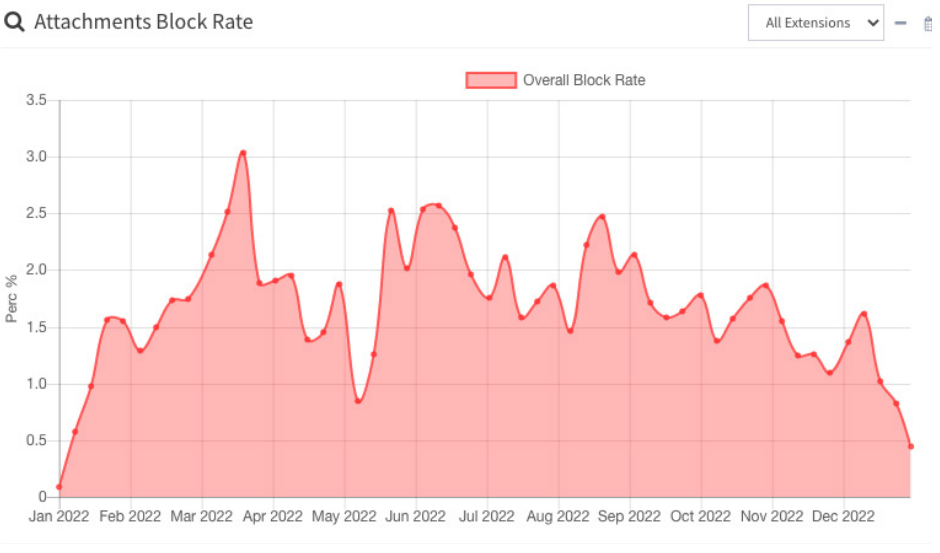


Figura 4: *Percentuale di allegati bloccati sul totale*

I documenti office e i file PDF, regolarmente scambiati per usi legittimi, sono sempre più frequentemente abusati dai cyber criminali per diffondere codice malevolo. Il contenuto pericoloso può essere offuscato per cercare di evadere i controlli dei sistemi di sicurezza. Circa il 4% dei documenti ricevuti via email appartengono a questa categoria, e solo in percentuali molto basse vengono intercettati dagli antivirus.

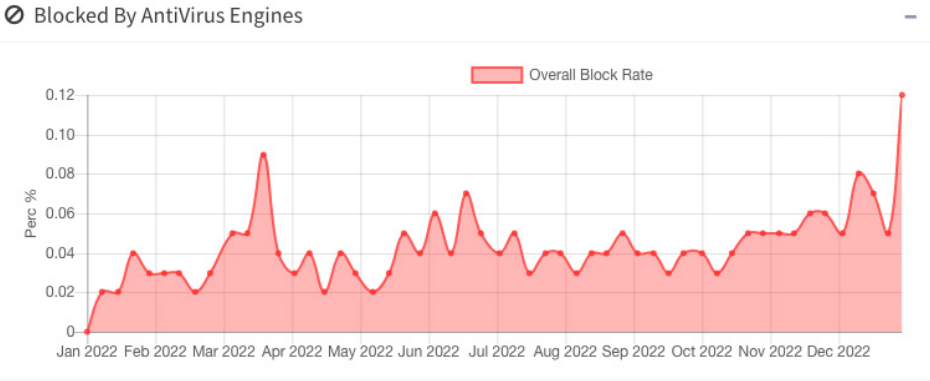


Figura 5: *Percentuale di email bloccate dagli engine antivirus*

La posta elettronica è il primo punto di ingresso per le nuove famiglie e varianti di malware e gli autori stanno diventando sempre più attenti e abili nello sviluppare dropper che possano evadere le tecniche di rilevamento più diffuse (il dropper è il piccolo codice malevolo solitamente allegato all'email che si occupa di installare il malware vero e proprio). Questo rende ancora più importante che le organizzazioni implementino solide misure di sicurezza in grado di rilevare le minacce zero-day.

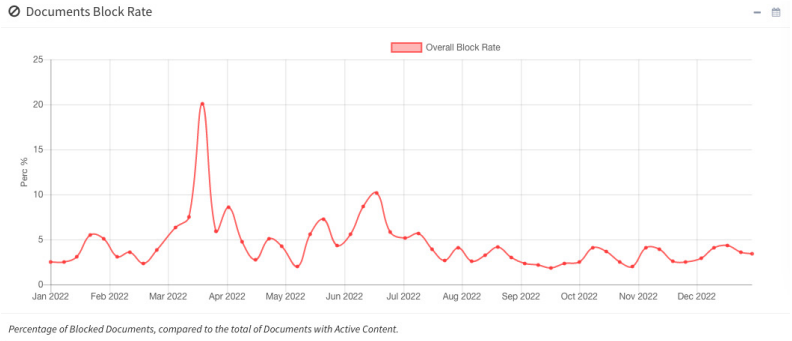


Figura 6: *Percentuale di documenti bloccato sul totale di documenti con contenuto attivo (macro o altro codice)*

La tendenza alla specializzazione degli autori di campagne di ransomware sta diventando sempre più consolidata, così come l'utilizzo della "double extorsion" da parte degli attaccanti. In queste campagne, i dati vengono esfiltrati prima di essere crittografati dal malware, e il riscatto viene chiesto non solo per ottenere la chiave per decifrare i dati, ma anche per evitare la pubblicazione dei dati esfiltrati. Ciò significa che le vittime sono costrette a pagare il riscatto per proteggere la privacy dei propri dati e prevenire conseguenze negative per la propria reputazione. Questo metodo è molto efficace perché, anche se un'organizzazione ha un piano di disaster recovery efficiente, potrebbe comunque essere costretta a pagare il riscatto per proteggere i propri dati sensibili. È quindi importante che le organizzazioni implementino solide misure di sicurezza per prevenire questo tipo di attacchi e per proteggere i propri dati.

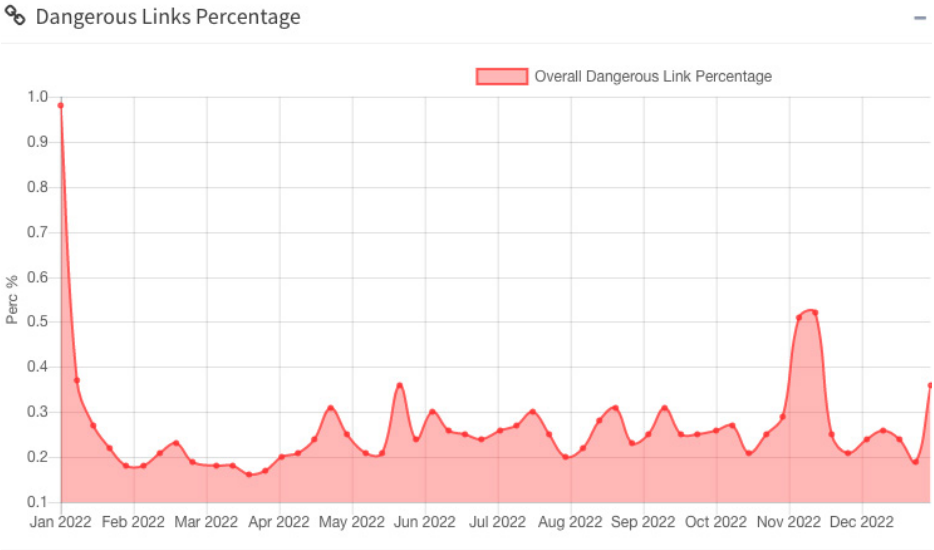


Figura 7: *Percentuale di link pericolosi sul totale di link consegnati e cliccati*

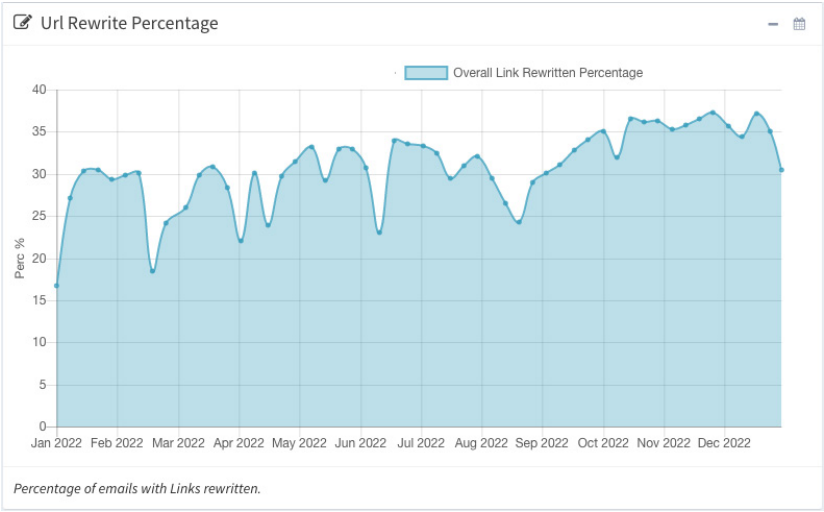


Figura 8: *Percentuale di email contenenti link*

A dimostrazione della crescente cura e professionalità nella conduzione di campagne malevole, nel 2022 abbiamo rilevato che alcuni gruppi di criminali informatici creavano riproduzioni molto fedeli di servizi legittimi di sicurezza di vari vendor al fine di dare credibilità ai propri attacchi. Tra questi, una finta sandbox di Libraesva che appariva molto simile a quella vera e fingeva di analizzare il link cliccato dalla vittima nel tentativo di convincerla che il messaggio fosse stato analizzato e non rappresentasse una minaccia. In realtà, la sandbox falsa portava la vittima ad un sito di phishing che consentiva ai criminali di raccogliere le credenziali di accesso e di infiltrarsi nei sistemi informatici delle organizzazioni.

Figura 9: *Emulazione della sandbox di Libraesva per dare credibilità a una campagna di phishing*

La tendenza all'invio di link malevoli per attacchi di phishing o malware sta crescendo. Gli autori di questi attacchi usano sempre più spesso servizi legittimi come OneNote o altri servizi di Microsoft e Google, piattaforme di storage cloud come quelle di Amazon e di altri fornitori di servizi di object storage, piattaforme per l'email marketing, oppure siti internet legittimi che sono stati compromessi. Questo rende più difficile per i sistemi di sicurezza individuare e bloccare questi link malevoli. Inoltre, l'utilizzo di account di posta legittimi

per inviare questi link rende ancora più complicato il loro rilevamento. Nonostante questo, nelle nostre misurazioni solo una piccola percentuale di questi link riesce ad arrivare all'inbox dell'utente. Tuttavia, anche se solo lo 0,3% di questi link riesce a raggiungere la destinazione, questo significa che potenzialmente milioni di link malevoli possono essere a disposizione degli utenti. Una volta che un link malevolo arriva nella inbox, la probabilità che venga cliccato e che il dispositivo venga compromesso è molto alta e come ben sappiamo, una sola compromissione può avere conseguenze molto costose. L'analisi dei link al momento del click offre un livello di protezione aggiuntivo importante.

L'utilizzo dei link malevoli per perpetrare attacchi è un fenomeno in costante crescita, con il 60% circa delle campagne di phishing che fanno affidamento su questa tecnica e il 40% che viene utilizzato per la distribuzione del malware. L'obiettivo dei cyber criminali è quello di ingannare gli utenti facendoli cliccare su link apparentemente innocui, ma che in realtà conducono a siti o domini compromessi. Questi siti possono essere utilizzati nello stesso momento sia per scopi di phishing che per la diffusione di malware, rendendo così l'identificazione della minaccia più difficile. Inoltre, l'utilizzo di domini e siti legittimi compromessi aumenta la credibilità del link e aumenta le probabilità che gli utenti clicchino su di essi, mettendo così a rischio la sicurezza dei loro dispositivi e delle loro informazioni personali.

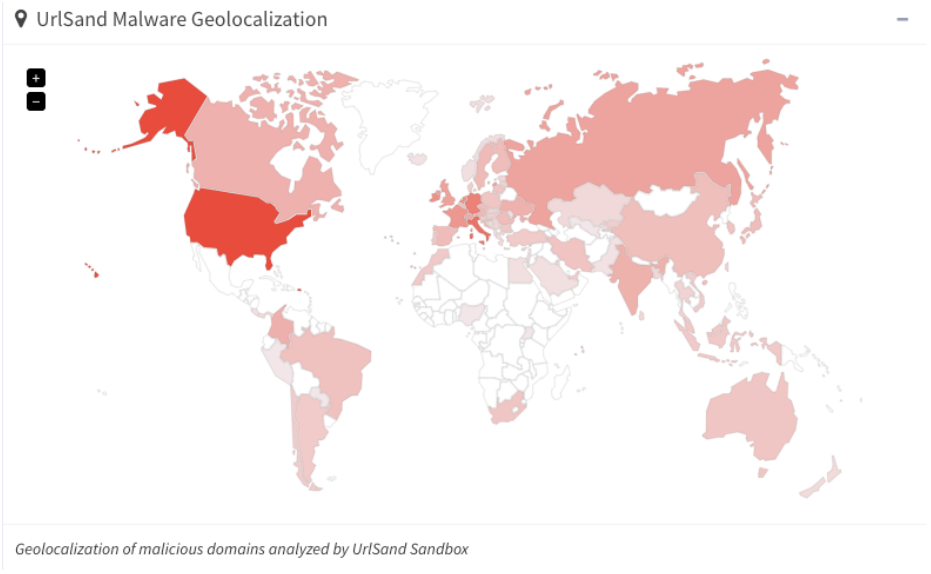


Figura 10: *Geo-localizzazione dei domini malevoli analizzati dalla UrlSand sandbox*

La distribuzione geografica dei servizi web che ospitano contenuti malevoli vede gli Stati Uniti come leader, a causa della grande quantità di servizi cloud presenti sul territorio e della loro frequente utilizzazione da parte degli attaccanti per diffondere questi tipi di minacce. Inoltre, la presenza di una vasta rete di infrastrutture tecnologiche e di un alto tasso di adozione di tecnologie avanzate, rende il territorio statunitense particolarmente vulnerabile alle campagne di questo tipo. Nonostante gli sforzi delle autorità competenti e dei fornitori di servizi per garantire la sicurezza dei propri sistemi, gli attaccanti riescono spesso a eludere le misure di protezione e a utilizzare questi servizi come piattaforme per attività malevoli.

La tecnica dell'utilizzo di servizi di shortening è uno dei tentativi più comuni di eludere la rilevazione, ma i sistemi di sicurezza delle email sono sempre più sofisticati e in grado di effettuare la risoluzione di questi link in tempo reale. Inoltre, l'uso di link che puntano a siti web legittimi compromessi è molto diffuso e spesso viene utilizzato per creare un percorso tortuoso che nasconde la vera destinazione del link. Il passaggio intermedio serve a rendere il link meno individuabile e a prevenirne il blacklisting. In alcuni casi, viene utilizzato anche un doppio o triplo passaggio intermedio per aumentare la difficoltà nell'individuare la destinazione finale. È importante essere consapevoli di queste tecniche e di utilizzare strumenti di sicurezza affidabili per proteggere i propri sistemi da questi attacchi.

Si rileva un incremento del 30% circa nell'adozione del DMARC. DMARC (Domain-based Message Authentication, Reporting and Conformance) è uno standard di autenticazione delle email che aiuta a prevenire la falsificazione del mittente (spoofing) e il phishing. Fornisce anche un meccanismo per la generazione di report sul come il proprio flusso di posta viene trattato dai servizi destinatari e sui tentativi di invio di email sospette o non autorizzate dal dominio del proprietario. In sintesi, DMARC fornisce maggiore sicurezza e trasparenza nell'invio e nella ricezione di email e la crescita della sua adozione da parte delle organizzazioni italiane è un segnale positivo. Una maggiore adozione di DMARC può indicare che le organizzazioni stanno diventando sempre più consapevoli della necessità di proteggere la propria reputazione online e di prevenire frodi. In generale, la crescita dell'adozione di DMARC indica che le organizzazioni stanno prendendo sul serio la sicurezza delle email e stanno lavorando per creare un ambiente più sicuro per le comunicazioni via email.

Le proiezioni per il futuro della sicurezza delle email indicano che le minacce informatiche continueranno a evolversi e che saranno necessarie sempre più misure di sicurezza per proteggere le email. Ci si aspetta inoltre una maggiore adozione di standard di autenticazione come DMARC, SPF e DKIM, che aiutano a prevenire il phishing e la falsificazione del mittente.

Le tensioni geopolitiche richiedono una particolare attenzione nei confronti dell'utilizzo delle email come mezzo per condurre attacchi informatici contro obiettivi strategici e infrastrutture critiche. Il 2022 ci ha dato una anticipazione di questo rischio attraverso numero-

se compromissioni di organizzazioni rilevanti con impatti più o meno marcati sulla capacità operativa. Tutte le organizzazioni governative sono spinte ad adottare politiche più rigide per la protezione delle proprie email e collaborare con altre nazioni per prevenire attacchi informatici.

Le minacce informatiche continueranno a rappresentare una sfida per la sicurezza delle email, e le organizzazioni dovranno continuare a investire in tecnologie di sicurezza avanzate e in programmi di formazione per i propri dipendenti per prevenire la diffusione di email dannose. In sintesi, la sicurezza delle email rimarrà un'area critica di attenzione per le organizzazioni e per i fornitori di posta elettronica nei prossimi anni.

Sanità, tra cyberattacchi e rischi per la salute

[A cura di Sonia Montegiove, Sofia Scozzari e Anna Vaccarelli, Women for Security]

Quello della sanità è, nel 2022, il secondo settore più colpito dagli attacchi informatici dopo "multiple targets", con una percentuale sul totale del 12,2 per cento. I cyber attacchi registrati sono stati in totale 304 (a fronte di un numero complessivo record pari a 2.489), quasi tutti riferibili a "cybercrime" e uno soltanto riconducibile ad attività di spionaggio verso ospedali ucraini da parte di un gruppo APT. Rispetto al passato si nota subito come oltre ad aumentare il numero di attacchi (erano praticamente la metà, 154, appena 4 anni fa) sono cambiate le ragioni dell'attacco, tutte spostate adesso sulla criminalità informatica, spesso finalizzata a monetizzare invece che fare azioni dimostrative o di spionaggio. Il motivo di tanto interesse rispetto ai dati sanitari è facilmente comprensibile: queste informazioni sono preziose da leggere per molti soggetti. Il mercato nero dei dati sanitari – rintracciabile nel dark web - è fiorente e ad alto valore visto che, come riportato da Il Sole 24 ore nel maggio 2022[1], una cartella sanitaria di una persona può arrivare a costare anche 2000 dollari.

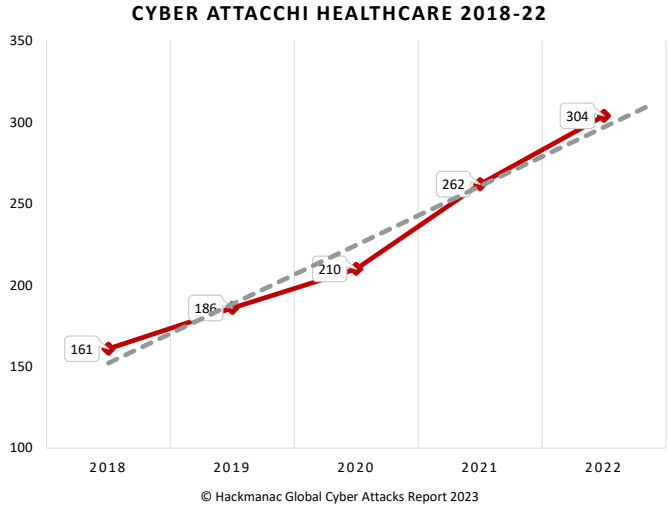


Figura 1: *Trend dei cyber attacchi nel settore sanitario nel periodo 2018 - 22*

Ciò che sicuramente può e deve preoccupare è che oltre il 70 per cento degli attacchi ha avuto impatti gravi (46 per cento) o molto gravi (25 per cento) sulle strutture sanitarie colpite.

[1] https://www.sanita24.ilsole24ore.com/art/aziende-e-regioni/2022-05-25/attacchi-cyber-strutture-ospedaliere-perche-nostri-dati-sanitari-fanno-gola-hacker-e-come-possono-proteggersi-aziende-sanitarie-133203.php?uuid=AEvKDGbB

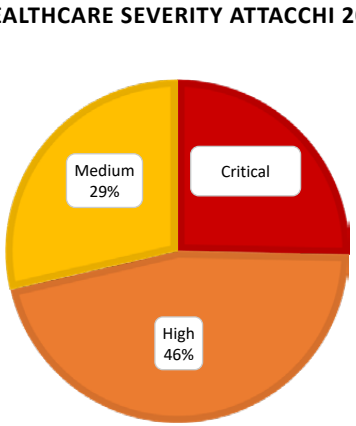


Figura 2: *Severity dei cyber attacchi in ambito sanitario nel 2022*

Soltanto un 29 per cento fa rilevare incidenti con impatti medi, a dimostrazione del fatto che i cyberattacchi in questo settore possono seriamente mettere a repentaglio la salute delle persone. Il trend degli ultimi quattro anni mostra come nell'ultimo anno siano aumentati proprio gli attacchi critici (3,1 per cento nel 2022 rispetto al 2,5 per cento del 2021).

Se si guarda alla distribuzione geografica dei cyberattacchi al settore salute, si nota subito come in testa ci sia l'America, con un 84 per cento dei target colpiti. Il dato non deve stupire, visto che in questo Paese già da anni esiste un obbligo di disclosure degli incidenti. A seguire l'Europa con un 11 per cento degli incidenti informatici, l'Asia e l'Oceania (2 per cento) e un Multiple Targets (1 per cento).

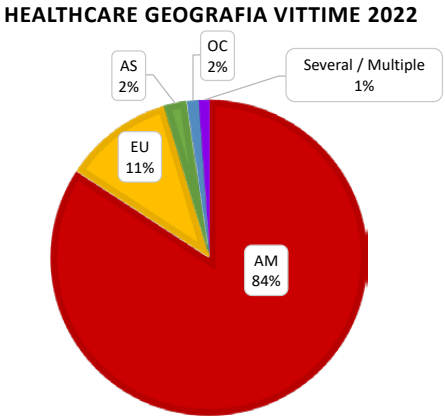


Figura 3: *Geografia delle vittime dei cyber attacchi in ambito sanitario nel 2022*

Rispetto agli anni precedenti, i numeri americani, di Asia e Oceania restano sostanzialmente costanti, mentre quelli europei diminuiscono percentualmente rispetto allo scorso anno (erano il 14 per cento), ma sono di 3 punti percentuali più alti rispetto a 4 anni fa quando erano l'8 per cento del totale.

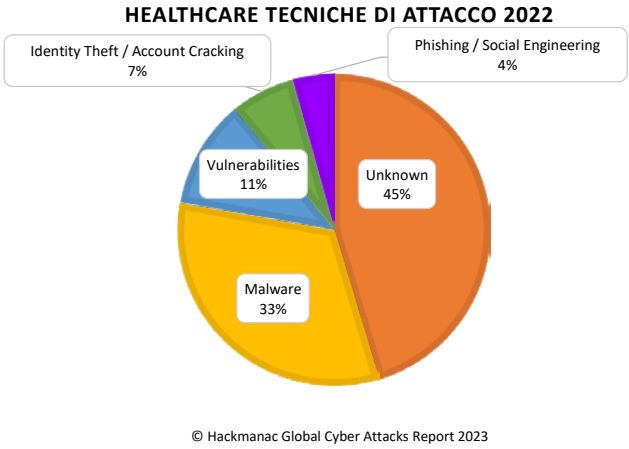


Figura 4: *Tecniche nei cyber attacchi del settore sanitario nel 2022*

Le tecniche maggiormente utilizzate per colpire il settore sanitario, nel 45 per cento dei casi, sono sconosciute (perlopiù data breach). Seguono malware per il 33 per cento degli

attacchi, sfruttamento di vulnerabilità (11 per cento), compromissione di account (7 per cento) phishing o social engineering (4 per cento).

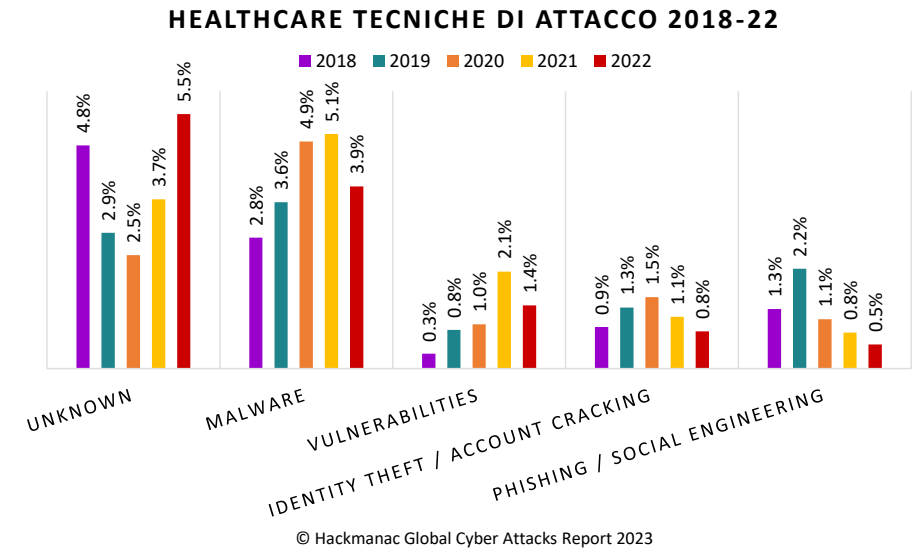


Figura 5: *Tecniche di attacco nel settore sanitario nel periodo 2018-22*

Rispetto agli anni precedenti, si nota come siano praticamente raddoppiati i cyberattacchi realizzati con tecniche sconosciute, mentre sono diminuiti, anche se di poco, i malware, che nel 2021 rappresentavano il 39 per cento dei tipi di attacchi. Sotto di 5 punti percentuali rispetto al totale anche gli attacchi legati allo sfruttamento di vulnerabilità (erano il 16 per cento nel 2021).

In Italia i cyber attacchi negli ultimi quattro anni sono praticamente triplicati, visto che si passa dai 3 del 2018 ai 9 del 2021 e 2022, con una severity che nell'ultimo anno è critica nel 78% dei casi e alta nel restante 22%.

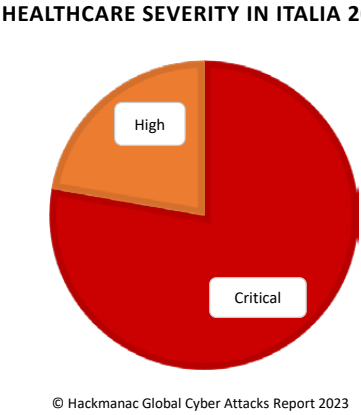


Figura 6: *Severity dei cyber attacchi verso il settore sanitario in Italia nel 2022*

Le tecniche preferite utilizzate per violare le strutture sanitarie italiane sono Malware (in particolare ransomware) e Data Breach (tecnicamente risultano come "tecniche sconosciute"), minacce per le quali il Paese dovrebbe certamente attrezzarsi meglio, anche con una verifica puntuale delle vulnerabilità dei sistemi.

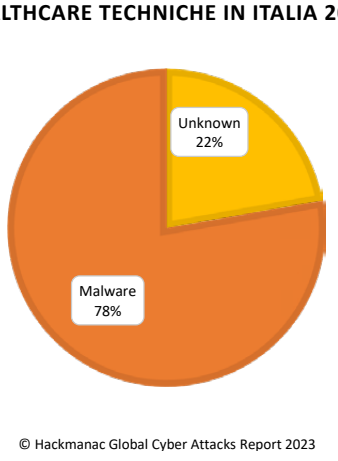


Figura 7: *Tecniche dei cyber attacchi verso il settore sanitario in Italia nel 2022*

I principali incidenti internazionali

Nel marzo 2022 fa notizia l'attacco a Scottish Association for Mental Health (SAHM), un ente di beneficenza scozzese, fondato nel 1923, che fornisce servizi a sostegno della salute mentale, colpito da un ransomware rivendicato dalla gang RansomEXX. I criminali hanno pubblicato 12 Gb di informazioni sensibili nel dark web, a seguito di un attacco che ha mandato in tilt il sistema di posta elettronica dell'associazione. Billy Watson, chief executive di SAMH, nella sua seconda dichiarazione afferma: "We are devastated by this attack. It is difficult to understand why anyone would deliberately try to disrupt the work of an organization that is relied on by people at their most vulnerable. Our priority is to continue to do everything we can to deliver our vital services."

Non meno grave il caso del sistema sanitario della Groenlandia, avvenuto nel maggio 2022, che ha praticamente paralizzato i sistemi informatici della sanità, con conseguenti disagi nella erogazione dei servizi, perdurati per diverse settimane.

Tra la fine di settembre e gli inizi di ottobre un altro ransomware colpisce una delle maggiori organizzazioni no-profit degli Stati Uniti, CommonSpirit Health. A seguito dell'attacco sembra che siano state sottratte le informazioni private di oltre 620mila persone, tanto da portare alcuni cittadini a intentare cause presso il tribunale federale, sostenendo che l'organizzazione non aveva implementato giuste misure di sicurezza necessarie a proteggere le informazioni sulla salute dei pazienti.

I principali incidenti italiani

Il 15 gennaio 2022 alle 23.30 di un sabato qualunque, sul sito della cybergang LockBit 2.0 vengono pubblicati migliaia di file prelevati alla Ulss 6 Euganea a seguito di un attacco informatico compiuto il 3 dicembre 2021. La Ulss prontamente lo comunica ai cittadini scrivendo: "Fino ad oggi non sussisteva alcuna certezza che i malviventi fossero riusciti a venire in possesso di informazioni, in che quantità e il loro genere. I criminali avevano avanzato una richiesta di riscatto in denaro in cambio della non pubblicazione delle informazioni a loro dire sottratte all'Azienda Ulss 6. Tentativo estorsivo prontamente denunciato alle forze dell'ordine e alla Procura della Repubblica". Da una prima analisi di quanto pubblicato, si scopre che ci sono oltre 9mila documenti a disposizione contenenti dati sensibili , che vanno dagli esiti dei tamponi molecolari, a informazioni sugli stipendi e i turni dei sanitari, ai referti medici dei pazienti. La Ulss 6 Euganea, da una prima analisi stima che i file pubblicati (9346 in totale, suddivisi in 51 cartelle) siano per lo più documenti di carattere amministrativo e gestionale, come procedure, verbali, regolamenti e disposizioni interne. Ma dalle indagini successive emergono anche file con dati personali e sanitari. Le cartelle pubblicate riguardano la singola struttura ospedaliera di Schiavonia".
È il 28 febbraio 2022 quando il CSIRT - Computer security incident response team, struttura istituita presso l'Agenzia per la cyber sicurezza nazionale ACN – emana l'allarme per un possibile rischio di cyber attacchi in Italia. "Sono attesi attacchi informatici provenienti dalla Russia e da Paesi orientali, indirizzati su vasta scala anche verso l'Italia". Possibili bersagli

le aziende sanitarie e ospedaliere in quanto "obiettivo molto sensibile". La comunicazione ufficiale invita ad "alzare al massimo i livelli di sicurezza, chiedendo ai vostri referenti aziendali ed ai fornitori, di monitorare in tempo reale i sistemi di sicurezza", prestando particolare attenzione ai fine settimana e agli orari notturni quando si "registra un allentamento delle difese da possibili intrusioni informatiche".

L'anno comincia in Italia con un allarme al quale seguono diversi cyber attacchi che vedono coinvolte aziende sanitarie, ospedali e anche l'Istituto Superiore di Sanità che, a maggio 2022, subisce u attacco, rivendicato dal collettivo filo russo "Killnet", insieme a molte altre Istituzioni, tra le quali ci sono Senato e Difesa e Aci.

Il giorno della Festa dei Lavoratori, 1° maggio, ad andare in tilt è l'intero sistema gestionale del pronto soccorso degli ospedali Fatebenefratelli, Sacco, Buzzi e Macedonio Melloni e il portale delle Aziende Socio Sanitarie Territoriali. La nota diramata fa riferimento genericamente a "problemi tecnici all'infrastruttura informatica aziendale" per i quali "nei giorni 2 e 3 maggio 2022 il Pronto Soccorso e i Punti Prelievo dei presidi ospedalieri dell'ASST Fatebenefratelli Sacco (Sacco, Fatebenefratelli, Buzzi e Melloni) non saranno in grado di accettare gli accessi dei pazienti. Per analoghe motivazioni potranno esserci gravi disagi anche nell'erogazione delle prestazioni ambulatoriali negli ospedali e nelle prestazioni presso le sedi territoriali. Ci scusiamo per il disagio". I problemi tecnici sono però riferibili a un attacco informatico. A confermarlo è Aria Spa, l'azienda regionale per l'innovazione: "L'attacco hacker sui server dei siti Fatebenefratelli e Sacco ha avuto conseguenze su tutte le sedi aziendali (Buzzi, Melloni e 33 sedi territoriali) e su tutti i sistemi aziendali attaccando anche i servizi di base "nonostante l'accrescimento delle misure di sicurezza poste in essere negli ultimi mesi. Intanto è iniziato il lavoro di ripristino che però "non ha al momento tempi definibili. Sarà presentata denuncia formale". Al di là delle comunicazioni formali da parte delle Aziende Socio Sanitarie Territoriali e da azienda regionale, l'attacco è di tipo ransomware, rivendicato dalla gang Vice Society.

Sempre nel mese di maggio, a finire nel mirino è Ats Insubria che serve una popolazione di oltre un milione di abitanti. Tra i disagi maggiori registrati, la gestione dei tamponi molecolari Covid il sito di Como e la messa off line del sito. Una nota dell'Agenza di Tutela della Salute di Como e Varese informa i cittadini sul fatto che le attività di ripristino dei servizi vengono fatte dando precedenza a quelle con impatto diretto sugli utenti, anche se sono necessari diversi giorni per ripristinare i servizi visto che "Proseguono le operazioni per la rimozione del virus dalle singole postazioni dei dipendenti di Ats Insubria". Anche in questo caso l'attacco informatico è di tipo ransomware di BackByte ransomware gang.

Nella settimana del Ferragosto a essere sotto attacco è la Asl Torino che dirama subito una breve nota in cui comunica che i sistemi informatici di 4 plessi ospedalieri (Giovanni Bosco, Maria Vittoria, Martini e Oftalmico) sono stati colpiti da un attacco informatico. Molti i disagi per i pazienti che per diversi giorni non riescono ad accedere ai sistemi della Asl. Nel comunicato inviato cinque giorni dopo si fa un elenco dei disservizi: referti radiologici da ritirare esclusivamente presso le segreterie delle radiologie, visite specialistiche ed esami impossibili da prenotare online, centri di prelievo che riducono al minimo la propria attività, impossibilità di pagare il ticket in modalità digitale. Dal poco che si sa dell'attacco, pare che si sia una richiesta di riscatto e che, pertanto, sembra trattarsi di ransomware.

Due le interrogazioni regionali presentate all'assessore alla Sanità del Piemonte, il quale ribadisce che le criticità hanno riguardato solo la Asl Torino e non l'infrastruttura regionale e che c'è stata una tempestiva reazione del Servizio Informatico e della Task Force aziendale, appositamente costituita che - insieme ai tecnici dell'Agenzia per la Cybersicurezza del Ministero degli Interni, agli esperti del Csirt Italia e agli agenti della Polizia Postale - hanno adottato tutte le misure necessarie per mettere in sicurezza il sistema e riavviare gradualmente le attività, garantendo che le indagini investigative procedessero parallelamente.
Tra gli ultimi attacchi del 2022, il 28 dicembre, quasi in concomitanza con l'ultimo giorno dell'anno, quello all'azienda ospedaliera di Alessandria a opera di Ragnar Locker. Nella nota dell'ospedale si legge: "Siamo stati al centro di un attacco informatico a cui ha dato seguito attivandosi immediatamente in stretta sinergia con la Regione Piemonte e l'Azienda zero, garantendo così la continuità dei servizi e delle prestazioni. Contemporaneamente, abbiamo subito avviato una collaborazione con l'Acn, l'Agenzia per la Cybersicurezza Nazionale, e sporto denuncia penale agli organi competenti". Anche in questo caso è complesso comprendere se ci sono stati furti di dati. La nota, però, si chiude con una rassicurazione: "Stiamo lavorando per predisporre, nel minor tempo possibile, un piano di potenziamento strutturale, tecnico e professionale che si inserisce in una programmazione a medio e lungo termine già avviata nei mesi precedenti".

Il ruolo di tecnologie, processi e competenze nella protezione della salute delle persone

Oggi in quasi tutti gli ambienti di lavoro bisogna usare la tecnologia, la rete, strumenti digitali e, per garantire la sicurezza dell'intero sistema, sarebbe opportuno che ciascun operatore/utente fosse consapevole del loro uso e avesse la conoscenza di base dei rischi informatici e soprattutto delle contromisure. I dati mostrano che la sanità è uno dei target più attraenti per gli hacker, grazie alla ricchezza dei dati personali e sensibili, particolarmente preziosi da rivendere nel dark web. L'accesso ai sistemi da parte di un hacker può essere ottenuto con tecniche sofisticate o semplicemente con tecniche di ingegneria sociale, in cui l'utente ingenuo o sprovveduto viene ingannato dalla classica email di phishing o da un download accattivante o forse con qualche meccanismo un po' più sofisticato, e apre la "falla" attraverso cui gli hacker possono entrare nei sistemi. Analogamente, l'utente poco consapevole, può invalidare le contromisure messe in atto all'interno dell'organizzazione con comportamenti imprudenti o sbagliati, come, ad esempio, mantenere il computer collegato ad un sistema per cui è richiesta l'autenticazione e lasciarlo incustodito, allontanandosi senza fare "log out", alla mercé di un dipendente infedele o di un estraneo infiltrato. Contrariamente a quanto si pensa e a quanto spesso la cronaca ci racconta, non sono solo gli utenti con posizioni intermedie all'interno di una azienda ad avere bisogno di essere formati, ma spesso lo sono anche i vertici, i manager, che magari hanno competenze specifiche e di elevato livello in economia, in temi legali, in temi di salute, ma nessuna in ambito di cybersecurity, eppure tutti i giorni hanno a che fare con la tecnologia, accedono ad account privilegiati da cui possono compiere operazioni bancarie, dare autorizzazioni eccetera. Dal punto di vista di un attaccante, questo tipo di manager è un bersaglio particolarmente interessante perché, accedendo ai suoi profili, si aprono direttamente le porte dei conti bancari o di informazioni

riservate e magari "preziose" se rivendute, ottimizzando così il "lavoro" dedicato a realizzare l'attacco.
Il primo punto, quindi, per la prevenzione è la "formazione" che deve portare alla consapevolezza nell'uso delle tecnologie digitali, per operare in sicurezza e non compromettere le contromisure messe in atto. Questa attenzione dovrebbe essere particolarmente alta nella sanità, dove cadere in una banale trappola di phishing può compromettere la salute di molti utenti, ai quali può essere negata la possibilità di accedere alle cure, a interventi programmati, a visite già prefissate, con un potenziale grave danno per la loro salute. Le conseguenze di questi attacchi non sono solo economici e organizzativi ma hanno un pesantissimo effetto proprio sulle persone, sui pazienti e sui cittadini.
Purtroppo, l'attenzione a questi temi e alla necessità di fare formazione è ancora molto bassa, nella sanità come nella maggior parte degli ambienti di lavoro, soprattutto pubblici. Anche il PNRR prevede ingenti finanziamenti (circa 2,5 miliardi) per il potenziamento degli strumenti digitali, della infrastruttura, del fascicolo sanitario e così via ma non per la formazione specifica del personale sanitario.
Pertanto, è importante che le organizzazioni sanitarie investano in programmi di formazione e sensibilizzazione per il personale e che adottino politiche e procedure di sicurezza appropriate per proteggere i dati sanitari e prevenire gli attacchi cyber.

Elementi sul cybercrime nel settore finanziario in Europa

[A cura di Pier Luigi Rotondo, IBM]

Il cybercrime finanziario continua ad evolversi, indubbiamente dominato da gruppi internazionali, ben strutturati e organizzati.
Nell'analisi che segue, presento e commento i risultati delle rilevazioni sul cybercrime nel settore finanziario in Europa nel corso del 2022, ed evidenzio alcune tendenze che potremmo osservare nei primi mesi del 2023. Questo lavoro è reso possibile anche grazie ai contributi del gruppo di ricerca IBM Security, IBM 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 del capitolo.

Un anno di cybercrime finanziario

Per alcuni anni il settore finanziario è stato il più attaccato, alternando recentemente il podio con il settore manifatturiero. In tutto il 2022, limitatamente alla sola area geografica Europa, finanza e assicurazioni sono stati i settori più attaccati, con il 25% degli attacchi in cui IBM X-Force è stata coinvolta. [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 l'istituzione finanziaria, si preferisce attaccarne i clienti in quanto obiettivo indubbiamente più permeabile.
L'analisi delle principali campagne del 2022 mostra che la frode avviene prevalentemente attraverso i seguenti vettori di attacco:

- phishing per la fase di furto di credenziali di accesso (credential theft), spesso combinata con una successiva interazione con un finto operatore per il furto dei fattori di autenticazione forte;
- malware per il furto di credenziali o fattori addizionali di autenticazione o manipolazione di una transazione;
- hacking del dispositivo mobile tramite SIM Swap o emulazione software dello smartphone;
- e infine ma in misura inferiore, con l'attacco diretto all'infrastruttura dell'istituzione finanziaria, sfruttando vulnerabilità quasi sempre note ma ancora non fissate.

La tecnica, o la combinazione di tecniche, varia in base alla tipologia di vittima, con sostanziali differenze tra il cliente finale (retail) oppure aziendale (corporate).

Financial malware

ENISA, Agenzia dell'Unione Europea per la Cybersecurity, pone il malware tra le principali minacce cyber del 2022 [2], secondo solo agli attacchi ransomware.
Nel contesto variegato di tutti i malware, qui analizziamo *solo i financial malware* o malware

per frodi finanziarie. 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 2022.
Ramnit e QakBot/QBot sono stati i principali malware dell'anno, seguiti da una lunga lista di altri malware con impatto minore.

Non ci sono sostanziali novità rispetto al 2021, piuttosto un riposizionamento di alcuni codici malware di minore diffusione. Prosegue la perdita di terreno di TrickBot, due anni fa il malware per frodi finanziare più diffuso in EMEA, e ora circoscritto solo ad un numero molto limitato di infezioni, con una caduta legata indubbiamente allo smantellamento della Botnet di TrickBot (ottobre 2020) [3], seguita poi dallo smantellamento delle tre botnet Epoch 1, 2 e 3 di Emotet (gennaio 2021) [4][5][16], principali veicoli di diffusione di TrickBot.
Sono tuttavia comparsi nuovi codici malware, per adesso ancora di impatto limitato, a riprova della prolificità del settore cyber crime. Un settore che continua a popolarsi di persone e organizzazioni tecnicamente molto preparate e capaci di mettere alla prova le soluzioni tecnologiche e i processi introdotti per limitare il fenomeno.

Figura 1

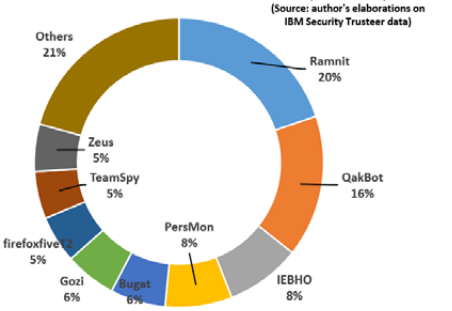
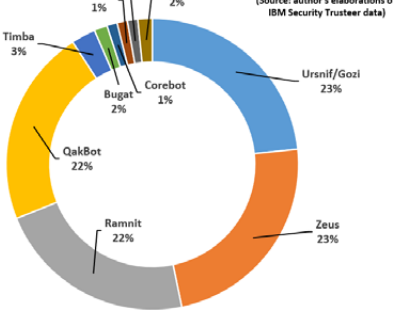


Figura 2



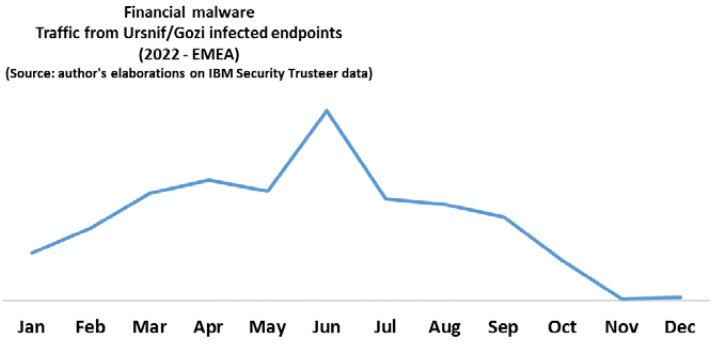
Il primo diagramma (**Figura 1**) descrive la distribuzione dei malware così come sono stati rilevati sui dispositivi utente (endpoint) infetti.
In questo primo diagramma e nel successivo (Figura 2) abbiamo scelto di *non* riportare l'incidenza di Emotet, indubbiamente diffuso in Italia e nel resto d'Europa, in quanto il suo ruolo è stato prevalentemente di *loader* (veicolo di distribuzione) per altri malware, in particolare QakBot, TrickBot e IcedID, attraverso un probabile sodalizio tra i gruppi criminali. In questo connubio, Emotet è il veicolo che elude le misure di protezione della rete e dell'endpoint, infettando la macchina della vittima per poi scaricare il payload, spesso l'eseguibile di QakBot o TrickBot, a cui poi lascia il controllo. Questi ultimi, in molti casi, hanno

poi ulteriormente veicolato ransomware, Ryuk o altri malware, con un incapsulamento di malware all'interno di altro malware e con un meccanismo in cui ciascun attore cyber guadagna anche affittando spazio e accesso ad altri gruppi.
Nel diagramma di **Figura 2** catturiamo e analizziamo il traffico generato da endpoint infetti da malware verso il sito web dell'organizzazione target, ad esempio una banca, e il traffico verso le rispettive infrastrutture di Command and Control (C2, o C&C) per perpetrare una transazione fraudolenta.
In questo caso, rispetto al 2021, vediamo una spiccata polarizzazione attorno a quattro malware principali Ursnif/Gozi, Zeus, Ramnit, QakBot che cumulativamente totalizzano il 90% delle infezioni. Nel posizionamento di questi quattro malware non c'è praticamente stata differenza rispetto all'anno precedente. Anche in questa analisi di traffico assistiamo alla scomparsa di Trickbot.

Questa seconda tipologia di rilevazione è speculare a quanto già osservato relativamente agli endpoint infetti. Le due rilevazioni si integrano l'un l'altra.
Mentre il diagramma di *Figura 1* misura la capacità del malware di evadere le protezioni di rete e di endpoint e infettare il computer o smartphone della vittima, la *Figura 2* misura invece la quantità di traffico che i dispositivi infetti riescono a generare verso il sito web target o verso l'infrastruttura di Command-and-Control (tipicamente una botnet) e che potenzialmente mettono a rischio l'account utente. Nel raffrontare i due diagrammi occorre tenere in giusta considerazione il diverso comportamento di ciascun malware e soprattutto come vengono rilevati i dati.
Una soluzione di sicurezza deve essere in grado di osservare, individuare e rispondere ad entrambi i fenomeni, combinandoli per proteggere l'endpoint durante ciascuna fase della transazione bancaria.

Attività dei principali financial malware nel corso dell'anno

I malware per frodi finanziarie mirano a dare accesso ai cyber criminali a conti bancari di vittime, oppure dirottare pagamenti verso altri conti ad insaputa della vittima.



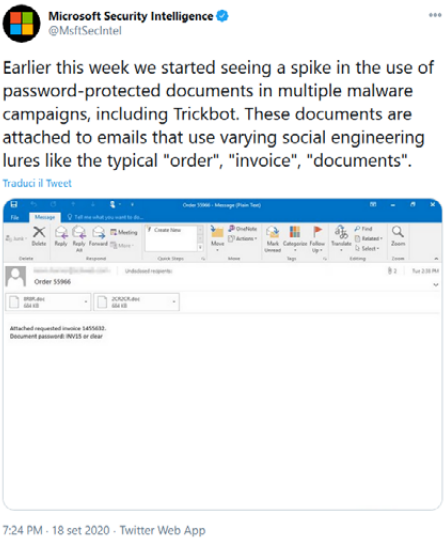
A seconda della tattica, l'attacco può spaziare dal semplice furto di credenziali di accesso, al furto del fattore di autenticazione forte del cliente (SCA – Strong Customer Authentication) introdotto dalla normativa PSD2 [6], al furto dei dati delle carte di pagamento e, infine, allo "IBAN Swapping" o "on-device fraud (ODF)" ovvero la sostituzione delle coordinate di pagamento IBAN o del wallet elettronico; questo ultimo caso soprattutto per i malware sui dispositivi mobili.
Ursnif, conosciuto anche come Gozi, è uno dei più antichi malware bancari ancora attivi e al centro di numerose campagne verso utenti di online banking anche in Italia. IBM X-Force ha individuato ed analizzato una variante di Ursnif/Gozi [7] costruita per infettare il sistema Windows della vittima e contemporaneamente anche il suo dispositivo Android con il malware Cerberus. La componente Cerberus dell'attacco serve a catturare i codici dispositivi inviati dalla banca attraverso SMS.
Cerberus è un malware per dispositivi Android di tipo overlay. Consente di mostrare sullo schermo del dispositivo mobile schermate appositamente create dagli attaccanti per richiedere l'inserimento di elementi di autenticazione, che vengono catturati fraudolentemente e inviati all'esterno. Emerso nel 2019, era inizialmente privo di funzionalità avanzate. Ora si è evoluto fino ad implementare la capacità di catturare gli SMS ricevuti ad esempio con One Time Password, aprire overlay personalizzati sul layout grafico della banca online e rubare codici 2FA da Google Authenticator. Funzionalità aggiuntive includono l'accesso alla carta di credito del cliente, la possibilità di reindirizzare le chiamate telefoniche, accedere al dispositivo tramite le funzionalità di Remote Access Tool e di concedere le autorizzazioni richieste dalle App. Tutti strumenti utili a portare a termine una frode, anche articolata.
Il vettore iniziale di Ursnif/Gozi è costituito da 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, ha fortunatamente limitato l'impatto che questo tipo di campagne potrebbe aver avuto.
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.

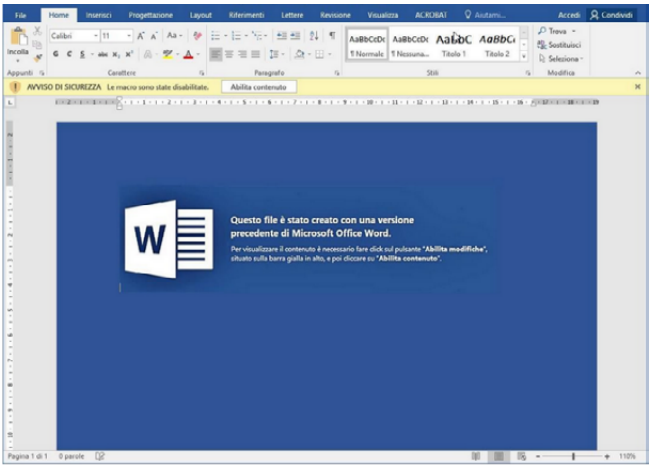
Ciascun elemento, anche apparentemente insignificante, può essere utile per costruire e dare maggiore credito all'attacco, o collezionare informazioni per attacchi futuri.

Come nell'esempio di Ursnif già citato, i malware sono stati veicolati nella maggioranza dei casi attraverso documenti Office allegati ad e-mail [2] 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.

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 funzioni 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 annunciato nel corso del 2022 [10] un importante cambiamento nell'apertura di macro VBA in document Office provenienti da Internet.
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. Vedremo nei prossimi mesi l'effetto di questo cambiamento.
Nel caso del file zip, il documento malevolo è all'interno del pacchetto compresso e protetto da password, ma con una password molto semplice e inclusa in chiaro nel testo della mail. In questo modo la vittima è in grado di aprire il file compresso e poi il documento malevolo contenuto all'interno. 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 ad espandere archivi protetti da password.

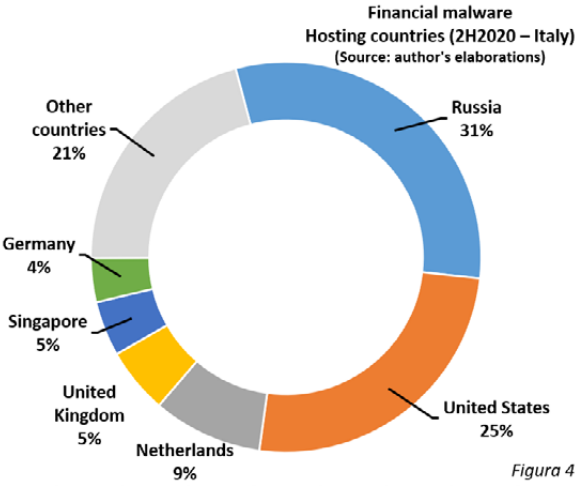


Figura 4

Sulla base delle ultime rilevazioni del 2H2020, il malware era ospitato su provider russi nel 31% dei casi, statunitensi del 25% dei casi, ed in percentuali descrescenti anche in altri paesi.
La collocazione geografica del provider indica solo dove è stato inizialmente caricato il malware e non ci fornisce indicazioni precise sui threat actors.
Analizzando nel dettaglio le singole URL, e i provider usati, si nota che i cyber criminali noleggiano spazio presso provider, oppure molto più frequentemente compromettono siti internet già esistenti, non aggiornati o con cattive configurazioni, oppure ancora depositano il malware in folder di upload pubblici e visibili, dai quali è poi universalmente disponibile. Spesso all'insaputa dei legittimi proprietari dello spazio che diventano vittime loro stesse.
Phishing verso il settore finanziario italiano
Il settore finanziario, anche in Italia, è da sempre tra le maggiori vittime del phishing per il furto di credenziali.

Lo studio che segue si basa sull'analisi di 687 campagne di furto di credenziali per l'accesso a banche e altre istituzioni finanziarie italiane nel periodo 1 gennaio – 31 dicembre 2022, verificate e monitorate fino a disattivazione.
Questa analisi non prende in considerazione i numerosi domini registrati con nomi verosimili di banche o prodotti finanziari (domain squatting) ma mai attivati, presumibilmente bloccati durante l'attivazione oppure abbandonati dagli stessi creatori, oppure ancora pronti per essere attivati in futuro. Akamai [11] stima che circa il 20.1% di tutti i domini registrati nel secondo semestre 2022 sono malevoli.

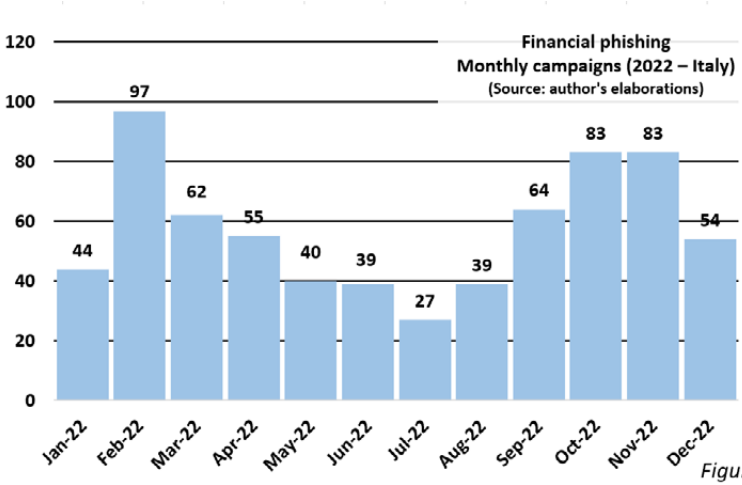


Figura 5

Limitandosi al settore finanziario italiano, in tutto il 2022 è stata osservata una media di circa 2 nuove pagine di phishing al giorno attivate e perfettamente funzionanti, in diminuzione rispetto ai dati rilevati nel 2021.
La massima attività si è raggiunta nel mese di febbraio 2022, con una media di 3,5 nuove pagine attivate al giorno.

I brand maggiormente obiettivo di phishing sono stati BPER Banca (22% delle campagne di phishing analizzate), Intesa Sanpaolo (20% delle campagne), Poste Italiane (14% delle campagne), Banca MPS (10% delle campagne). Poi altri brand con un impatto minore, tra questi Nexi (8%), Banco BPM (6%), UniCredit (5%), Crédit Agricole e Banca BCC (3%), e poi Findomestic, Banca Mediolanum e Fineco Bank (2%).

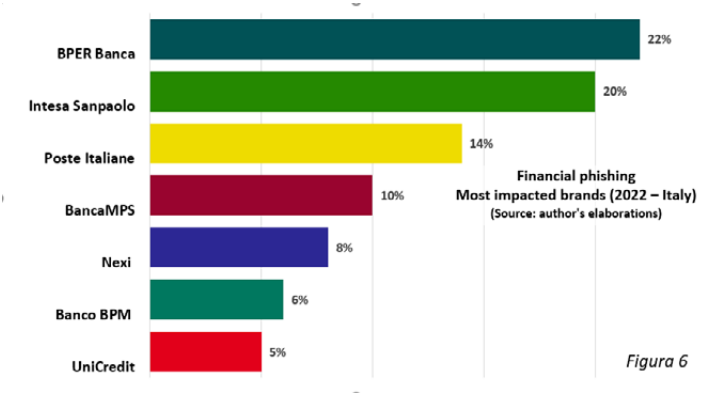


Figura 6

In totale nel corso del 2022 sono state tracciate campagne phishing verso clienti di 24 istituzioni finanziarie italiane.
Le prime stime per gennaio 2023 vedono poco più di 2.1 nuove campagne al giorno, in linea con le ultime settimane del 2022.
Nel corso del 2022 il 44% dei siti di phishing verso il settore finanziario italiano è stato ospitato negli Stati Uniti. Ancora una volta il provider che ha ospitato in assoluto più pagine di phishing è stato lo statunitense Namecheap, tra le principali aziende di web hosting al mondo con oltre 10 milioni di domini gestiti, che da solo ha ospitato il 17% di tutte le pagine phishing prese in considerazione in questo studio. Un valore di tutto rispetto ma in netto calo rispetto ai dati 2021 in cui aveva ospitato il 36% delle pagine phishing. Provider Italiani hanno invece ospitato l'11% delle pagine di phishing finanziario italiano, e questo numero è più che raddoppiato rispetto alle rilevazioni del 2021.

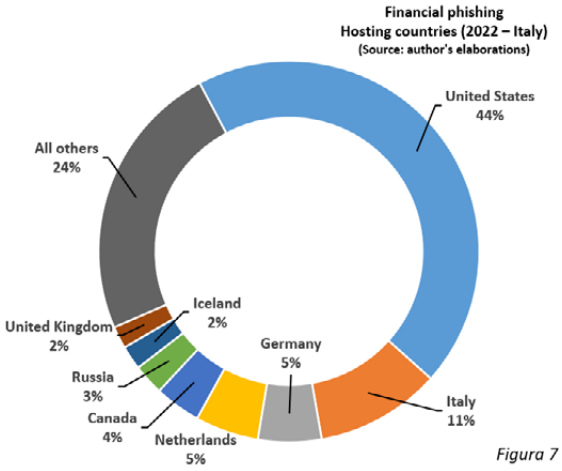


Figura 7

Proprio come per le drop URL del malware, la collocazione geografica del provider che ospita la pagina di phishing non fornisce alcuna indicazione su dove siano realmente i threat actors. È ipotizzabile che la collocazione e la scelta del provider siano da attribuirsi alla combinazione della facilità di creare domini, anche in maniera automatica via API e pagando in criptovaluta, o addirittura usando offerte di siti web gratuiti, assieme agli scarsi controlli operati dal provider.
Altro dato che deve farci riflettere è che ormai il 97% delle URL di phishing usa il protocollo HTTPs, il cosidetto 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, tuttavia l'icona del lucchetto nella barra indirizzi del browser può creare la falsa illusione che un sito web possa essere considerato 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.
La decisione sulla veridicità di una connessione HTTPS dovrebbe essere legata alla *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, malgrado siano 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 phisher 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 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).
Molti browser forniscono un'indicazione visiva sul tipo di validazione del certificato ed è su questo che gli utenti dei servizi di banking andrebbero informati e istruiti. Purtroppo, l'indicazione è di difficile comprensione per un utente non attento.

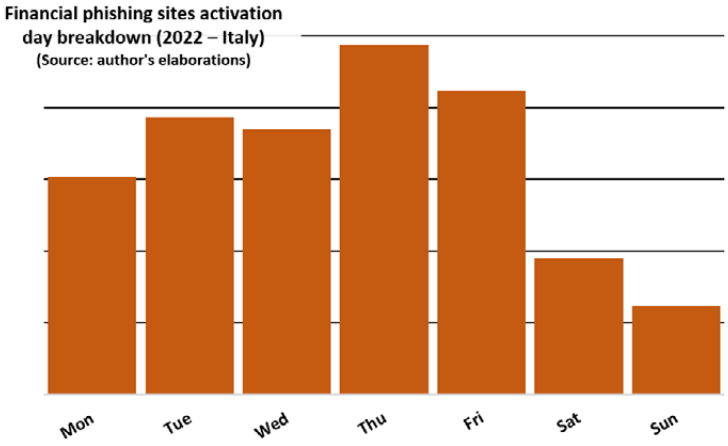


Figura 8

Le pagine di furto di credenziali vengono attivate prevalentemente verso la fine della settimana lavorativa, il 40% nelle due giornate di giovedì e venerdì. La vita di una pagina è generalmente breve, meno di 48h nella maggioranza dei casi. La combinazione di questi fattori determina una sostanziale prevalenza di attacchi phishing bancario che si sviluppano durante il fine settimana, proprio quanto la vittima è più vulnerabile con gli sportelli bancari chiusi, a cui non è possibile rivolgersi tempestivamente.
Ci sono comunque notevoli eccezioni, con alcune pagine rimaste attive molto a lungo e che hanno continuato a "pescare" preziose credenziali per mesi. Alcune pagine sono rimaste perfettamente funzionanti per un tempo superiore ai 30 giorni, ed in un caso particolare una pagina è rimasta attiva per oltre 3 mesi e mezzo.

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.

Il phishing verso il settore finanziario italiano è veicolato principalmente tramite e-mail e SMS, e quest'ultima variante è comunemente denominata *smishing*, parola ottenuta dalla contrazione di SMS e phishing. 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.
La frode è normalmente realizzata attraverso una sequenza di passi successivi, 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. 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, quindi non c'è da sorprendersi se alcune delle chiamate dai finti operatori arrivano da un numero di telefono che è proprio quello della banca [12].
Approccio simile si ha nelle finestre di chat live che cominciano ad 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 bonifici.
Vista la semplicità realizzativa e del basso livello di rischio di chi la perpetra, si prevede una crescita di questo approccio combinato al phishing.

Per riassumere, le caratteristiche distintive delle campagne di phishing e malware sono:
- Perfetta localizzazione in lingua italiana. Sono pressoché 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 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.
- 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.

Molti phishing kit espongono in chiaro, tramite URL accessibili a chi ne conosce il path esatto, i dati delle vittime della campagna di phishing. Questa, che ad una prima analisi potrebbe apparire un errore di chi ha scritto il phishing kit (Sensitive Data Exposure), per la sua frequenza potrebbe invece essere spiegata come una 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.
Questa situazione 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 seguono gli attacchi, e catturano le credenziali di accesso per poi costruirci nuove campagne di attacco.

L'era del low cost phishing

Una frazione non trascurabile di 38 campagne di phishing finanziario, soprattutto nella seconda parte dell'anno, è stata ospitata direttamente su fresh installation della 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 3Q 2022, hanno preso di mira principalmente clienti di Poste Italiane e BPER Banca.

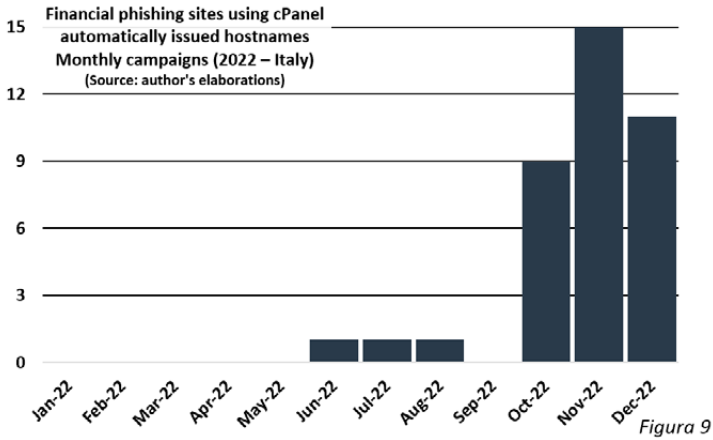


Figura 9

Al momento dell'installazione, se l'interfaccia WebHost Manager (WHM) interface di cPanel non dispone di un hostname, viene automaticamente assegnato un hostname nel dominio cprapid.com. L'hostname è generato sulla base dell'IP del server, ad esempio WHM

installato sull'IP 20.59.39.5 riceve un hostname del tipo 20-59-39-5.cprapid.com. Inoltre, la Certification Authority di cPanel genera un certificato SSL/TLS per il server web e questo consentirà connessioni HTTPS senza generare messaggi di errore nei browser client.
Questo meccanismo consente in maniera estremamente semplice di attivare in autonomia siti web di phishing senza poggiarsi su provider Internet, il che semplifica l'attività dei cyber criminali.
Questo fenomeno sembra continuare nelle osservazioni delle prime settimane del 2023.
Altre strategie low-cost e con pochi o senza controlli per il phishing hanno visto siti appoggiati su sistemi di web hosting gratuito come 000webhost (16 domini osservati, di cui 15 per pagine di phishing verso BPER Banca) e duckdns (15 domini).

Molti schemi di attacco hanno origine nel furto di credenziali

IBM Security stima che il furto o la compromissione delle credenziali è stato il vettore di attacco nel 19% dei data breach del 2022 [14]. Anche secondo ENISA il phishing è tornato il vettore di accesso iniziale più comune, non solo nelle frodi finanziarie [2]. Ancora nel 2022, secondo IBM Security X-Force, il phishing in tutte le sue forme, inclusi allegati e link, è rimasto il principale vettore di attacco coinvolto nel 41% degli gli incidenti gestiti [1]. Per confronto, nel 2020 era stato il 33%, con una crescita di 8 punti percentuali in 2 anni.
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 [15], 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 finanziare, ad esempio bonifici, 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 PSD2 [6] ha introdotto, ormai 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 rein-

serire 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. 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 di più si stanno diffondendo sistemi di MFA resistenti al phishing, i cosiddetti *Phishing-Resistant Multi-Factor Authentication*, intesi come processi 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 così pervasiva minaccia phishing, tutti i sistemi ad alto valore di un'organizzazione dovrebbero implementare o pianificare la loro migrazione a MFA resistente al phishing.

Al momento i due sistemi più efficaci [18] 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.

Conclusioni

In un contesto di attacchi in costante evoluzione, molte delle soluzioni usate finora non sono più sufficienti a fornire un adeguato livello di protezione. Vi è necessità di implementare soluzioni in grado di adattarsi rapidamente ed automaticamente ad una minaccia estremamente mutevole.

Si delinea sul mercato una virtuosa convergenza di soluzioni di sicurezza già esistenti e conosciute da tempo verso l'adozione di feed di Threat Intelligence, che ne consentono l'aggiornamento e adattamento veloce alle minacce che si avvicendano, ora dopo ora. I feed veicolano descrizioni di attacchi e minacce e questi aggiornano costantemente le soluzioni

di sicurezza con nuove definizioni, proprio come abbiamo imparato per gli antivirus. È imperativo integrare i SIEM, le soluzioni SOAR, i firewall e gli altri dispositivi di rete, i DNS, e adesso anche le soluzioni di Identity e Access Management con feed di Threat Intelligence. Questo però da solo non basta, in quanto sempre di più si assiste ad attacchi unici e *fileless* (senza file, che si sviluppano per lo più interamente in memoria) per i quali estrarre tempestivamente una firma (signature) è estremamente difficile se non impossibile.
L'EDR - Endpoint Detection and Response, nelle sue svariate declinazioni, interviene laddove l'antimalware non riesce più ad arrivare, attraverso un'analisi comportamentale dei file durante l'esecuzione in memoria (behavioural analysis), pronto a bloccare comportamenti anomali come la creazione e l'esecuzione di file eseguibili. In quest'area il Machine Learning può essere estremamente efficace.

È quindi di grande valore adottare quanto prima, sia per gli endpoint utente che per i server, un EDR specializzato che faccia della behavioural analysis, da affiancare alle soluzioni antimalware e antivirus già esistenti. Gli EDR con un motore comportamentale sono decisamente efficaci nel rilevare varianti di ransomware ancora sconosciute, e quindi non individuabili con un approccio signature-based. Analizzano le attività e l'accesso ai file, e se viene rilevato un tentativo di cifrare file e la catena del processo è sospetta, il processo viene bloccato e i file crittografati vengono prontamente ripristinati.
La naturale evoluzione in *Extended Detection and Response (XDR)*, integra 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. Questo protegge i dati aziendali, spesso custoditi o acceduti dal terminale del dipendente, anche quando si lavora al di fuori dell'ufficio e quindi dalla naturale protezione offerta dalla rete aziendale. Capacità autonome di detection e risposta agli attacchi vengono abilitate già sull'endpoint, e sono sempre attive, anche quando il computer non è disconnesso dal resto dell'infrastruttura IT aziendale, ad esempio in mobilità.
Estendere 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 [19]. Si tratta di un servizio gratuito che sostituisce il DNS generalmente fornito dal provider internet o dal DNS aziendale. Ogni volta che il dispositivo esegue una transazione Internet che utilizza il DNS (e la maggior parte delle

transazioni lo fa), Quad9 blocca la risoluzione per gli hostname considerati dannosi sulla base di elenchi costantemente aggiornati di siti malevoli. 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 malware, phishing, spyware e botnet.
Laddove è presente un DNS aziendale, il monitoraggio del traffico DNS è una ricca fonte di informazioni per la sicurezza aziendale, capace di evidenziare prontamente sistemi infetti o con pattern di traffico anomalo. Il DNS aziendale va quindi integrato con i SIEM per la correlazione con altri eventi, e per alimentare i SOAR (Security Operation and Automation Response) ed essere infine presentato agli operatori del SOC (Security Operation Centre). In questo caso la soluzione deve implementare meccanismi di Artificial Intelligence e Machine Learning per predire la minaccia, ad esempio analizzando i Domain Generation Algorithms (DGA), e sostituire alcune attività manuali di reverse engineering.
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 MFA. Molte implementazioni comuni, 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. Dotare le proprie applicazioni di un'infrastruttura di supporto per schemi di autenticazione resistenti al phishing (phishing-resistant MFA) anche con l'ausilio dell'autenticazione biometrica deve essere un'altra priorità.

Il *cloud computing* e l'*intelligenza artificiale* sono due fenomeni inarrestabili che caratterizzano il panorama informatico di questi anni. Nel corso del 2022 è continuato incessante e imponente, 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 lascia la più ampia scelta e flessibilità 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 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.
Pervasiva anche l'Intelligenza Artificiale, non come soluzione ultima a tutti i problemi, ma con soluzioni mirate in grado di gestire determinate classi di fenomeni. Il Machine Learning, ad esempio, può rivelarsi davvero utile per catturare anomalie rispetto al comportamento "caratteristico" di ciascun utente o del traffico di rete, facendosi carico dell'onere di

capire cosa è caratteristico utente per utente. Collegarsi da una località geografica insolita, oppure collegarsi a un orario insolito, e sappiamo quando lo smart working abbia rivoluzionato il concetto di orario di lavoro e luogo di lavoro, e lo abbia diversificato persona per persona. Sequenze di operazioni insolite, navigare all'interno di un sito o applicazione seguendo pattern anomali, fare file transfer insoliti o verso reti o servizi considerati a rischio, oppure ancora accedere ad una quantità insolita di documenti office, come fanno molti ransomware. Ora siamo in grado di seguire questi andamenti utente per utente, proprio perché ciascun utente nell'organizzazione ha un modo di lavorare unico che il Machine Learning è in grado di delineare.
Il tema è quantomai attuale. Il Cost of a Data Breach Report 2022 [14], condotto da Ponemon Institute, e analizzato e pubblicato da IBM Security, ormai da diversi anni consecutivi, mostra come l'intelligenza artificiale e l'automazione nella risposta agli incidenti, siano i 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] *X-Force Threat Intelligence Index 2023* IBM Security, February 2023
[2] *ENISA Threat Landscape 2022* ENISA European Union Agency for Cybersecurity, November 2022
[3] C. Cimpanu *Microsoft and others orchestrate takedown of TrickBot botnet* ZDNet, October 2020
[4] *Emotet Botnet Disrupted in International Cyber Operation* The United States Department of Justice, 28 January 2021
[5] *World's most dangerous malware EMOTET disrupted through global action* Eurojust – Europol, 27 January 2021
[6] *Directive (EU) 2015/2366 of the European Parliament and of the Council* Official Journal of the European Union, November 2015
[7] I. Chimino *Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy* SecurityIntelligence, June 2021
[8] Pier Luigi Rotondo *Elementi sul cybercrime nel settore finanziario in Europa* Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia, ottobre 2020
[9] *Monitoraggio sul corretto utilizzo del protocollo HTTPS e dei livelli di aggiornamento delle versioni dei CMS nei portali Istituzionali della PA* Cert-AgID, dicembre 2020
[10] Microsoft *Macros from the internet will be blocked by default in Office*
[11] *Flagging 13 Million Malicious Domains in 1 Month with Newly Observed Domains* Akamai Security Research, September 2022
[12] *Contrasto alla criminalità finanziaria - Attività della Polizia Postale contro le frodi "Alias"* Commissariato di P.S. online, novembre 2020
[13] A. Pilkey *Phishing is here to stay* F-Secure, December 2020
[14] IBM Security *Cost of a Data Breach Report 2022* July 2022
[15] MITRE Enterprise ATT&CK v12

[16] *NCA in international takedown of notorious malware Emotet* United Kingdom National Crime Agency, January 2021
[17] J. Gregory *Cybersecurity Trends: IBM's Predictions for 2023* SecurityIntelligence, January 2023
[18] S. Weeden *What makes FIDO and WebAuthn phishing resistant?* IBM Security Community, December 2021
[19] *2023 – Cybersecurity and Privacy Predictions for the Coming Year* Quad9, December 2022
[20] S. Gritzman, L. Kessem *IBM Trusteer Exposes Massive Fraud Operation Facilitated by Evil Mobile Emulator Farms* SecurityIntelligence, December 2020
[21] Pier Luigi Rotondo *Shopping e saldi invernali più sicuri con i pagamenti elettronici* IBM thinkMagazine, dicembre 2019
[22] Pier Luigi Rotondo *IBM X-Force: un passo avanti nella difesa dagli attacchi finanziari più evoluti* IBM thinkMagazine, febbraio 2018
[23] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019
[24] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019
[25] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, maggio 2019
[26] O. Ozer *The Curious Case of a Fileless TrickBot Infection* SecurityIntelligence, August 2019
[27] Pier Luigi Rotondo *Sai cosa sono gli attacchi BEC?* IBM thinkMagazine, giugno 2019 https://ibm.biz/attacchibec
[28] Pier Luigi Rotondo *Multifactor Authentication Delivers the Convenience and Security Online Shoppers Demand* SecurityIntelligence, January 2019
[29] Pier Luigi Rotondo *How Will Strong Customer Authentication Impact the Security of Electronic Payments?* SecurityIntelligence, September 2019
[30] Pier Luigi Rotondo *Come proteggersi dagli attacchi Business Email Compromise* INTESA, maggio 2019
[31] Pier Luigi Rotondo *Acquisti online? Ecco come farli in modo sempre più sicuro* IBM thinkMagazine, dicembre 2018 https://ibm.biz/ibmblackfriday
[32] 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
[33] M. Schieppati *I 5 tech-trend del 2020 in banca* Bancaforte, gennaio 2020
[34] Pier Luigi Rotondo *Soluzioni di sicurezza più efficaci con la threat intelligence di IBM X-Force Exchange* IBM thinkMagazine, aprile 2021 https://ibm.biz/xforcethreatintelligence
[35] Pier Luigi Rotondo *Sarà un anno sicuro, a patto che …* IBM thinkMagazine, marzo 2021 https://ibm.biz/2021sicuro
[36] G. Badalucco *Identity security, la sicurezza basata sull'identità* Data Manager, Settembre 2022
[37] R. Fouchereau *2022 Global DNS Threat Report* IDC, June 2022

Lo scenario evolutivo della minaccia ransomware

[A cura di Pasquale Digregorio, Chiara Ferretti e Daniele Filoscia – CERT Banca d'Italia][1]

L'accelerazione nella digitalizzazione dei processi di business e la conseguente virtualizzazione delle interazioni sociali ed economiche, anche correlati alla diffusione del lavoro da remoto, le crescenti dipendenze dalle filiere di approvvigionamento (*supply chain*), hanno contribuito ad incrementare la superficie di esposizione sfruttabile per la conduzione di attacchi cyber efficaci ai danni di cittadini, organizzazioni e istituzioni. In questo scenario si osserva un ampliamento significativo della minaccia *ransomware*, considerata particolarmente remunerativa anche a causa della crescente centralità dei servizi e sistemi ICT per la conduzione di attività economiche, aspetto in grado di rafforzare il potenziale estorsivo degli attaccanti.

Il termine *ransomware*[2] nasce con riferimento a un *malware*[3] utilizzato per condurre attacchi cyber con finalità estorsiva (*ransom*). Originariamente questa si basava esclusivamente sulla cifratura dei dati presenti sui sistemi informativi della vittima e sulla conseguente richiesta del pagamento di un riscatto per l'ottenimento della chiave crittografica, necessaria per ripristinare la disponibilità dei dati. Attualmente il termine assume un'accezione più ampia, includendo anche altri tipi di cyber *extorsion* basati, ad esempio, sulla compromissione della disponibilità dei sistemi e servizi ICT e sulla riservatezza dei dati.

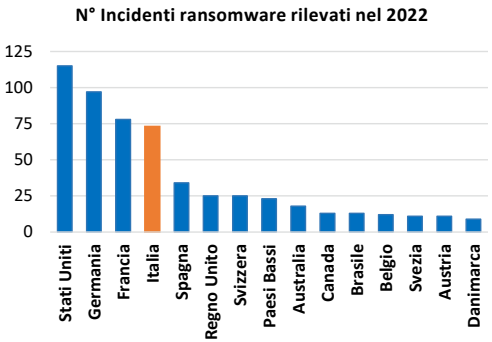


Figura 1: *Prime 15 nazioni per numero di incidenti ransomware riportati all'ENISA: l'Italia è al quarto posto.*

[1] Le opinioni sono espresse a titolo personale e non impegnano la responsabilità dell'Istituto.

[2] Ransomware: malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari. Fonte: Glossario ACN CSIRT: https://www.csirt.gov.it/glossario/23

[3] Malware: contrazione di malicious software. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. Fonte: Glossario ACN CSIRT: https://www.csirt.gov.it/glossario/22

Si assiste, quindi, ad una continua evoluzione delle tecniche, tattiche e procedure (TTP) per garantire l'efficacia nel tempo degli attacchi *ransomware*, sfruttando in maniera sinergica vulnerabilità di tipo tecnologico, procedurale, psicologico e sociale.
Questa minaccia continua a crescere per sofisticatezza e aggressività. Nella prima metà del 2022 sono stati identificati oltre 10.000 nuovi ceppi *ransomware* unici, quasi il doppio di quelli individuati nel semestre precedente, come testimoniano i dati del FortiGuard Labs Threat Report[4].
Secondo l'*ENISA*[5], tra dicembre 2021 e giugno 2022 si è riscontrato un incremento della quantità di dati violati attraverso attacchi *ransomware* perpetrati in Europa, Regno Unito e Stati Uniti superiore al 50%. L'Italia risulta al quarto posto come paese maggiormente colpito dopo Stati Uniti, Germania e Francia[6] (Figura 1). Al fine di comprendere efficacemente i profili evolutivi della minaccia *ransomware* è stato sviluppato un modello utile a rappresentare il ciclo di vita di un attacco di questo tipo dal punto di vista dell'attaccante, descritto nel paragrafo seguente. Successivamente, nel corso della trattazione si analizzeranno tre direttrici, che hanno caratterizzato in modo determinate la rapida trasformazione di questa minaccia.

1. Il ciclo di vita di un'offensiva ransomware dal punto di vista dell'attaccante

Analizzando in modo sinottico un numero consistente di attacchi, è stato possibile definire un modello utile a rappresentare il ciclo di vita di un'offensiva *ransomware* dal punto di vista dell'attaccante. È interessante notare come lo schema individuato (raffigurato in Figura 2) sia strutturato su alcune attività iniziali che portano ad un ciclo che può prevedere diverse iterazioni, in base al piano estorsivo e al comportamento della vittima. Si propone di seguito la descrizione di ciascuna fase del ciclo di vita sviluppato.

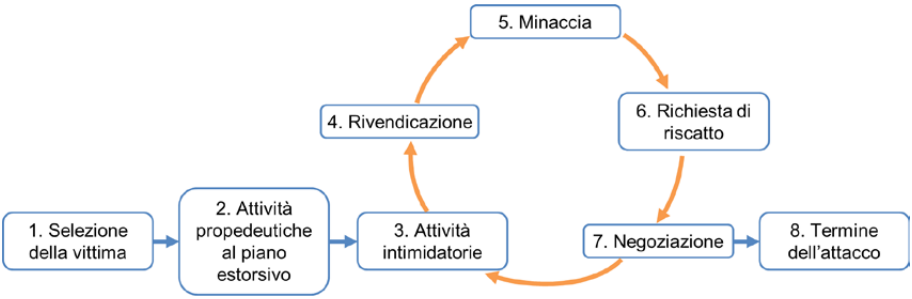


Figura 2: *Ciclo di vita di un attacco ransomware dal punto di vista dell'attaccante.*

[4] https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings
[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

1. Selezione della vittima

In base alla modalità di selezione della vittima, un attacco *ransomware* si può distinguere in tre categorie: attacco opportunistico, mirato o ibrido.
Gli attacchi opportunistici si caratterizzano per la mancanza di una strategia specifica sulla selezione degli obiettivi da colpire e, di conseguenza, sulla volontà di compromettere potenzialmente un ampio numero di vittime, da cui trarre indistintamente profitto con un investimento di risorse relativamente basso. A tal fine i *threat actor* sfruttano, generalmente, strumenti automatizzati quali ad esempio *phishing toolkit*, in grado di distribuire in massa e-mail malevole, o programmi per la scansione automatica di vulnerabilità software.
Spesso l'orchestrazione di un attacco opportunistico è connessa con la disponibilità di uno specifico *exploit* che rappresenta l'opportunità, per chi ne ha la disponibilità, di organizzare una campagna di attacchi. In questo caso gli obiettivi sono selezionati non per la loro specificità, ma perché considerati vulnerabili all'*exploit* in questione.

Gli attacchi mirati, invece, sono offensive rivolte contro uno specifico obiettivo. In questo caso i cyber-criminali stabiliscono una precisa strategia da adottare in base alle informazioni disponibili sulla vittima. A tal fine attacchi evoluti prevedono l'effettuazione di investimenti significativi utili, ad esempio, per eseguire un'estesa attività di ricognizione sulla vittima o *customizzare* il *ransomware* da impiegare nell'attacco. Inoltre lo studio preliminare della vittima supporta gli attaccanti anche nella valutazione delle migliori leve estorsive da impiegare, così da poter quantificare al meglio l'importo della somma da estorcere.
Gli attacchi ibridi si caratterizzano per la combinazione di tecniche e procedure impiegate in attacchi opportunistici e mirati: un avversario potrebbe, in un primo momento, lanciare un'offensiva rivolta a un numero indefinito di vittime per poi concentrare l'attività, in un secondo momento, su specifiche organizzazioni sulla base delle informazioni acquisite durante la prima ondata di attacchi cyber.

2. Attività propedeutiche al piano estorsivo

Questa fase racchiude tutte le attività che gli attaccanti svolgono per predisporre gli asset da impiegare durante gli step successivi del loro piano criminale, quali ad esempio la predisposizione di una *botnet* attraverso cui distribuire il *ransomware* o eseguire un attacco DDoS - *Distributed Denial of Service*[7], la personalizzazione del *ransomware* in base alle caratteristiche della vittima selezionata, oppure la predisposizione di canali di comunicazione da utilizzare per interagire con la stessa durante la negoziazione del riscatto.
In questa fase rientra anche la prima compromissione delle risorse IT della vittima, funzionale ad esempio all'accesso abusivo ai suoi sistemi e all'esfiltrazione di dati sensibili, azioni che in base al modello proposto vengono svolte una sola volta, indipendentemente dall'uti-

[7] Con il termine DDoS si fa riferimento a una tipologia di attacco cyber finalizzato all'interruzione della disponibilità di servizi informatici, creando le condizioni per la saturazione delle risorse disponibili. L'utilizzo di molteplici e dinamiche sorgenti di attacco (distributed) rende molto complessa l'attuazione di strategie di difesa efficaci.

lizzo ciclico di diverse leve estorsive funzionali a massimizzare la probabilità di pagamento del riscatto, cfr. fasi n° 3-7.

3. Attività intimidatorie

Una volta acquisite le potenzialità per portare avanti il piano estorsivo, gli attaccanti pongono in essere specifiche azioni con l'intento di produrre effetti intimidatori. Come si approfondirà nel capitolo *L'evoluzione delle leve estorsive*, in questa fase si svolgono attività volte a creare le condizioni affinché la vittima si convinca che l'attaccante abbia effettivamente le capacità e l'intento di nuocerle. In particolare questo avviene con azioni atte a minare la disponibilità di dati e/o sistemi informativi attraverso tecniche di cifratura o cancellazione di dati e/o con attacchi DDoS; oppure con tecniche volte a compromettere la riservatezza di informazioni sottratte direttamente o indirettamente alla vittima. Generalmente tali azioni sono eseguite in cicli successivi ad impatto crescente, in base all'andamento della trattativa per il pagamento del riscatto.

4. Rivendicazione

Ad ogni azione effettuata nella fase n° 3 segue la rivendicazione dell'attività intimidatoria. Le strategie di comunicazione connesse con questa fase si sono evolute nel corso del tempo, con una maggiore propensione per la rivendicazione pubblica. In passato, infatti, sui sistemi inficiati veniva mostrata una "*ransom note*" contenente le istruzioni su come mettersi in contatto con l'attore della minaccia per l'eventuale negoziazione e su come effettuare il pagamento per ottenere la chiave di decrittazione. Al giorno d'oggi, invece, i *threat actor* pubblicano sui propri *Data Leak Site* informazioni sulle vittime dei presunti attacchi *ransomware* da loro perpetrati. Tale modalità permette ai cyber-criminali anche di incrementare la propria reputazione, soprattutto nel caso di vittime particolarmente rilevanti.

Figura 3: *Ransom note utilizzata durante gli attacchi WannaCry, contenente la rivendicazione, la minaccia e la richiesta di riscatto.*

5. Minaccia

Alla rivendicazione dell'attività intimidatoria segue la minaccia. In questa fase l'attaccante minaccia la vittima di rendere persistenti i danni recatigli fino a quel momento, o di produrne di maggiori, e utilizza le azioni dimostrative svolte fino al quel momento come testimonianza della propria capacità di nuocere. Tale dinamica è propedeutica a indurre psicologicamente la vittima al pagamento del riscatto, facendo

leva sulla sua paura relativa agli impatti intimati. La minaccia si basa, quindi, sul danno che il *threat actor* potrebbe arrecare se le sue richieste non venissero soddisfatte. In questo ambito i cyber-criminali possono anche far uso dell'inganno, ad esempio rivendicando azioni eseguite da altri, o facendo credere alla vittima di poter arrecare più danno di quello che è nella loro reale possibilità. È possibile che in taluni casi gli attaccanti tentino di accreditarsi come attori della minaccia di tipo statuale per incutere maggior timore nelle vittime.

6. Richiesta di riscatto

Tutte le fasi precedenti sono finalizzate a creare le condizioni per aumentare la probabilità che la vittima decida di pagare il riscatto, in questa fase avviene la richiesta di denaro. La vittima riceve le informazioni su come procedere al pagamento e in quali tempi farlo. In alcuni casi le fasi n° 4, 5 e 6 prevedono un'unica comunicazione (**Figura 3**).

7. Negoziazione

A fronte della richiesta di riscatto, può avviarsi una fase di negoziazione tra il *threat actor* e la vittima, generalmente attraverso specifici canali di comunicazione predisposti ad hoc durante la fase n° 2.

Nel caso in cui la negoziazione dovesse andare a buon fine, la vittima procederà al pagamento della somma concordata, ponendo termine all'attacco. In caso negativo, l'attore potrebbe eseguire ulteriori azioni intimidatorie e cominciare un nuovo ciclo estorsivo.

8. Termine dell'Attacco

Nel caso di negoziazione andata a buon fine, il *threat actor* nella maggior parte dei casi pone fine al proprio piano d'attacco e condivide con la vittima le informazioni necessarie per annullare gli impatti subìti fino a quel momento. Nel caso di dati e infrastrutture ICT resi indisponibili attraverso tecniche crittografiche, la vittima riceve la chiave crittografica nominalmente utilizzabile per decifrare i dati. Tuttavia, in questo caso non vi è alcuna garanzia che la crittografia sia stata eseguita correttamente e che i file possano essere quindi decriptati a valle del pagamento della somma richiesta. Nel 2021 le organizzazioni che hanno pagato il riscatto hanno recuperato mediamente solo il 61% dei propri dati, rispetto al 65% del 2020, mentre solo il 4% è riuscita a recuperare l'intera quantità di risorse inficiate[8]. Se la disponibilità può considerarsi un processo reversibile, a netto dell'efficacia della cifratura, lo stesso non si può dire nel caso in cui sia la confidenzialità del dato ad essere compromessa: a fronte del pagamento di un riscatto, infatti, il *threat actor* potrebbe comunque vendere a terzi i dati della vittima o utilizzarli per attacchi futuri. Nel caso di fallimento della negoziazione, l'attaccante potrebbe concretizzare le azioni minacciate al punto n° 5 o, nell'eventualità in cui si sia avvalso dell'inganno per rafforzare l'intimidazione, potrebbe non effettuare alcuna azione.

[8] https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

L'attacco può anche terminare nel caso in cui la vittima riesca a mettere in campo contromisure tali da annullare il potere estorsivo dell'attacco, ad esempio recuperando i dati resi indisponibili dal *threat actor*[9] o sfruttando vulnerabilità negli algoritmi di cifratura utilizzati.

2. L'evoluzione delle leve estorsive

I primi attacchi *ransomware* condotti dai cyber-criminali usavano come unica leva estorsiva l'indisponibilità dei dati dell'organizzazione colpita, ottenuta attraverso la loro cifratura. Per incrementare ulteriormente il potere ricattatorio dell'attacco *ransomware*, i cyber-criminali hanno nel tempo sviluppato ulteriori tattiche che, usate in combinazione fra loro, permettono di ottenere livelli multipli di estorsione: doppia, tripla e quadrupla (**Figura 4**)[10].

Spesso gli attaccanti affiancano gradualmente nuove azioni estorsive a quelle già poste in essere nel caso in cui queste non siano sufficienti per l'ottenimento del pagamento del riscatto. Questo *modus operandi* è raffigurato nel ciclo, ripetibile più volte, descritto nello schema in Figura 2. Tipicamente con la doppia estorsione gli attaccanti, oltre a cifrare i dati delle vittime, ne minacciano la divulgazione nel *dark/clear web*[11] o la vendita a terzi (come, ad esempio, a *competitor* di settore).

La tripla estorsione, nella maggior parte dei casi prevede di aggiungere alla cifratura e alla minaccia di divulgazione dei dati, quella di attacchi DDoS ai danni dei servizi IT della vittima esposti su internet, finchè quest'ultima non ottempera alle condizioni poste dai *threat actor*. Con la quadrupla estorsione gli attaccanti, per porre ulteriormente sotto pressione la vittima e convincerla al pagamento del riscatto, interagiscono direttamente con entità interdipendenti dall'organizzazione colpita, come ad esempio i dipendenti, i clienti, il *Board* o i fornitori, minacciando la pubblicazione dei dati a loro riferiti.

[9] L'utilizzo del back-up rimane, infatti, il metodo più utilizzato per ripristinare i dati criptati, usato dal 73% delle organizzazioni colpite da ransomware nel 2021.

[10] https://www.theregister.com/2022/10/09/extortion_ransomware_threats_category

[11] Nel primo trimestre del 2023, il gruppo cyber-criminale ALPHV ha aggiornato la propria tattica estorsiva introducendo la creazione di falsi siti, replicanti quelli delle proprie vittime (typosquatting), su cui pubblicare i dati sottratti. https://www.bleepingcomputer.com/news/security/ransomware-gang-cloned-victim-s-website-to-leak-stolen-data/

Figura 4: *Livelli di estorsione possibili durante un attacco ransomware.*

Una variante di tale leva estorsiva è stata introdotta dal gruppo *cyber*-criminale russofono DarkSide nei confronti delle organizzazioni quotate al NASDAQ: la nuova tattica consiste nell'informare anticipatamente gli *stock trader* dell'imminente pubblicazione di dati esfiltrati relativi alle stesse, favorendo potenziali profitti derivanti dal calo di prezzo delle loro azioni a seguito della divulgazione della violazione subìta[12]. Un'altra variante di quadrupla estorsione particolarmente innovativa è stata quella utilizzata dal gruppo *ransomware* DeadBolt che nel 2022 ha colpito i possessori di NAS del fornitore QNAP attraverso una vulnerabilità *zero-day*. Il gruppo ha contemporaneamente richiesto un riscatto sia ai possessori dei NAS, per ottenere la chiave di decifrazione del loro dispositivo, sia al fornitore stesso, per il rilascio della chiave principale di decrittazione di tutti i clienti vittima. Inoltre, il gruppo ha offerto la sua disponibilità a fornire l'*exploit* utilizzato per l'attacco al prezzo di 5 Bitcoin (pari a 184.000 dollari) al fornitore QNAP.
La combinazione delle leve estorsive fin qui esposta corrisponde a quanto riscontrato nei principali casi di attacchi *ransomware* occorsi negli ultimi anni. È possibile, tuttavia, trovare anche delle casistiche diverse. Il gruppo cyber-criminale Lockbit, ad esempio, ha specificamente richiesto ai propri affiliati di impiegare la sola divulgazione dei dati, senza la loro cifratura, per i settori maggiormente critici, come quello sanitario, poiché l'impiego della criptazione, con la conseguente paralizzazione del sistema informativo di un ospedale, potrebbe avere conseguenze drammatiche sulle vite umane.

[12] https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

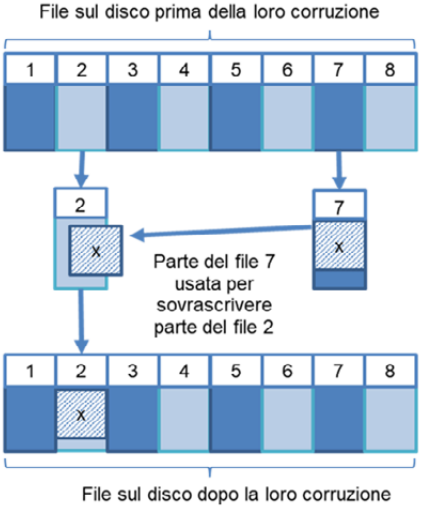


Figura 5: *Attacco ransomware mediante corruzione parziale dei file*

La cifratura totale dei dati non è la sola tecnica utilizzata dagli attaccanti per rendere indisponibili i dati della vittima al primo livello di estorsione. Negli ultimi anni, infatti, si sono riscontrate diverse varianti di tale tecnica, in particolare: *(a)* la crittografia intermittente, che consiste nella cifratura di alcune porzioni dei file al posto della loro totalità, al fine di ridurre il tempo necessario per completare il processo di crittografia; *(b)* la corruzione parziale dei dati, mediante la quale alcuni file sono sovrascritti casualmente da porzioni di altri file (**Figura 5**). Tutto ciò, oltre a rendere l'attacco più difficilmente individuabile dagli algoritmi euristici dei *software* di sicurezza, riduce la durata complessiva dell'attacco, mantenendo comunque elevati gli impatti sulla disponibilità dei dati alla vittima. Infine in tale caso gli attaccanti non devono più preoccuparsi di sviluppare e mantenere complessi moduli crittografici, né le relative infrastrutture per la distribuzione delle chiavi di cifratura, riducendo notevolmente i costi gestionali legati all'impiego del *ransomware*.

In **Figura 6** si propone uno schema sinottico riepilogativo delle prestazioni delle leve estorsive, in termini di rapidità di conduzione dell'attacco e impatti sulla disponibilità e riservatezza dei dati compromessi, relative a quattro tecniche principali che prevedono: la sola esfiltrazione dei dati, la crittografia completa senza esfiltrazione, la crittografia intermittente e l'esfiltrazione unita alla corruzione parziale dei dati.

3. I nuovi modelli di business

L'industrializzazione degli attacchi *ransomware*, avvenuta progressivamente negli ultimi anni, si è caratterizzata per la diffusione del modello di *business* criminale denominato *Ransomware as a Service (RaaS)* e per la sua successiva evoluzione in *Ransomware as a Corporation (RaaC)*. Nel primo caso si è assistito ad una stratificazione della catena del valore degli attacchi *ransomware* e ad una conseguente creazione di un indotto di servizi specializzati, funzionali all'orchestrazione di attacchi efficaci. Questo ha determinato una diversificazione dei cyber-criminali in sottogruppi altamente qualificati, che erogano "servizi" *RaaS* gli uni versi gli altri o verso terze parti. In **Figura 7** sono rappresentate le principali specializzazioni e le relative interazioni per l'organizzazione e la conduzione di un attacco *ransomware*: *(a)* gli «*Initial Access Broker*» **(IAB)** sono attori specializzati nell'ottenere e

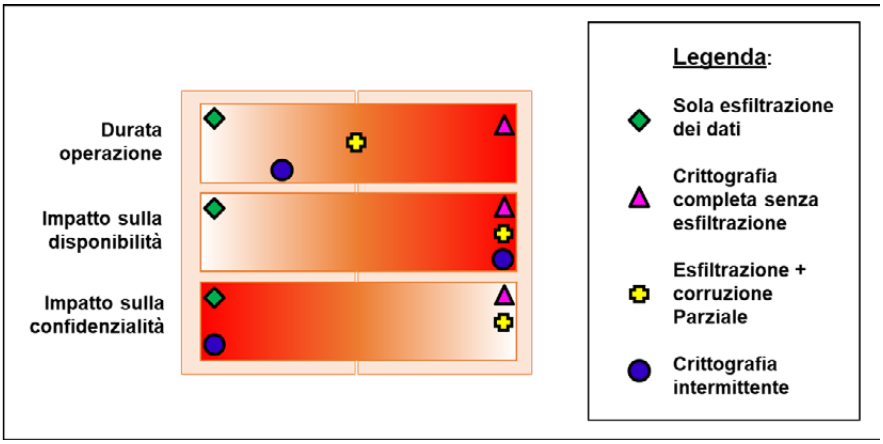


Figura 6: *Confronto fra gli impatti sulla disponibilità, la confidenzialità e velocità di operazione di quattro diverse azioni effettuabili dai cyber-criminali durante un attacco ai dati*

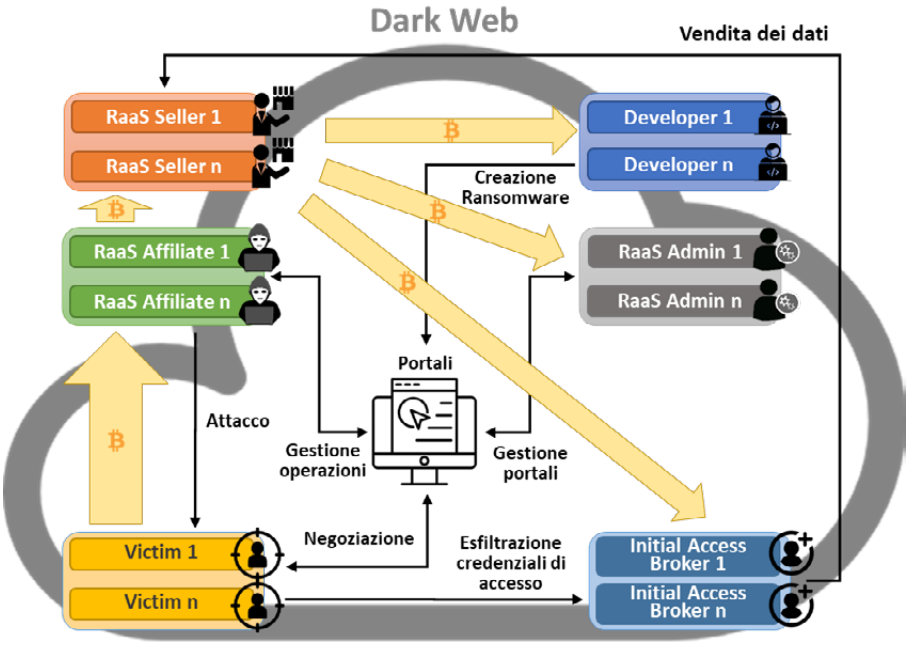


Figura 7: *Relazioni fra i vari attori del modello criminale Ransomware as a Service*

vendere gli accessi remoti alle reti aziendali delle vittime; *(b)* i «*RaaS Seller*» **si occupano di coordinare le compravendite** di tool e informazioni utilizzate nell'attacco, gestendo i contatti con tutti gli altri attori; *(c)* i «*RaaS Admin*» **forniscono l'accesso all'infrastruttura da** adoperare per gestire le operazioni; *(d)* i «*Malware Developer*» sono incaricati dello sviluppo e della personalizzazione del *ransomware; (e)* i «*RaaS Affiliate*» sono coloro che effettivamente attaccano la vittima, inoculando il *ransomware* e gestendo poi tutte le azioni finalizzate al pagamento del riscatto. L'infrastruttura che i *Raas Admin* forniscono agli affiliati può includere, a seconda dei casi: un *data leak site* (*DLS*), in cui vengono pubblicati i dati sottratti alle vittime; un *affiliate portal*, da cui l'affiliato lancia e gestisce le proprie offensive *ransomware*; un terzo portale dedicato alla comunicazione con le vittime durante la trattativa del pagamento del riscatto.

La piattaforma tecnologica di cui usufruiscono gli affiliati può contenere non soltanto un arsenale *ransomware* completo con capacità operative pronte all'uso, ma anche materiali didattici e *playbook* che spiegano le procedure di attacco consigliate[13]. A prescindere dalle loro capacità tecniche quindi, gli affiliati dei servizi *RaaS* possono gestire in piena autonomia tutte le fasi operative dell'attacco, partendo dalla creazione di *ransomware* ad hoc fino ad arrivare alla ricezione del riscatto da parte delle vittime, attraverso servizi integrati di pagamento in criptovaluta. Durante una campagna d'attacco, gli affiliati possono anche monitorare l'impatto dell'offensiva mediante *key perfomance indicator (KPI)*[14]. Infine i servizi dei portali *RaaS* consentono anche di minacciare ulteriormente la vittima attraverso l'esecuzione di attacchi *DDoS,* gestibili direttamente dal *management panel* del portale, come avviene ad esempio nel caso dei gruppi Darkside e Lockbit. La diffusione di questi servizi ha portato ad una riduzione delle competenze necessarie per entrare nell'industria del *ransomware*, incrementando, allo stesso tempo, il grado di sofisticatezza e la relativa percentuale di successo delle azioni offensive, anche quando queste sono condotte da attori poco specializzati.

Gli ampi guadagni ricavabili dai riscatti pagati dalle organizzazioni colpite da attacchi *ransomware* ha nel tempo aumentato la competizione tra i gruppi criminali, la quale ha favorito l'evoluzione del RaaS verso un più avanzato modello organizzativo già citato, denominato *Ransomware as a Corporation*, caratterizzato dall'utilizzo di innovative piattaforme tecnologiche per la gestione automatizzata degli attacchi, efficienti canali di supporto ai clienti e specifiche strategie di marketing.
Al riguardo, alcuni gruppi *ransomware* adottano, ad esempio, un forte approccio incentrato sul cliente, facendo pubblicità dei loro servizi su *forum underground* e su siti presenti nel

[13] Nel mese di agosto 2022, un affiliato del gruppo Conti, scontento per la sua paga, ha pubblicato un archivio contenente diverso materiale relativo al gruppo (tool, playbook, guide, etc.), che dimostra il livello di supporto fornito dai provider di servizi RaaS: https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/

[14] Asseritamente: numero di macchine infettate, volume di dati trafugati e stato di pagamento da saldare da parte delle vittime.

dark web, oltre che prevedendo canali dedicati alla vendita e all'assistenza per i propri affiliati, unitamente a portali *"press center"* all'interno dei quali divulgare gli incidenti di sicurezza o pubblicare le informazioni esfiltrate. Si assiste allo sviluppo di vere e proprie strategie di comunicazione rivolte, contestualmente, sia ai cyber-criminali che all'opinione pubblica. In questo ultimo frangente si concedono interviste alla stampa in cui si sottolineano, ad esempio, i codici di condotta adottati, che possono includere il divieto per gli affiliati di prendere di mira alcuni settori particolari come quello sanitario (**Figura 8**), o le donazioni di parte dei guadagni illeciti in beneficenza. Non di rado i gruppi *ransomware* stringono accordi con società di sicurezza specializzate nella decriptazione dei dati, al fine di supportare le vittime nelle attività di ripristino delle risorse inficiate, o con società intermediarie che si occupino della gestione della negoziazione o del pagamento del riscatto.

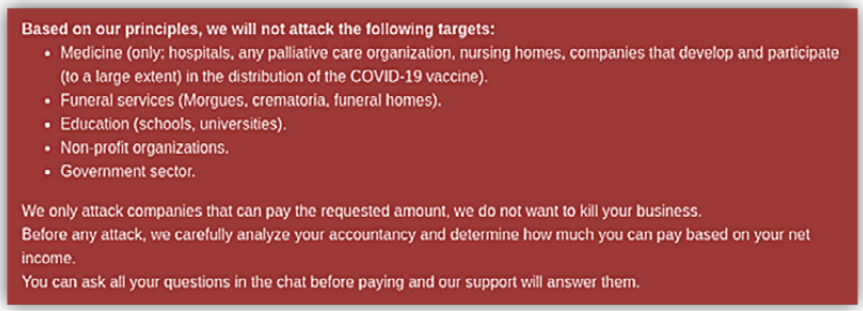


Figura 8: *Codice di condotta del gruppo ransomware DarkSide*

Recentemente si osserva anche una crescente attenzione da parte dei cyber-criminali alla sicurezza cyber delle loro infrastrutture tecnologiche: ad esempio il gruppo Lockbit 3.0 ha avviato un'iniziativa pubblica per la rilevazione di vulnerabilità sui propri sistemi IT (*"Bug Bounty Program"*).

Con riferimento alla prima fase del modello in Figura 2, i *RaaS Affiliate*, al pari di aziende lecite, cercano di massimizzare il profitto economico sui loro investimenti, conducendo prima della scelta della vittima vere e proprie analisi di mercato al fine di comprendere il quadro finanziario dell'azienda *target* al fine di identificare la somma adeguata da chiedere per il riscatto; ad esempio, nel caso in cui la vittima abbia un'assicurazione contro i rischi cyber, allora gli attaccanti potrebbero utilizzare l'ammontare del premio assicurativo per fissarne l'importo.

4. L'impiego dei ransomware per supportare interessi statuali

Il *ransomware* nasce originariamente con lo scopo criminale di ottenere un provento economico. Tuttavia recentemente si è rilevato un incremento di attacchi *ransomware* correlato a motivazioni geopolitiche, plausibilmente per via delle sue potenzialità intrinseche di causare danni sistemici alle infrastrutture critiche nazionali. Questo *trend* è emerso special-

mente in relazione al mutamento dello scenario della minaccia cyber connesso al conflitto russo ucraino in cui, attraverso la strategia della *proxy warfare*[15], *threat actor* generalmente afferenti alla sfera del *cyber-crime* hanno plausibilmente agito negli interessi di Mosca[16]. La *proxy warfare* non solo permette all'entità (ad esempio attori di matrice statuale) che ingaggia intermediari (cyber-criminali) di potersi dichiarare totalmente estranea alle attività cyber condotte da quest'ultimi (*plausible deniability*), ma consente anche di eseguire una esternalizzazione delle capacità offensive, rendendo possibile sfruttare TTP già consolidate. Oltre che da cyber-criminali, il *ransomware* è utilizzato anche da *threat actor* statuali, che sfruttano tale minaccia con diversi obiettivi. Può ad esempio essere impiegata come diversivo per le attività di spionaggio digitale o come supporto alle operazioni cinetiche ai danni delle infrastrutture critiche di paesi avversari, come nel caso dell'attacco di ottobre 2022 perpetrato da Sandworm (noto anche come IRIDIUM[17]) attraverso la campagna *ransomware* Prestige[18] rivolta contro alcune organizzazioni ucraine e polacche del settore dei trasporti e della logistica. Anche a livello nazionale sono stati registrati attacchi *ransomware*, con impatti circoscritti, ai danni di entità operanti nelle filiere dell'energia, dei trasporti, della finanza e del settore governativo perpetrati da gruppi criminali sponsorizzati, in alcuni casi, da entità statuali[19].

Attori di matrice statuale utilizzano il *ransomware* anche come strumento di guerra economica, al fine di raccogliere fondi a supporto del governo che li commissiona. Un esempio è rappresentato dalla campagna del 2017 nota con il nome di WannaCry, la cui responsabilità è stata attribuita ufficialmente al *threat actor* nordcoreano Lazarus. L'attacco ha avuto un impatto globale, reso possibile da un metodo di auto propagazione del *ransomware* altamente efficace, basato sullo sfruttamento di EternalBlue[20], e ha permesso di colpire più di

[15] Nel contesto del conflitto tra stati nel dominio cibernetico, l'espressione proxy warfare identifica la strategia che prevede la conduzione di operazioni cyber offensive da parte di "forze non convenzionali". Queste sono costituite da intermediari (proxy), non appartenenti all'entità statuale che li ingaggia, funzionali ad aumentare la non riconducibilità tra mandanti ed esecutori materiali di operazioni cyber. L'obiettivo è quello di dichiararsi formalmente estranei a qualsivoglia fattispecie deprecabile commessa da terzi (plausible deniability).

[16] A supporto di tale trend evolutivo, Alexander Khinshtein, capo del Comitato della Duma di stato per la politica dell'informazione della Federazione Russa, il 10 febbraio ha rilasciato una dichiarazione in cui affermava che si sarebbero dovute stabilire delle garanzie legislative per gli hacker che lavorano nell'interesse dello Stato. https://www.vedomosti.ru/politics/news/2023/02/10/962551-v-gosdume-predlozhili-ne-nakazivat

[17] Sandworm è un attore statuale russo ritenuto legato al GRU, il Servizio d'intelligence delle forze armate in Russia. Il gruppo è noto per il devastante attacco globale NotPetya che nel 2017 causò il blocco di numerose industrie e ospedali, generando danni stimati in oltre un 1 miliardo di dollari.

[18] https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

[19] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2023/02/Relazione_annuale_2022_interattiva.pdf

[20] Un exploit sviluppato dalla National Security Agency (NSA) degli Stati Uniti per i sistemi Windows. EternalBlue è stato rubato e trapelato da un gruppo chiamato The Shadow Brokers un mese prima dell'attacco.

300.000 computer in 150 paesi[21] causando perdite globali di circa 4 miliardi di dollari[22].

5. La flessione dei ricavi rivenienti da attacchi ransomware

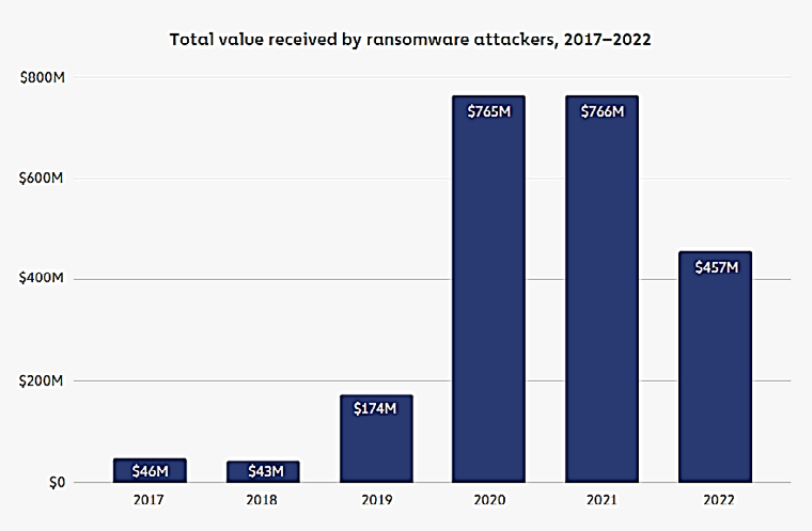


Figura 9: *Ricavi annuali complessivi ottenuti con attacchi ransomware (fonte Chainalys, "The 2023 Crypto Crime Report", Febbraio 2023)*

Come confermato da studi specialistici di settore, nel 2022 si è registrata una flessione rilevante dei ricavi annuali complessivi ottenuti dagli attacchi ransomware rispetto al trend degli anni precedenti[23] (**Figura 9**). Tale fenomeno è imputabile ad una pluralità di fattori, fra cui spiccano sia le diverse iniziative internazionali volte a disincentivare il pagamento del riscatto, che la promozione di azioni di prevenzione e contrasto utili a innalzare la cyber-resilience a livello globale.
Ad esempio l'Office of Foreign Assets Control (OFAC) degli Stati Uniti D'America nel 2021 ha emesso delle raccomandazioni in merito alla gestione della minaccia *ransomware*, sottolineando i rischi di sanzioni a cui le organizzazioni potrebbero incorrere nel caso in cui dovessero cedere al pagamento di un riscatto.

[21] https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

[22] https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[23] La flessione registrata al momento è circa il 40% rispetto all'anno precedente. Tuttavia il valore dei ricavi del 2022 potrebbe plausibilmente aumentare di alcuni punti percentuale in considerazione di potenziali nuovi elementi informativi.

Tra le iniziative per il contrasto della minaccia *ransomware* a livello globale è importante citare anche: (a) il progetto **No More Ransom**[24] lanciato nel 2016 dal National High Tech Crime Unit della Polizia Olandese in collaborazione con EUROPOL, Kaspersky e McAfee con lo scopo di fornire supporto alle vittime, fornendo anche numerosi strumenti di decriptazione dei dati[25]; (b) i **G7 Fundamental elements of ransomware resilience**, pubblicati nell'Ottobre 2022 dai Ministri dell'Economia e delle Finanze e i Governatori delle Banche Centrali dei Paesi G7[26], che contengono una serie di raccomandazioni e misure minime indirizzate alle entità finanziarie pubbliche e private; *(c)* l'iniziativa **Partnership against Cybercrime**, lanciata nel 2020 dal World Economic Forum, che mira a realizzare un partenariato pubblico-privato per combattere la criminalità informatica coinvolgendo le principali forze dell'ordine, organizzazioni internazionali, società di sicurezza informatica, fornitori di servizi e piattaforme.

Una sempre più efficiente coordinazione delle forze dell'ordine a livello internazionale, unitamente alla diffusione di *public rewards* per coloro che offrono informazioni sui cyber-criminali, hanno permesso di tracciare, perseguire e arrestare membri di diversi gruppi *ransomware*, dismettere le infrastrutture impiegate e sequestrare parte dei fondi illecitamente ottenuti.

Anche la Banca d'Italia, nell'ambito delle attività propedeutiche alla rilevazione delle operazioni finanziare sospette, ha sottolineato già dal 2019[27] la necessità di valutare se l'attività di raccolta di capitale in valute virtuali possa essere messa in relazione con fondi di provenienza illecita, con particolare riferimento alle possibili connessioni con fenomeni criminali caratterizzati dall'utilizzo di tecnologie informatiche quali il *ransomware*. Ultimamente difatti, le informazioni nella disponibilità degli operatori in valute virtuali offrono nuove prospettive per l'analisi finanziaria: alla tradizionale ricostruzione dei flussi in valuta legale si affiancano le potenzialità derivanti dai sistemi di analisi forense della *blockchain,* che consentono di superare, almeno in parte, i problemi di tracciabilità delle valute virtuali, con la derivante possibilità di intercettare fenomeni anche emergenti.[28]

---

[24] https://www.nomoreransom.org/

[25] Dalla sua nascita fino a luglio 2021 l'iniziativa ha impedito ai criminali informatici di guadagnare illegalmente oltre 900 milioni di dollari. https://www.kaspersky.com/about/press-releases/2021_high-five-no-more-ransom-initiative-celebrates-fifth-successful-year-of-fighting-ransomware

[26] In particolare, i G7 Fundamental Elements of Ransomware Resilience for the Financial Sector contengono raccomandazioni indirizzate alle entità finanziarie pubbliche e private volte ad affrontare la crescente minaccia di attacchi ransomware, identificando le misure minime da adottare sia a fini di prevenzione che per mitigare gli impatti di eventuali attacchi.

[27] https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/comunicazione_vv_2019.pdf

[28] https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/Newsletter_5_2022.pdf

Conclusioni

La minaccia *ransomware* è caratterizzata da una capacità, particolarmente marcata, di innovarsi ed evolvere rapidamente. Per tale ragione, per contrastare efficacemente questo fenomeno a livello locale e sistemico è necessario conoscerlo e seguirne costantemente i molti profili evolutivi.

Tale abilità è definita con il termine di *situational awareness*, ovvero la capacità, ai diversi livelli decisionali di una organizzazione, di comprendere adeguatamente l'evoluzione dello scenario della minaccia cyber in relazione alle caratteristiche degli interessi da proteggere.

La *situational awareness* si basa su quattro pilastri fondamentali: *(a)* la CTI intesa come applicazione della dottrina intelligence all'analisi di informazioni utili a conoscere le caratteristiche dei *threat actor*; *(b)* la cooperazione e lo scambio informativo volontario sulla minaccia cyber[29]; *(c)* il monitoraggio del dominio digitale, in cerca di "precursori" connessi con potenziali attacchi cibernetici; *(d)* la *security awareness*, utile a trasformare il fattore umano da vulnerabilità in sensore vivente.

Considerando l'attuale scenario della minaccia cyber, è possibile desumere che l'inversione di tendenza nella continua consistente espansione di questo genere di fenomeno, potrà avvenire quando gli attaccanti considereranno meno profittevole il riscorso al cyberspazio per l'ottenimento dei propri obiettivi, in termini di costi e rischi.

[29] Incentivato anche dalla versione aggiornata della direttiva NIS pubblicata a dicembre 2022 e dal regolamento europeo DORA. La NIS2, in vigore dal 16 gennaio 2023, sancisce l'adozione da parte di ciascuno Stato membro di una strategia nazionale di cyber-security, aggiornata rispetto a quella disciplinata dalla NIS, che integra un quadro strategico volto al rafforzamento del coordinamento tra autorità competenti preposte alla condivisione delle informazioni (information sharing), anche di natura volontaria, eventualmente anche fra i soggetti rientranti e non nell'ambito di tale normativa, di appositi accordi di condivisione volontaria delle informazioni sulla cyber-security. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&from=IT. Il Digital Operational Resilience Act è un regolamento europeo atto a incrementare la cyber-resilience del settore finanziario, pubblicato a dicembre 2022 e che si applicherà a decorrere dal 17 gennaio 2025. Indirizzato alle entità finanziare degli stati membri e ai loro fornitori di servizi tecnologici, ha l'obiettivo di incrementare la resilienza digitale dell'intero sistema finanziario europeo attraverso lo sviluppo di capacità di cyber threat intelligence (CTI) funzionali all'innalzamento dei livelli di cyber-resilience e cyber-defense delle singole organizzazioni. Per raggiungere l'obiettivo prefissato, il Regolamento promuove la condivisione volontaria delle informazioni e dei dati sulle minacce cyber con lo scopo di potenziare la resilienza operativa digitale delle entità finanziarie su tutto il territorio dell'UE. https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2554&from=IT

Netwrix Cloud Data Security Report 2022

[A cura di Dirk Schrader e Michael Paye, Netwrix]

EXECUTIVE SUMMARY

L'infrastruttura cloud è diventata parte integrante dei carichi di lavoro quotidiani per milioni di organizzazioni in tutto il mondo. Dopo l'improvviso passaggio al lavoro da remoto nel 2020, l'adozione del cloud è ancora in corso e, come dimostra questo rapporto, dovrebbe continuare nei prossimi 12-18 mesi. Netwrix Research Lab ha aggiornato i propri report "Cloud Data Security" rilasciati rispettivamente nel 2020 e nel 2019 per riflettere l'evoluzione della sicurezza cloud. Nel 2022 abbiamo intervistato 720 professionisti IT in tutto il mondo tramite un questionario online. Questo report aiuterà le organizzazioni a concentrare i loro sforzi di sicurezza su cosa conti davvero ed evidenzia i principali ostacoli sulla strada verso un cloud computing sicuro.

ADOZIONE DEL CLOUD

Le organizzazioni si sono rivolte al cloud principalmente per ridurre i costi e migliorare la sicurezza. L'80% di coloro che utilizzano il cloud vi ci memorizza i dati sensibili. La più grande sfida per l'adozione del cloud, indicata dal 41% degli intervistati, è l'integrazione con l'ambiente IT esistente.

RILEVAMENTO DI UN INCIDENTE

L'84% degli intervistati ritiene che il tempo necessario per rilevare un incidente sia rimasto invariato. Questo è come hanno valutato i loro progressi nell'ultimo anno. Un'analisi più approfondita rivela che il tempo medio di rilevamento per la maggior parte dei tipi di attacchi è effettivamente aumentato dal 2020. I rallentamenti più significativi possono essere osservati in merito all'individuazione della compromissione della catena di approvvigionamento e degli attacchi ransomware.

INCIDENTI DI SICUREZZA NEL CLOUD

Il 53% degli intervistati ha subito un attacco informatico negli ultimi 12 mesi. Il phishing è stato l'incidente più comune: il 73% degli intervistati ha confermato di essere stato vittima di questo tipo di attacco nell'ultimo anno. Inoltre, gli attacchi mirati alle infrastrutture cloud sono aumentati in modo significativo: il 29% degli intervistati ha subito questo tipo di attacco nel 2022, rispetto al 16% nel 2020.

LE CONSEGUENZE DI UNA VIOLAZIONE DATI

Le violazioni dei dati stanno diventando sempre più costose. Quest'anno, il 49% degli intervistati ha affermato che un attacco ha portato a spese non pianificate per colmare le falle di sicurezza, rispetto al 28% nel 2020. La percentuale di coloro che hanno subito sanzioni in materia di conformità è più che raddoppiata (dall'11% al 25%), così come il numero di coloro che hanno visto calare la valutazione della propria azienda (dal 7% al 17%).

MISURE DI SICUREZZA DEL CLOUD

Più della metà (55%) degli intervistati ha dichiarato che gli attori esterni sono la principale minaccia per il loro ambiente IT. L'autenticazione a più fattori (MFA) e il backup su cloud sono in cima all'elenco delle misure di protezione. Entrambi hanno registrato aumenti dal 2020: l'adozione dell'MFA è passata dal 57% al 69% e i backup sono aumentati, seppur marginalmente, dal 58% al 63%.

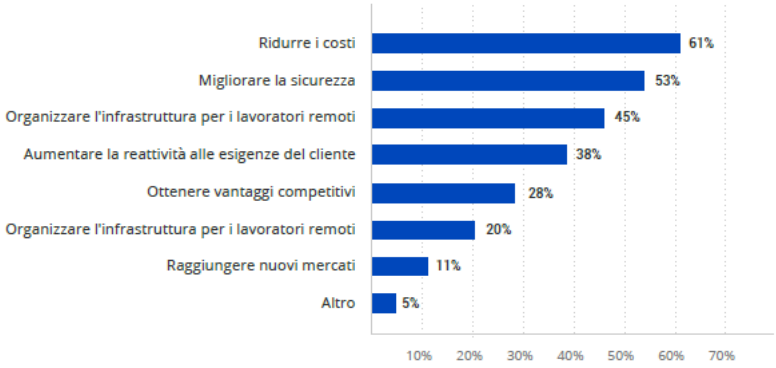
BUDGET

Il 49% dei nostri intervistati ha affermato che il proprio budget per la sicurezza nel cloud è aumentato nel 2022. Inoltre, le organizzazioni stanno allocando una parte maggiore del proprio budget relativo alla sicurezza informatica a quello della sicurezza nel cloud: in media, il 32% del budget per la sicurezza informatica viene ora speso per la sicurezza nel cloud, rispetto al 27 % nel 2020. Ciò significa un aumento del 23% del budget speso per la sicurezza del cloud nel 2022 rispetto al 2020.

OBIETTIVI E SFIDE DELL'ADOZIONE DEL CLOUD

Il sondaggio ha rilevato che i due principali obiettivi dell'adozione del cloud sono la riduzione dei costi ed il miglioramento della sicurezza. Il supporto ai lavoratori remoti si è classificato al terzo posto, il che indica che la pandemia potrebbe aver accelerato l'adozione del cloud, ma l'efficienza in termini di costi e la sicurezza sono i driver più significativi.

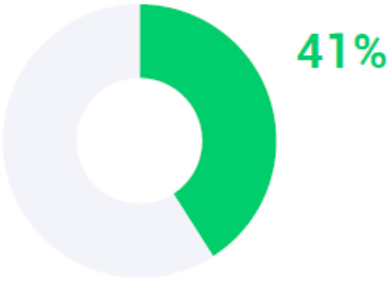
Obiettivi principali dell'adozione del cloud



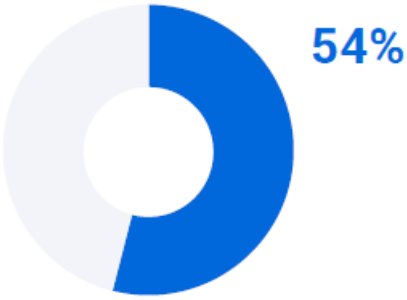
COSA C'È NEL CLOUD?

In media, le organizzazioni riferiscono che il 41% dei loro carichi di lavoro è già nel cloud e si aspettano che tale quota aumenti al 54% entro la fine del 2023.

Qual è la percentuale dei tuoi carichi di lavoro che si trova attualmente nel cloud?



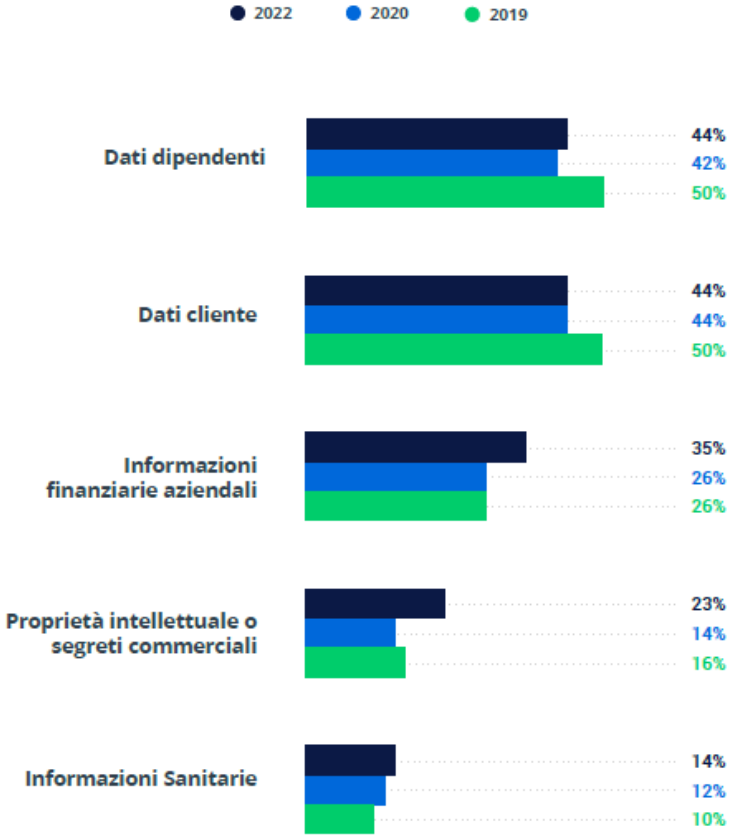
Qual è la percentuale dei tuoi carichi di lavoro che è pianificata per passare al cloud tra 12-18 mesi?



L'archiviazione di dati sensibili nel cloud non è cambiata molto da quando è scoppiata la pandemia nel 2020; tuttavia, i numeri per le due categorie principali sono ancora inferiori rispetto a quelli del 2019. Ad esempio, la percentuale di organizzazioni che archiviano i dati dei clienti nel cloud è scesa dal 50% nel 2019 al 44% nel 2020 per poi rimanere invariata nel 2022; i dati dei dipendenti sono scesi dal 50% nel 2019 al 42% nel 2020, per poi salire gradualmente fino al 44% nel 2022. D'altra parte, la quota di coloro che archiviano informazioni finanziarie aziendali nel cloud è passata dal 26% nel 2019 e 2020 a 35% nel 2022.

L'**80%** degli intervistati archivia i dati sensibili nel cloud. Le tipologie di dati più comuni sono le informazioni personali dei dipendenti e le informazioni identificative personali dei clienti.

Tipi di dati sensibili che le organizzazioni archiviano nel cloud

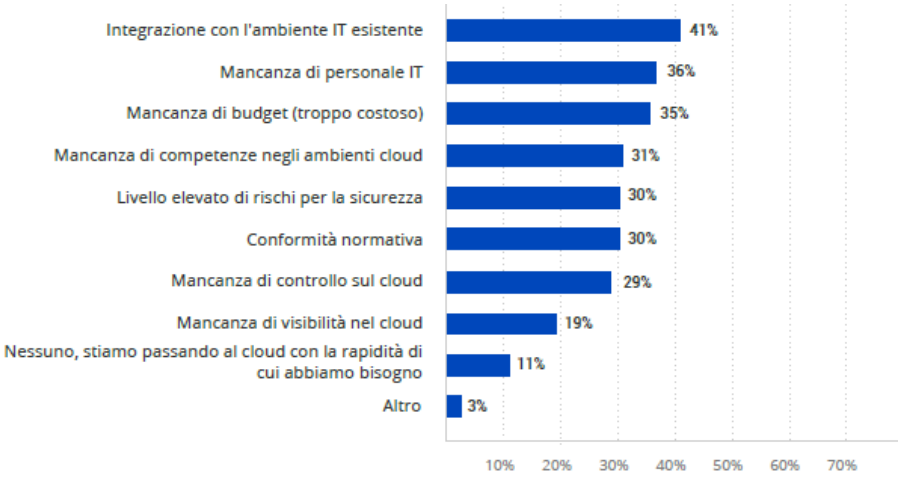


Solo il **20%** delle organizzazioni che utilizzano il cloud non vi memorizzano i propri dati sensibili.

QUALI SONO LE PIÙ GRANDI SFIDE DEL CLOUD?

La sfida più grande per una rapida adozione del cloud, citata dal 41% degli intervistati, è l'integrazione con l'ambiente IT esistente. Il secondo fattore che ostacola il processo è la mancanza di personale IT. La riduzione dei costi è la ragione principale per passare al cloud per il 61% degli intervistati, ma il 35% ha affermato che la spesa per l'adozione del cloud ha rallentato il passaggio al cloud. "*Questo è un aspetto complicato dell'infrastruttura cloud: le infrastrutture cloud ed on-premise sono troppo diverse per provare a spostare ogni carico di lavoro così com'è; in effetti, un approccio lift-and-shift può comportare notevoli spese extra e persino richiedere costose riprogettazioni dell'architettura se i problemi vengono rilevati in una fase avanzata del processo*", commenta Mike Paye, vicepresidente della ricerca e sviluppo di Netwrix. "*Ad esempio, se si dispone di un'applicazione che si basa su un backend SQL, è possibile riprodurla esattamente nel cloud con una macchina virtuale che esegue Microsoft SQL Server. Tuttavia, questa sarà probabilmente l'architettura meno efficiente e più costosa a cui si possa pensare. Da questo punto di vista, sembra che alcuni degli intervistati che affermano che la loro migrazione al cloud è stata troppo costosa potrebbero non avere competenze sufficienti con gli ambienti cloud*". Tuttavia, le spese di un'infrastruttura cloud possono essere più difficili da prevedere rispetto a quelle di un ambiente locale.

Fattori che rallentano l'adozione del cloud

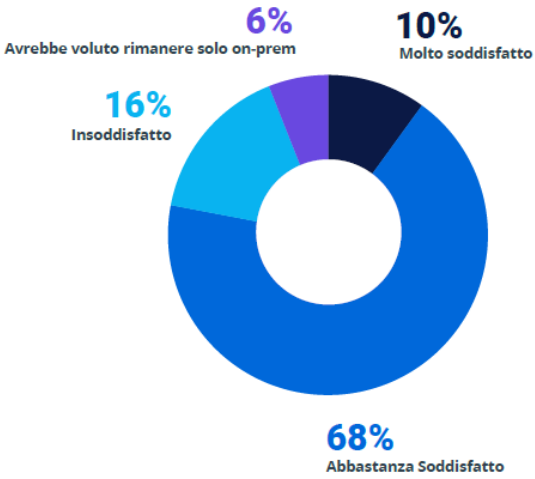


Tra i maggiori grattacapi che i CIO devono affrontate vi sono sicuramente la mancanza di esperienza nel cloud e l'integrazione con l'ambiente IT esistente: questi sono in cima alla lista per il 33% dei CIO interpellati.

INCIDENTI DI SICUREZZA NEL CLOUD

Più della metà (53%) degli intervistati ha scelto il miglioramento della sicurezza come obiettivo principale per l'adozione del cloud. Sembra che abbiano raggiunto questo obiettivo: il 78% degli intervistati, infatti, afferma di essere soddisfatto della sicurezza cloud della propria organizzazione.

Tasso di soddisfazione per la sicurezza del cloud



Il **25%** dei CISO non è soddisfatto della sicurezza cloud della propria organizzazione

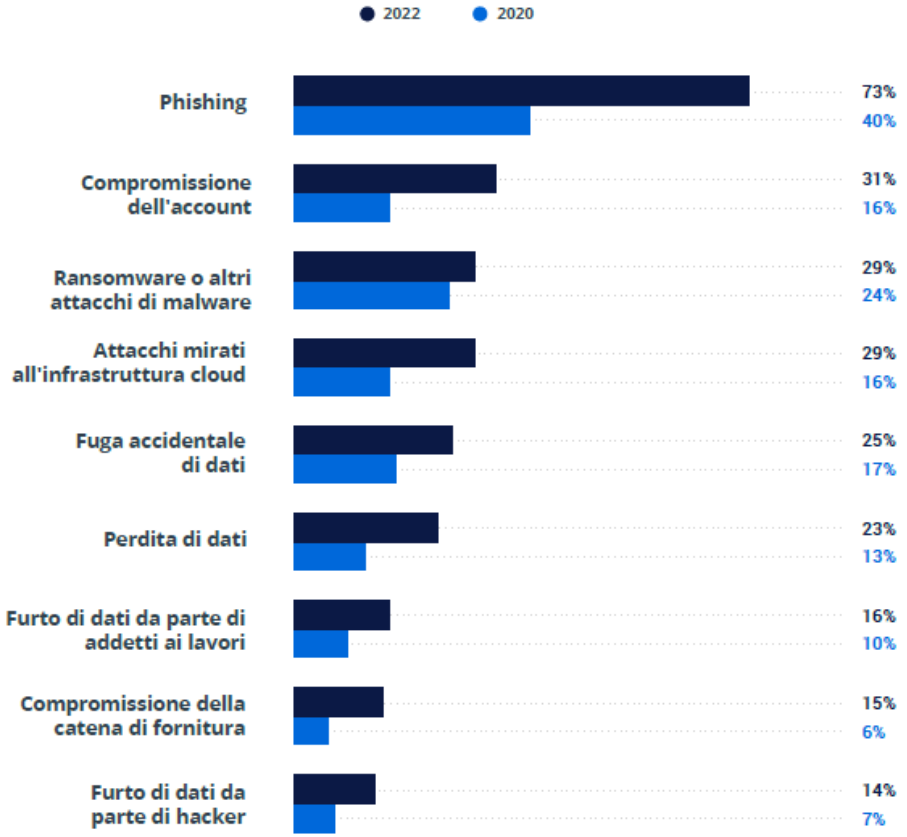
ATTACCHI NEL CLOUD

CIO:

> *"Gli attacchi non sono una questione di se, ma di quando."*

Il 53% degli intervistati 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 47% ha avuto un anno molto fortunato o semplicemente non ha ancora scoperto l'incidente. Abbiamo chiesto a coloro che hanno subito attacchi informatici di fornire maggiori dettagli su quanto accaduto e abbiamo confrontato queste risposte con i risultati del 2020.

Gli incidenti di sicurezza cloud più comuni

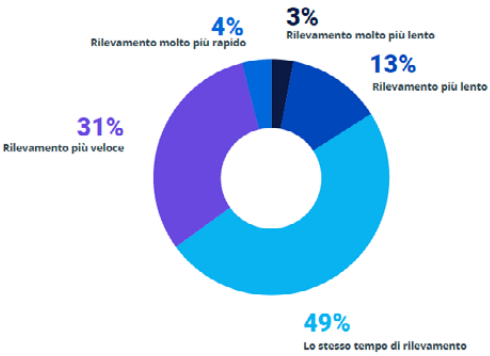


Il phishing è stato l'incidente più comune. Nonostante fosse in cima anche nel 2020, la percentuale di organizzazioni che hanno subito questo tipo di attacco è quasi raddoppiata, passando dal 40% al 73%. Inoltre, il 63% degli intervistati ha affermato di aver subito questo tipo di attacco più volte. Anche gli attacchi mirati all'infrastruttura cloud sono aumentati in modo significativo: il 29% degli intervistati ha subito questo tipo di attacco nel 2022, rispetto al 16% nel 2020. E questo perché più sono i carichi di lavoro che vengono spostati nel cloud, e più saranno gli attacchi mirati agli ambienti cloud.

TEMPO DI RILEVAMENTO

Abbiamo poi chiesto se il tempo necessario per rilevare un incidente nel cloud è cambiato rispetto ai 12 mesi precedenti. Più di un terzo degli intervistati (35%) ha affermato che il rilevamento è ora più veloce, mentre il 49% ha affermato che il tempo di rilevamento non è cambiato.

Cosa è cambiato nei tempi di rilevamento dell'incidente



Per approfondire, abbiamo chiesto agli intervistati quanto tempo hanno impiegato per individuare e rispondere agli incidenti di sicurezza del cloud che hanno subito negli ultimi 12 mesi. Il grafico seguente confronta questi risultati con i dati del 2020 per mostrare quali tipi di attacchi sono diventati più facili da scoprire.

RANSOMWARE O ALTRI ATTACCHI MALWARE

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	35%	35%
ORE	51%	39%
GIORNI	9%	19%
SETTIMANE	5%	3%
MESI E OLTRE	0%	5%

PHISHING

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	44%	42%
ORE	42%	40%
GIORNI	13%	12%
SETTIMANE	1%	3%
MESI E OLTRE	0%	3%

ATTACCHI MIRATI ALL'INFRASTRUTTURA CLOUD

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	32%	31%
ORE	51%	42%
GIORNI	15%	17%
SETTIMANE	2%	4%
MESI E OLTRE	0%	6%

PERDITA DI DATI

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	23%	25%
ORE	42%	36%
GIORNI	29%	24%
SETTIMANE	6%	9%
MESI E OLTRE	0%	6%

PERDITA ACCIDENTALE DI DATI

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	16%	22%
ORE	23%	31%
GIORNI	47%	28%
SETTIMANE	14%	12%
MESI E OLTRE	0%	7%

FURTO DI DATI DA PARTE DI INSIDER

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	23%	20%
ORE	27%	26%
GIORNI	27%	28%
SETTIMANE	19%	14%
MESI E OLTRE	4%	12%

FURTO DI DATI DA PARTE DI HACKER

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	16%	23%
ORE	53%	30%
GIORNI	21%	26%
SETTIMANE	0%	12%
MESI E OLTRE	10%	9%

COMPROMISSIONE DELLA SUPPLY CHAIN

TEMPI DI RILEVAMENTO	2020	2022
MINUTI	23%	20%
ORE	53%	27%
GIORNI	18%	30%
SETTIMANE	0%	12%
MESI E OLTRE	6%	10%

COMPROMISSIONE DELL'ACCOUNT

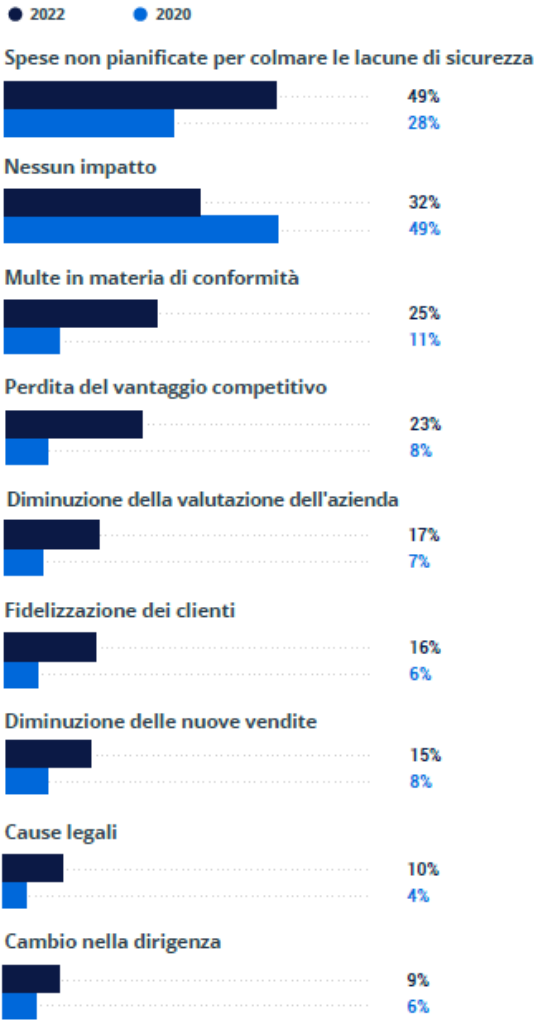
TEMPI DI RILEVAMENTO	2020	2022
MINUTI	20%	30%
ORE	49%	36%
GIORNI	24%	23%
SETTIMANE	7%	6%
MESI E OLTRE	0%	5%

In risposta alla domanda precedente, l'84% degli intervistati ha affermato che il tempo medio necessario per rilevare l'incidente non è cambiato o si è ridotto, ma questo approfondimento rivela che il tempo medio di rilevamento per la maggior parte dei tipi di attacchi è effettivamente aumentato dal 2020. I rallentamenti più significativi possono essere osservati in merito all'individuazione di compromissioni della catena di approvvigionamento ed agli attacchi ransomware.
Inoltre, nel 2020, solo tre tipi di attacchi hanno richiesto più tempo per essere individuati; nel 2022, invece, ogni tipo di attacco ha richiesto molto più tempo per essere individuato, richiedendo a volte mesi. Tuttavia, notiamo che ci sono stati dei progressi per i diversi tipi di attacco.
Il 53% degli intervistati è riuscito a rilevare la perdita accidentale di dati in pochi minuti o un paio d'ore, contro solo il 39% nel 2020. Inoltre, il numero degli intervistati che ha scoperto la compromissione dell'account in pochi minuti è aumentato dal 20% nel 2020 al 30% nel 2022.

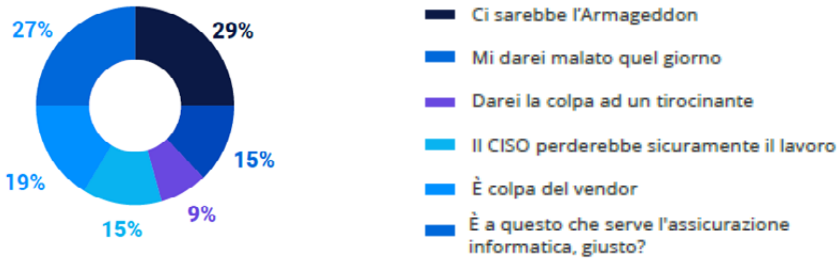
LE CONSEGUENZE DI UNA VIOLAZIONE DATI

Non tutti gli attacchi sono catastrofici. La verità è che nel 32% dei casi l'attacco non ha alcun impatto sul business. Tuttavia, si tratta di un calo significativo rispetto al 49% del 2020.

Conseguenze di una violazione dati



I nostri intervistati prendono molto sul serio le proprie responsabilità; quindi, abbiamo aggiunto un po' di leggerezza al sondaggio di quest'anno solo per alleviare momentaneamente la pressione. Abbiamo quindi chiesto quanto potrebbe essere devastante la violazione laddove si verificasse nel loro archivio dati cloud.

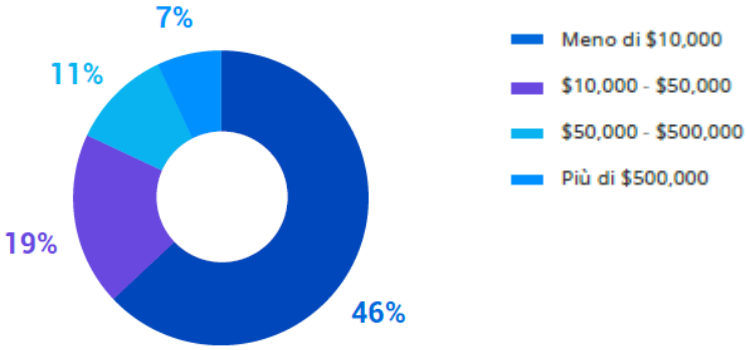


I professionisti IT non sono estranei a una bella risata. Un intervistato ha commentato: "Quali potrebbero essere le conseguenze di una violazione dati? Alcuni servizi non funzionerebbero, quindi un'ottima occasione per andare in spiaggia a prendere un po' di sole e rilassarmi". Ammiriamo la capacità dei professionisti della sicurezza di mantenere la calma (e il senso dell'umorismo) in qualsiasi circostanza.

QUANTO COSTA UNA VIOLAZIONE?

Considerando che il 32% non ha riscontrato alcun impatto sulla propria attività dagli incidenti subiti, non sorprende che la maggior parte degli intervistati (63%) abbia stimato il danno derivante da una violazione dei dati a meno di $ 10.000.

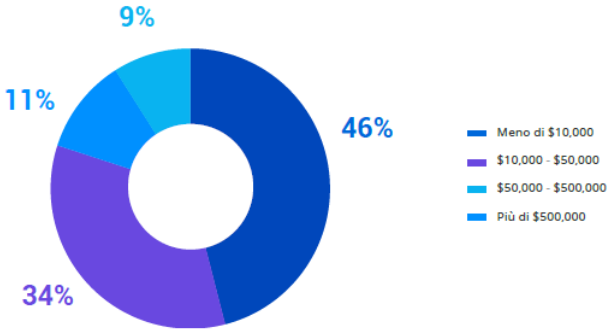
Stima del danno finanziario causato dalle minacce informatiche



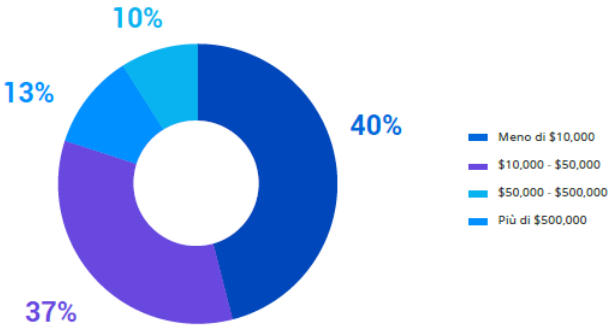
Tuttavia, nelle organizzazioni di grandi dimensioni (con oltre 1.000 dipendenti), è più probabile che le violazioni dei dati abbiano conseguenze costose. Mentre la maggior parte degli intervistati in questo gruppo (46%) stima ancora il danno a meno di $ 10.000, il 34% ha affermato che gli è costato $ 50.000– $ 500.000. Tra il pool complessivo di intervistati, solo il 19% ha stimato che il danno fosse così elevato.

Allo stesso modo, la percentuale degli intervistati che stima il danno a più di $ 500.000 è la più alta nelle grandi aziende (oltre 10.000 dipendenti): il 13% contro il 7% complessivo. In breve, più grande è un'organizzazione, più è probabile che le conseguenze della violazione dei dati siano costose.

Grande (oltre 1.000 dipendenti)



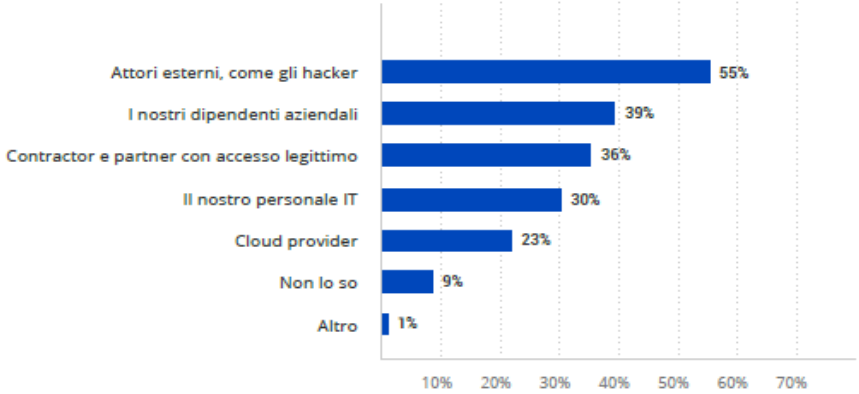
Molto Grande (oltre 10.000+ dipendenti)



MISURE DI SICUREZZA DEL CLOUD

Prima di approfondire le misure di sicurezza implementate dalle organizzazioni per mantenere i propri dati al sicuro, abbiamo chiesto cosa li preoccupa maggiormente. Più della metà (55%) degli intervistati ha affermato che gli attori esterni sono la principale minaccia per il proprio ambiente IT, seguiti dai propri dipendenti (39%) che potrebbero creare inavvertitamente falle nella sicurezza, nonché da contractor e partner che richiedono un accesso (36%).

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



Abbiamo poi chiesto quali siano le misure adottate dai nostri intervistati per proteggere i propri dati nel cloud ed abbiamo poi confrontato le loro risposte con quelle del nostro precedente report.
Nel 2020, i controlli di sicurezza cloud più comuni segnalati dalle organizzazioni sono stati la crittografia (62%), il controllo dell'attività degli utenti (58%) e la formazione dei dipendenti (58%). Nel 2022, la percentuale di intervistati che utilizza tali misure è esattamente la stessa.
Nell'attuale sondaggio, l'autenticazione a più fattori ed il backup su cloud sono in cima all'elenco delle misure di protezione. Entrambi hanno registrato aumenti dal 2020: l'adozione di MFA è passata dal 57% al 69% ed i backup sono aumentati dal 58% al 63%.

Pensi di adottare delle misure per proteggere i tuoi dati nel cloud?

	Non farà nulla	Ha in piano di farlo	Fa già
Autenticazione a più fattori	7%	24%	69%
Backup su cloud	7%	30%	63%
Crittografia	9%	29%	62%
Corsi di formazione dei dipendenti	7%	34%	59%
Controllo dell'attività dell'utente	7%	35%	58%
Revisione dei diritti di accesso (attestazione)	8%	37%	55%
Classificazione dei dati	17%	46%	37%
Rimozione dei file sensibili dal cloud	29%	37%	34%
Broker di sicurezza per l'accesso al cloud	30%	46%	24%

Il **99%** dei CIO sta già conducendo corsi di formazione sulla sicurezza dei dipendenti o prevede di farlo.

Il **70%** dei CISO controlla l'attività degli utenti nel cloud ed il 28% prevede di iniziare a farlo.

Solo il **5%** dei CISO non classifica i dati nel cloud e non prevede di farlo.

MISURE PER LA PROTEZIONE DEI DATI NEL CLOUD IN BASE ALLA DIMENSIONE DELL'ORGANIZZAZIONE

Grande (oltre 1.000 dipendenti)

	Non farà nulla	Ha in piano di farlo	Fa già
Autenticazione a più fattori	5%	20%	75%
Backup su cloud	4%	28%	68%
Crittografia	7%	26%	67%
Corsi di formazione dei dipendenti	5%	30%	65%
Controllo dell'attività dell'utente	5%	31%	64%
Revisione dei diritti di accesso (attestazione)	6%	34%	60%
Classificazione dei dati	9%	44%	47%
Rimozione dei file sensibili dal cloud	18%	38%	44%
Broker di sicurezza per l'accesso al cloud	20%	42%	38%

Il **95%** delle grandi aziende controlla l'attività degli utenti nel cloud o prevede di farlo. Il backup su cloud è la misura di protezione più comunemente utilizzata tra le grandi organizzazioni; solo il 5% di loro non utilizza già o prevede di utilizzare questa opzione.

Medio (101-1.000 dipendenti)

	Non farà nulla	Ha in piano di farlo	Fa già
Autenticazione a più fattori	7%	28%	65%
Backup su cloud	7%	31%	62%
Crittografia	6%	35%	59%
Corsi di formazione dei dipendenti	7%	38%	55%
Controllo dell'attività dell'utente	5%	43%	52%
Revisione dei diritti di accesso (attestazione)	8%	43%	49%
Classificazione dei dati	17%	54%	28%

Rimozione dei file sensibili dal cloud	33%	43%	24%
Broker di sicurezza per l'accesso al cloud	32%	51%	17%

Piccolo (1-100 dipendenti)

	Non farà nulla	Ha in piano di farlo	Fa già
Autenticazione a più fattori	9%	26%	65%
Backup su cloud	9%	28%	63%
Crittografia	12%	32%	56%
Corsi di formazione dei dipendenti	11%	34%	55%
Controllo dell'attività dell'utente	12%	34%	54%
Revisione dei diritti di accesso (attestazione)	11%	36%	53%
Classificazione dei dati	26%	40%	34%
Rimozione dei file sensibili dal cloud	39%	30%	31%
Broker di sicurezza per l'accesso al cloud	40%	45%	15%

UNCLOUDING

Il modo più risoluto per proteggere i dati nel cloud è quello di rimuoverli dal cloud. Nel 2019, il 48% degli intervistati aveva già adottato o pianificava di spostare nuovamente i dati sensibili in locale. Nel 2020, nonostante l'aumento dell'adozione del cloud, dovuto alla necessità di supportare il lavoro da remoto, questa cifra è salita al 62%. Nel 2022 è cresciuto al 66%.

Il **66%** **delle organizzazioni ha già rimosso i dati sensibili dal cloud o prevede di farlo**

L'impatto delle misure di sicurezza sul tempo di rilevamento

La classificazione dei dati consente alle organizzazioni di contrassegnare i file sensibili in modo da poter migliorare il controllo sull'archiviazione dei dati, ove essi risiedano e su chi possa accedervi. Questa tecnologia ha notevolmente migliorato la velocità di rilevamento per tutti i tipi di incidenti: la maggior parte degli intervistati che classificano i propri dati è stata in grado di rilevare un attacco in pochi minuti, mentre coloro che non classificano i dati di solito hanno bisogno di ore o addirittura giorni.

L'impatto della classificazione dei dati sulla velocità di rilevazione degli incidenti

	CLASSIFICA I DATI	NON CLASSIFICA I DATI
Phishing	48% l'ha rilevato in pochi minuti	41% l'ha rilevato in poche ore
Ransomware o altri attacchi di malware	46% l'ha rilevato in pochi minuti	42% l'ha rilevato in poche ore
Attacchi mirati all'infrastruttura cloud	44% l'ha rilevato in pochi minuti	46% l'ha rilevato in poche ore
Compromissione dell'account	39% l'ha rilevato in pochi minuti	35% l'ha rilevato in poche ore
Perdita di dati	37% l'ha rilevato in pochi minuti	37% l'ha rilevato in poche ore
Perdita accidentale di dati	32% l'ha rilevato in pochi minuti	31% l'ha rilevato in poche ore
Furto di dati da parte di hacker	32% l'ha rilevato in pochi minuti	31% l'ha rilevato in poche ore
Furto di dati da parte di addetti ai lavori	29% l'ha rilevato in pochi minuti	30% l'ha rilevato in pochi giorni
Compromissione della supply chain	29% l'ha rilevato in pochi minuti	29% l'ha rilevato in poche ore

L'impatto dell'audit sull'attività degli utenti e sulla velocità di rilevamento degli incidenti

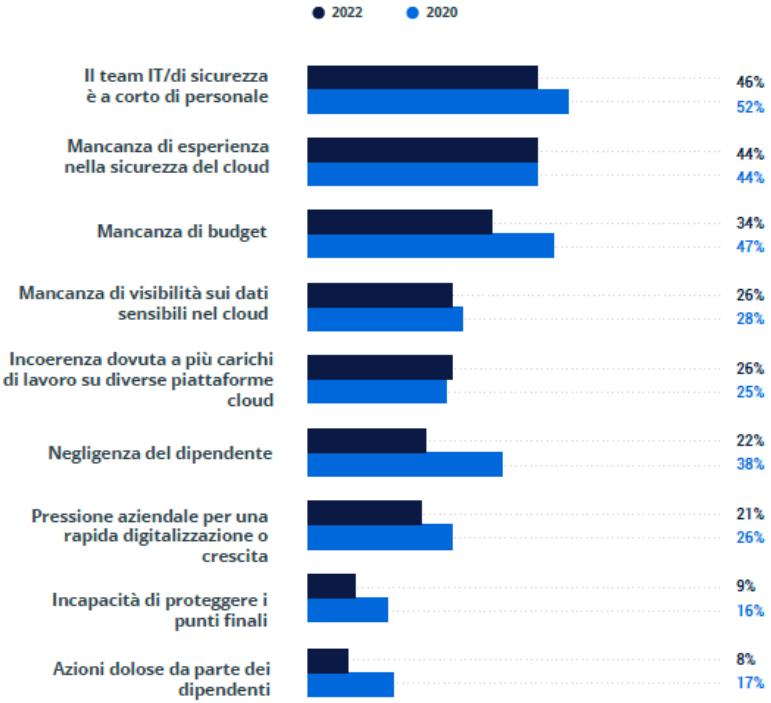
Il controllo dell'attività degli utenti si è rivelato un ottimo modo per migliorare la velocità di rilevamento degli incidenti. È stato particolarmente efficace per il phishing, gli attacchi ransomware e la compromissione degli account, dove ha ridotto i tempi di rilevamento da ore a minuti.

	VERIFICA L'ATTIVITÀ DELL'UTENTE	NON CONTROLLA L'ATTIVITÀ DELL'UTENTE
Phishing	49% l'ha rilevato in pochi minuti	45% l'ha rilevato in poche ore
Ransomware o altri attacchi di malware	41% l'ha rilevato in pochi minuti	43% l'ha rilevato in poche ore
Attacchi mirati all'infrastruttura cloud	35% l'ha rilevato in pochi minuti	35% l'ha rilevato in poche ore
Compromissione dell'account	36% l'ha rilevato in pochi minuti	23% l'ha rilevato in pochi minuti

Perdita di dati	30% l'ha rilevato in pochi minuti	18% l'ha rilevato in pochi minuti
Perdita accidentale di dati	26% l'ha rilevato in pochi minuti	17% l'ha rilevato in pochi minuti
Furto di dati da parte di hacker	26% l'ha rilevato in pochi minuti	17% l'ha rilevato in pochi minuti
Furto di dati da parte di addetti ai lavori	23% l'ha rilevato in pochi minuti	15% l'ha rilevato in pochi minuti
Compromissione della supply chain	23% l'ha rilevato in pochi minuti	26% l'ha rilevato in pochi minuti

Le sfide della sicurezza del cloud

Le 3 principali sfide per la sicurezza dei dati citate dagli intervistati sono rimaste le stesse del 2020: mancanza di personale IT, mancanza di esperienza negli ambienti cloud e mancanza di budget.



Nel 2020, il 48% dei CISO ha notato che il desiderio di crescita dell'azienda si scontri con quello degli sforzi per garantire la sicurezza dei dati nel cloud. Ora, questo problema è stato segnalato solo dal 20% dei CIO e dal 23% dei CISO.

Budget

Nel 2020, le organizzazioni hanno destinato il 27% del proprio budget totale allocato per la sicurezza informatica alla sicurezza nel cloud. Nel 2022 questa quota è salita al 32% complessivamente ed al 36% tra le grandi aziende (oltre 1.000 dipendenti).

Con il 54% dei carichi di lavoro che dovrebbero essere nel cloud entro il 2023, i budget per la sicurezza stanno crescendo. Il 49% dei nostri intervistati afferma che il proprio budget per la sicurezza nel cloud è aumentato nel 2022.

Nel **56%** delle grandi organizzazioni (oltre 1.000 dipendenti), il budget per la sicurezza del cloud è aumentato nel 2022.

"La quota crescente di denaro speso per la sicurezza del cloud all'interno del budget complessivo per la sicurezza mostra la crescente importanza dell'infrastruttura cloud all'interno degli ambienti IT delle organizzazioni. Man mano che la percentuale di budget per il cloud aumentava, qualcos'altro doveva diminuire poiché la sicurezza del cloud diventava una priorità più alta. Questo sarà un atto di bilanciamento cruciale per la maggior parte delle organizzazioni nei prossimi anni ", ha affermato Dirk Schrader, VP of Security Research presso Netwrix.), il budget per la sicurezza del cloud è aumentato nel 2022.

Parte del budget per la sicurezza informatica assegnata alla sicurezza del cloud (numero medio)

Dati sulle organizzazioni italiane

73% delle organizzazioni italiane archiviano i dati sensibili nel cloud.

I 3 principali tipi di dati sensibili che le organizzazioni italiane archiviano nel cloud

Informazioni di identificazione personale (PII) dei dipendenti	47%
Informazioni di identificazione personale (PII) dei clienti	33%
Informazioni finanziarie aziendali	27%

Quant'è la percentuale dei tuoi carichi di lavoro che si trova nel cloud oggi?

37%

Quant'è la percentuale dei tuoi carichi di lavoro che è pianificata per passare nel cloud tra 12-18 mesi?

51%

I 3 principali obiettivi di adozione del cloud in Italia

Ridurre i costi	71%
Migliorare la sicurezza	36%
Organizzare l'infrastruttura per i lavoratori remoti	29%

Il **64%** degli intervistati italiani ha definito l'integrazione con l'ambiente IT esistente uno dei fattori principali che rallenta l'adozione del cloud nelle proprie organizzazioni.

Le principali sfide che le organizzazioni italiane devono affrontare mentre cercano di garantire la sicurezza dei dati nel cloud

53%	**Mancanza di esperienza nella sicurezza del cloud**
40%	**Team IT/sicurezza a corto di personale**
33%	**Mancanza di visibilità sui dati sensibili nel cloud**

Il **54%** delle organizzazioni italiane ha subito attacchi informatici alla propria infrastruttura cloud negli ultimi 12 mesi.

Gli incidenti di sicurezza informatica più comuni in Italia

87%	**Phishing**
33%	**Compromissione dell'account**
33%	**Perdita accidentale di dati**

Tempo di rilevamento degli incidenti nel cloud

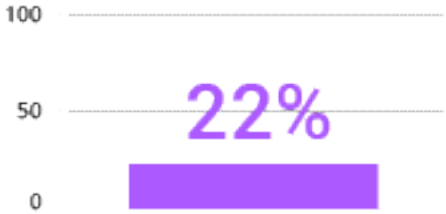
	MINUTI	ORE	GIORNI	SETTIMANE	MESI E MOLTO DI Più
Phishing	38%	31%	23%	8%	0%
Ransomware o altri attacchi di malware	23%	38%	23%	0%	16%
Attacchi mirati all'infrastruttura cloud	15%	38%	38%	0%	9%

Il **46%** delle organizzazioni italiane ha impiegato settimane per rilevare il furto di dati da parte di addetti ai lavori e il 23% ha impiegato mesi e più per rilevare la compromissione della supply chain.

Le 3 principali misure già adottate dalle organizzazioni italiane per proteggere i dati nel cloud

Autenticazione a più fattori	91%
Crittografia	82%
Revisione dei diritti di accesso (attestazione)/ Backup su cloud	77%

Distribuzione del budget per la sicurezza informatica



Il **38%** delle organizzazioni italiane prevede di implementare il controllo dell'attività degli utenti per proteggere meglio i dati nel cloud

A PROPOSITO DI QUESTO REPORT

Il report è stato redatto da Netwrix Research Lab, che conduce sondaggi di settore tra i professionisti IT di tutto il mondo per individuare i principali cambiamenti ed le tendenze di settore. Per ulteriori report, visita www.netwrix.com/go/research

La gestione del rischio cyber nelle grandi organizzazioni italiane

Uno studio dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano

[A cura di Alessandro Piva, Giorgia Dragoni e Nicola Ciani]

Negli ultimi anni, diversi avvenimenti hanno impattato l'intero ecosistema della gestione aziendale del rischio cyber. L'avvento della pandemia, per esempio, ha stravolto le modalità di lavoro, rendendo l'utente un potenziale punto debole sfruttabile dai cybercriminali per accedere alle risorse aziendali, ancora più di quanto già lo fosse in passato. La proliferazione di nuove tecnologie digitali, sia in ambito business sia in ambito consumer, ha generato un'estensione della superficie d'attacco. Anche la sicurezza della supply chain ha assunto una crescente rilevanza: gli attori lungo la filiera sono sempre più interconnessi e può essere più semplice per un aggressore accedere alla rete di un'azienda tramite un attacco alle sue terze parti. Infine, il conflitto russo-ucraino e le turbolenze geopolitiche hanno contribuito ad intensificare ulteriormente la componente di minaccia dolosa da cui le organizzazioni devono proteggersi.
Tale scenario coinvolge anche realtà aziendali poco mature, soprattutto per quanto riguarda la conoscenza e l'attenzione prestata a questo genere di rischi. Negli anni le disposizioni normative ed extra-normative hanno sopperito parzialmente alla carenza culturale delle organizzazioni, suggerendo o imponendo l'introduzione di sistemi di sicurezza, processi e tecnologie col fine di evitare il verificarsi di incidenti con potenziali ripercussioni anche a livello sociale.

Negli ultimi anni, anche grazie a una forte attenzione mediatica, si è assistito a una progressiva presa di consapevolezza da parte delle aziende, con un aumento della centralità della sicurezza informatica. Il rischio cyber, nella sua concezione tradizionale di minaccia ai sistemi informativi, non ha mutato nella manifestazione, quanto nella frequenza con cui colpisce e nella gravità degli effetti prodotti. La nuova immagine che le imprese hanno del rischio cyber, come un rischio operativo a tutti gli effetti, è probabilmente legata al fatto che è diventato evidente che tali rischi hanno un impatto concreto sulle performance e sulla reputazione aziendale. Il rischio cyber non è più percepito come una minaccia che si manifesta in un mero problema tecnico dell'infrastruttura aziendale, quanto come un pericolo che può avere impatto sugli azionisti e sugli investitori, sui partner commerciali e sui fornitori, sui dipendenti e sui clienti.

L'Osservatorio Cybersecurity & Data Protection, da 8 edizioni, si pone l'obiettivo di monitorare la maturità delle grandi organizzazioni, appartenenti a settori pubblici e privati, nell'approccio alla gestione del rischio cyber. La Ricerca 2022, di cui verranno illustrati i risultati nel presente capitolo, ha coinvolto 112 CISO, CSO, CIO, Compliance Manager,

Risk Manager, Chief Risk Officer e DPO appartenenti a grandi organizzazioni (250+ addetti) operanti in Italia.

La gestione del rischio cyber

L'evoluzione dello scenario si ripercuote anche sul processo di gestione del rischio cyber, nella sua connotazione e nelle attività che lo compongono. L'obiettivo tradizionale, riconducibile all'Information Security, era quello di garantire la Riservatezza, l'Integrità e la Disponibilità delle informazioni aziendali. Ripercorrendo l'ISO 27032, utile per indagare la relazione tra la cybersecurity e altri domini della security, si realizza come questo approccio sia però lontano dalla complessità dello scenario descritto in precedenza: l'attenzione dei processi di gestione del rischio si sta concentrando sempre di più verso la difesa del sistema informatico da attacchi cyber.

La gestione del rischio cyber prevede di identificare e monitorare i possibili scenari di rischio, valutarne i potenziali impatti e introdurre opportune azioni di mitigazione. Questo processo ha l'obiettivo di indirizzare le scelte strategiche, gli investimenti e le attività day-by-day nel contrasto alle minacce esterne.

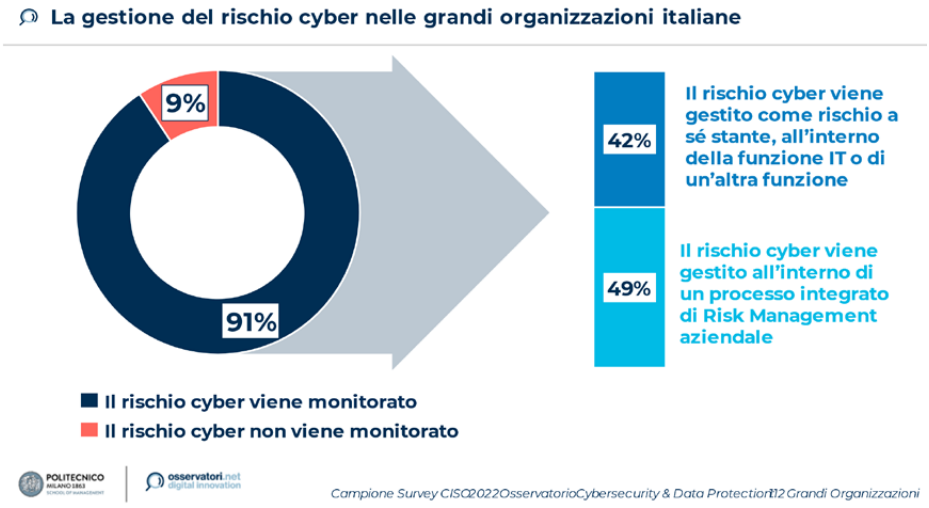


Figura 1: *La gestione del rischio cyber nelle grandi organizzazioni italiane – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

La fig. 1 aiuta a comprendere l'approccio alla gestione della materia nelle grandi organizzazioni: nel 2022, circa il 91% ha strutturato processi di monitoraggio del rischio cyber. Nonostante la percentuale sia sufficientemente alta da lasciare un messaggio positivo, è

importante evidenziare come permanga un 9% di organizzazioni di grandi dimensioni che trascura il problema, non monitorando il rischio cyber.
Indagando più in profondità, si evince come solo il 49% delle aziende abbia introdotto un approccio in cui il cyber risk viene gestito all'interno di un processo integrato di risk management aziendale, mentre la restante popolazione aziendale si limita a valutarlo come un rischio a sé stante, con attività attuate all'interno dell'IT o di un'altra funzione singola.
I risultati della Ricerca non indicano una particolare crescita della maturità, che anzi, vive un momento di stagnazione ormai da diversi anni. La necessità di riadattare processi strutturati sulla base dell'evoluzione dello scenario risulta quindi poco sentita dalle organizzazioni, che stentano a mettere a frutto la rivisitazione e innovazione del proprio approccio alla gestione del rischio cyber.

L'attività di quantificazione finanziaria del rischio cyber

La relativa bassa attenzione dedicata al tema cyber può essere riconducibile alle difficoltà di comunicazione nei confronti del Top Management della strategicità della materia. L'output degli assessment condotti in azienda, soprattutto se implementati all'interno della funzione IT con un taglio molto tecnico, difficilmente risulta comprensibile al business e al management. L'operatività del rischio impone però che tutti prendano coscienza della severità delle minacce, in primis i vertici aziendali. Per ridurre il gap tra l'anima tecnica, vicina alla security, e il risk management, può risultare determinante introdurre logiche di valutazione del rischio cyber in termini economico-finanziari: in tal modo, non solo si potrà mettere in luce il reale rischio per l'impresa, ma si potrà anche comprendere l'effettivo valore che l'attività di mitigazione può generare per l'organizzazione.

Tale esigenza non è mai stata così sentita: l'approccio di quantificazione finanziaria del rischio cyber sta vivendo un momento di forte attenzione proprio perché permette di sopperire alla difficoltà di comunicazione tra funzioni tecniche e funzioni di business. Tale attività si colloca, in maniera integrativa, all'interno della fase di valutazione del rischio: la costruzione di modelli di stima della probabilità si interfaccia con la quantificazione dei potenziali impatti di eventi di sicurezza in termini finanziari. Il fine ultimo, quindi, è la produzione di metriche di rischio finanziario, come il valore a rischio o la perdita attesa, ma anche indicatori che provano a misurare l'efficacia e l'efficienza delle scelte di sicurezza.

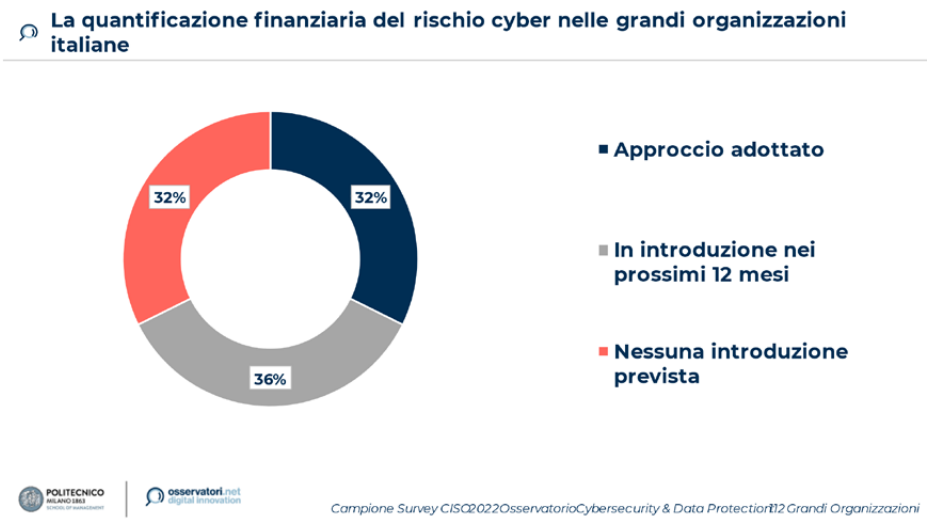


Figura 2: *La quantificazione finanziaria del rischio cyber nelle grandi organizzazioni italiane – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

La crescita dell'interesse delle grandi organizzazioni su questo fronte è testimoniata dall'impennata del numero di aziende che hanno adottato questo approccio tra il 2021 e il 2022: nell'ultimo anno si stima che il 32% delle realtà abbia integrato il processo di assessment con valutazioni di natura finanziaria, quota che supera la stima del 2021 di ben 11 punti percentuali. A ciò, si aggiunge un ulteriore 36% di imprese che dichiara di volersi attivare su questo fronte entro i prossimi 12 mesi.
L'interesse manifestato, quindi, sembra surclassare le possibili criticità connesse all'approccio di quantificazione del rischio cyber: la difficoltà di precisione delle stime, in termini di probabilità e impatto, e la necessità di aggiornarle periodicamente non risultano una barriera nel raggiungimento dei benefici prefissati. Tale "best practice" supporta la ricerca del commitment, indica potenziali strade percorribili nella copertura del rischio, agevola la scelta degli investimenti. Si pensi ad esempio all'introduzione di polizze di trasferimento del rischio: questa via è percorribile nel caso in cui il rischio trasferito sia effettivamente inferiore al premio pagato. Ad oggi è richiesta ancora molta pratica nell'affinamento dell'analisi, ma la percezione è che negli anni a venire questa soluzione possa diffondersi sempre di più.

Framework e approcci per la valutazione del rischio

La valutazione finanziaria del rischio cyber è una prassi complessa, in un contesto estremamente tecnico. È quindi ragionevole dedurre che l'introduzione possa avvenire in un'organizzazione già incline alla gestione del rischio: l'adozione di un framework di Information Security Risk Management, che includa le attività di identificazione, stima e valutazione del rischio, permette di abbracciare in maniera strutturale un approccio completo ed è certamente consigliabile. La distorsione della sua funzionalità, ossia una mera quantificazione finanziaria, rischierebbe di distogliere lo sguardo dalla reale necessità

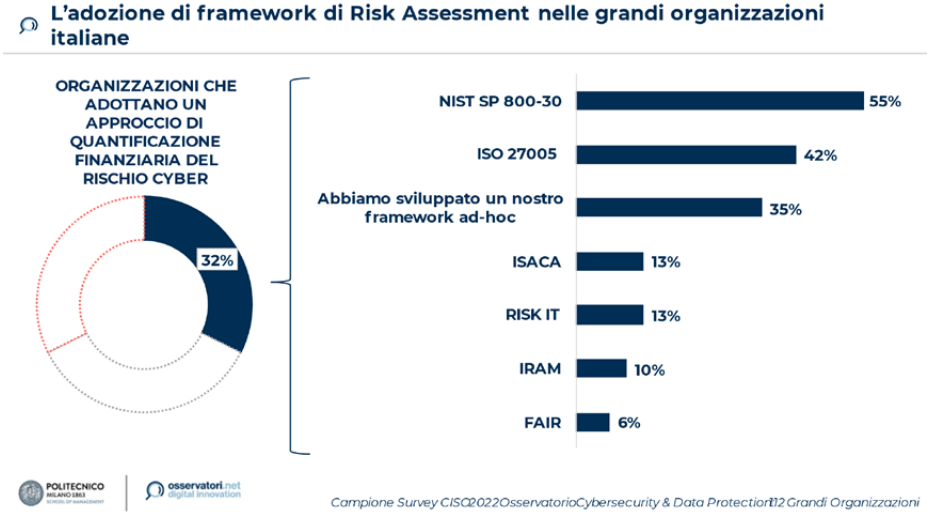


Figura 3: *L'adozione di framework di Risk Assessment nelle grandi organizzazioni italiane – Fonte: Osservatorio Cybersecurity & Data Protection, School of Management – Politecnico di Milano*

Tra le aziende che hanno introdotto la quantificazione del rischio cyber, oltre 1 su 2 ha dichiarato di applicare o aver applicato la metodologia NIST SP 800-30, disegnata per supportare le aziende di grandi dimensioni nel processo di risk management. Al secondo posto si posiziona la ISO27005, framework menzionabile per la sua completezza nelle diverse fasi. Chiude invece ultimo il FAIR (Factor Analysis of Information Risk), metodologia forte nell'attività di quantificazione del rischio cyber.

Da questa classifica, tuttavia, emerge un messaggio chiaro: un terzo delle grandi organizzazioni ha sviluppato un proprio framework, o eventualmente, ne ha riadattato uno esistente rispetto alle proprie esigenze. Questo messaggio conferma, una volta di più, che il rischio cyber assume connotati spesso diversi e richiede una gestione customizzata secondo il contesto aziendale di riferimento.

La Cybersecurity nelle micro e piccole imprese Una Survey di CNA Milano e dell'Unione Artigiani Milano

Introduzione

Questa ricerca è stata svolta dal CNA Milano e dall'Unione Artigiani Milano insieme al Clusit per ottenere una fotografia attuale della situazione degli iscritti delle due associazioni, relativamente ad alcuni temi di base di cybersecurity.
La ricerca è stata svolta tramite un questionario elaborato da un gruppo di lavoro del Clusit, proposto da CNA Milano e Unione Artigiani Milano ai propri iscritti su base volontaria, e somministrato mediante un sistema informatico messo gratuitamente a disposizione dei cittadini dall'Unione Europea. L'elaborazione dei risultati è del Clusit.
L'analisi si è svolta a cavallo tra il 2022 ed il 2023.
Le aziende rispondenti hanno aderito volontariamente, e pertanto si dovrà scontare un *bias* implicito dovuto all'interesse che ciascun rispondente aveva nei confronti dell'argomento. È ragionevole ipotizzare insomma che il campione riporti risultati in generale migliori della media degli aderenti a CNA ed UA, in altre parole che tutte le migliaia di aziende che non hanno risposto abbiano una situazione in termini di cybersecurity meno buona di quelle che hanno risposto.

Anagrafica delle aziende

Abbiamo collezionato e analizzato un totale di 110 risposte (a febbraio 2023).

Il campione dei rispondenti è composto da aziende perlopiù piccole con meno di 150 dipendenti, ma circa un quinto delle aziende contano un numero di collaboratori superiore ai 500 (**Figura 1**).

Il range di fatturato è molto variegato: il 33% ha un fatturato inferiore a €100.000, mentre in quasi un terzo (27% in totale) è compreso tra €300.000 e €1.000.000.
Il 19% afferma di avere un fatturato compreso tra €100.000 e €300.000 e un ulteriore 19% oltre €1.000.000 (**Figura 2**).

Gestione di IT, Privacy e Cybersecurity

La gestione dell'IT delle aziende rispondenti è affidata prevalentemente a fornitori esterni (34%) o a personale occasionale (19%).
Il personale dedicato che ricopre un ruolo fisso nell'IT all'interno del campione compare solo nel 16% dei casi, mentre nel 18% l'informatica aziendale è gestita da personale parzialmente dedicato (**Figura 3**).

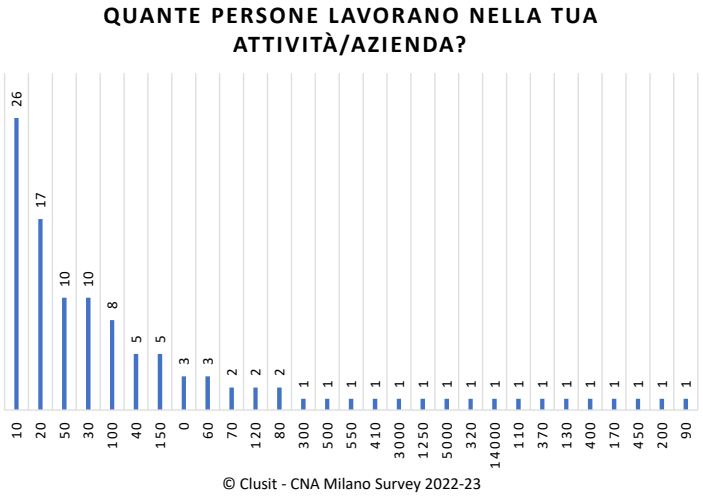


Figura 1: *Composizione delle aziende rispondenti* (© Clusit - CNA Milano Survey 2022-23)

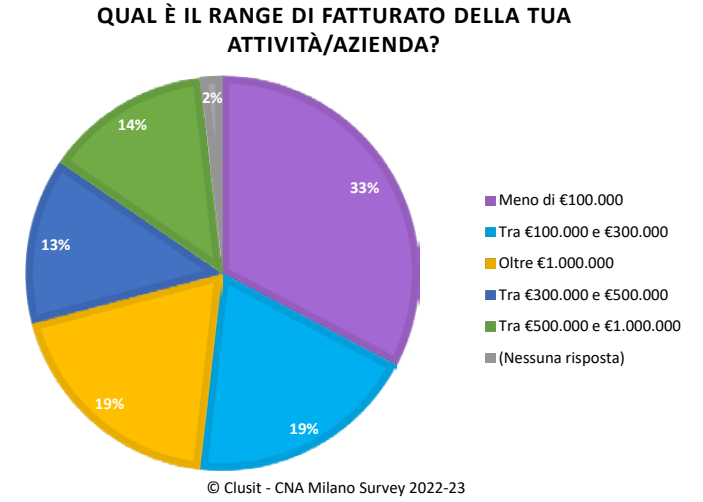


Figura 2: *Range di fatturato delle aziende rispondenti* (© Clusit - CNA Milano Survey 2022-23)

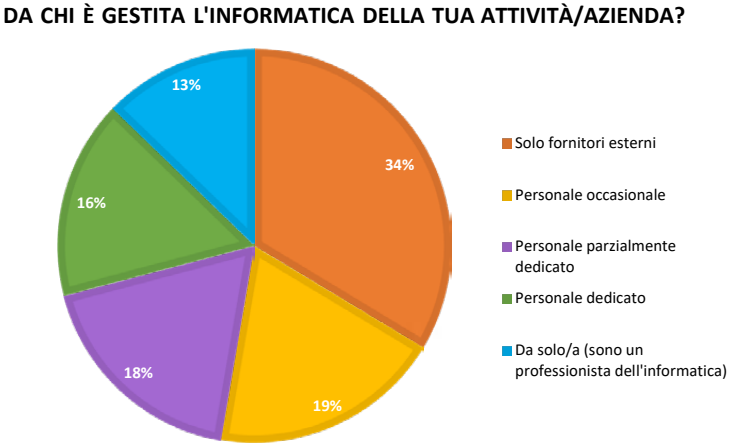


Figura 3: *Gestione IT del campione* (© Clusit - CNA Milano Survey 2022-23)

Nel 44% dei casi non esiste nessun responsabile aziendale in materia di Privacy e Cybersecurity, un dato certamente preoccupante. Ma, se il 17% dispone almeno di un responsabile privacy, solo il 2% gestisce in autonomia le responsabilità in materia di Cybersecurity, informazione che mette in luce quanto ci sia ancora da fare in questo ambito. Sono solo un quarto (25%) le aziende virtuose che dispongono di entrambi i responsabili.

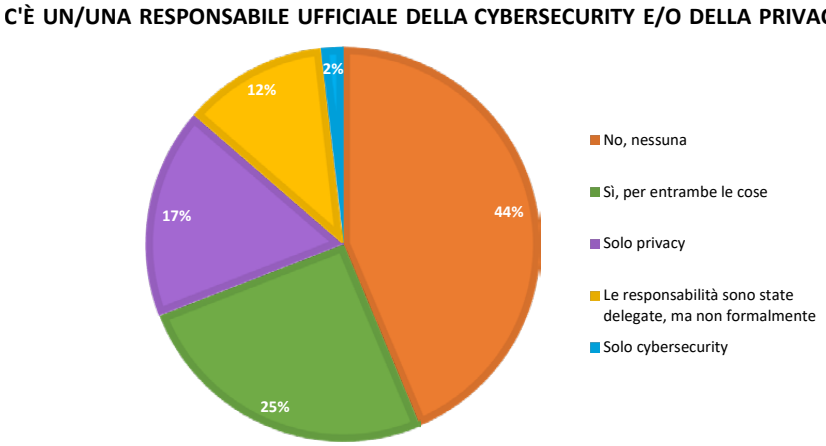


Figura 4: *Responsabilità in materia di Privacy e Cybersecurity*
(© Clusit - CNA Milano Survey 2022-23)

La gestione delle funzioni di Cybersecurity è forse l'aspetto più preoccupante: per oltre due terzi dei rispondenti nessuno è dedicato a questo ambito in azienda. Il restante terzo è suddiviso tra team esterni con un coordinatore aziendale (14%), un team interno con fornitori saltuari (7%) ed un mix di entrambe le soluzioni (13%).

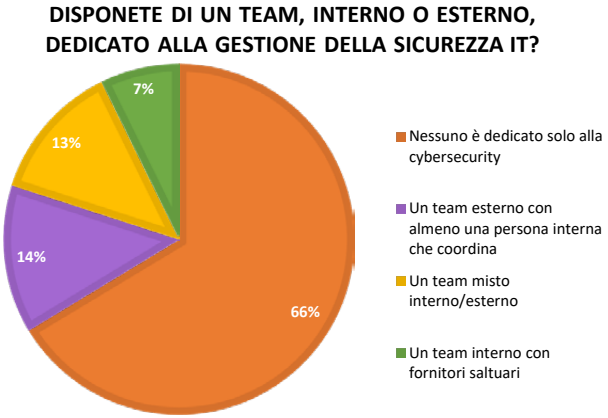


Figura 5: *Gestione della Cybersecurity in azienda* (© Clusit - CNA Milano Survey 2022-23)

La strumentazione informatica non è regolamentata nella metà delle aziende rispondenti, mentre solo il 22% ha definito un regolamento sull'utilizzo di dispositivi.

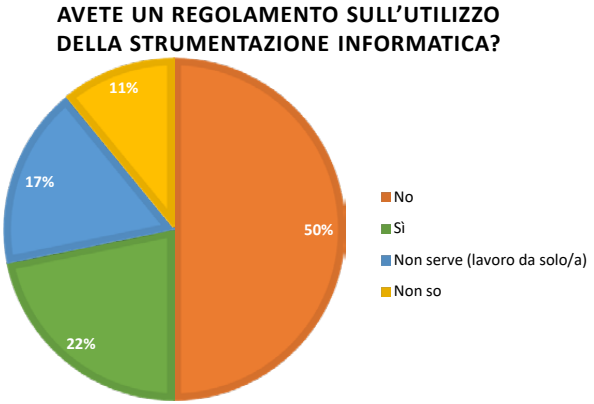


Figura 6: *Regolamentazione della strumentazione informatica*
(© Clusit - CNA Milano Survey 2022-23)

Quando si parla di cyber attacchi, il 72% ritiene di non esserne stato soggetto (o non ne è consapevole). In totale meno di un terzo dei rispondenti ammette di aver subito un attacco.

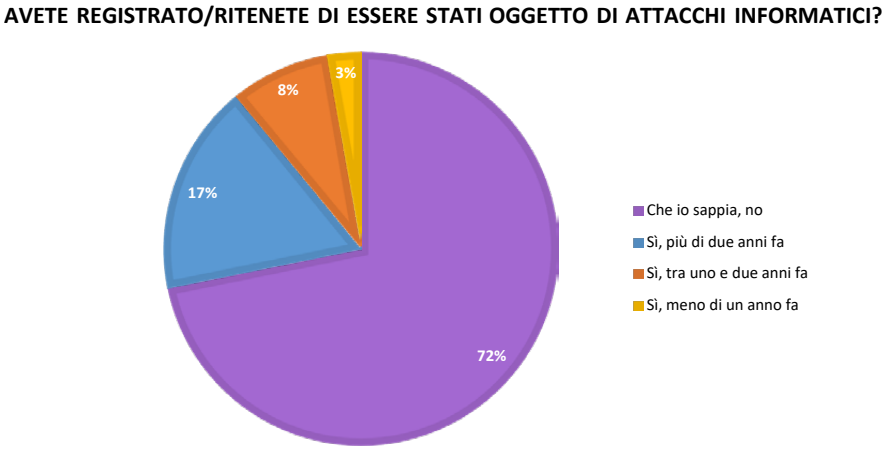


Figura 7: *Cyber attacchi negli anni precedenti* (© Clusit - CNA Milano Survey 2022-23)

Ma in caso di incidenti informatici circa due terzi di rispondenti si affiderebbero a fornitori esterni, mentre solo il 28% dispone di una procedura, scritta (16%) o informale (12%). Preoccupante anche il 12% che non sembra avere ancora riflettuto sul tema.

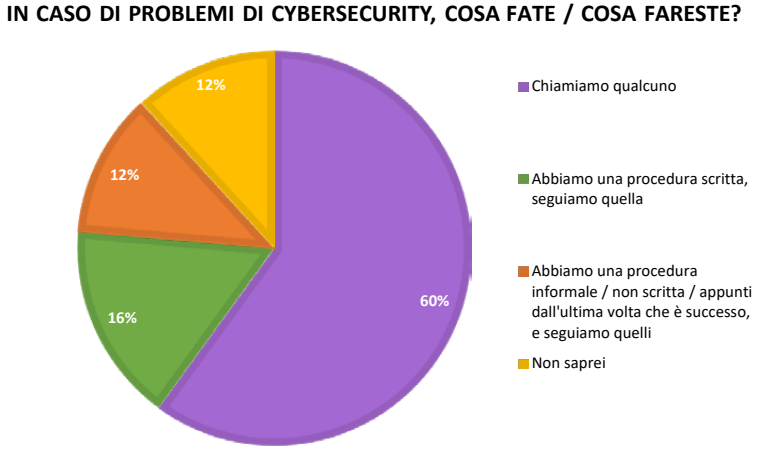


Figura 8: *Procedura in caso di attacchi informatici* (© Clusit - CNA Milano Survey 2022-23)

Quasi la metà (46%) dei rispondenti ha condotto almeno un progetto di adeguamento alla normativa GDPR

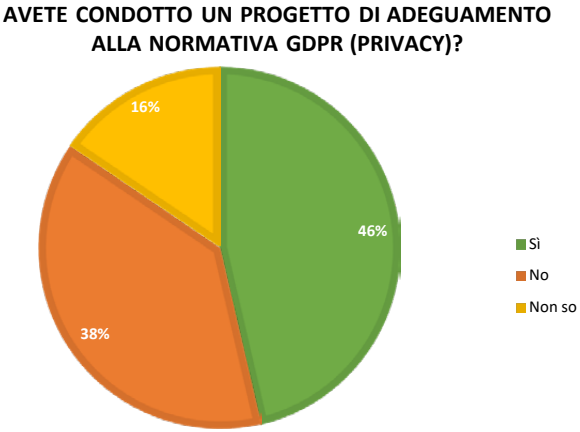


Figura 9: *Adeguamento a GDPR* (© Clusit - CNA Milano Survey 2022-23)

A conferma di ciò, una percentuale simile di aziende rispondenti (44%) dispone di un registro aggiornato per il trattamento dei dati personali.

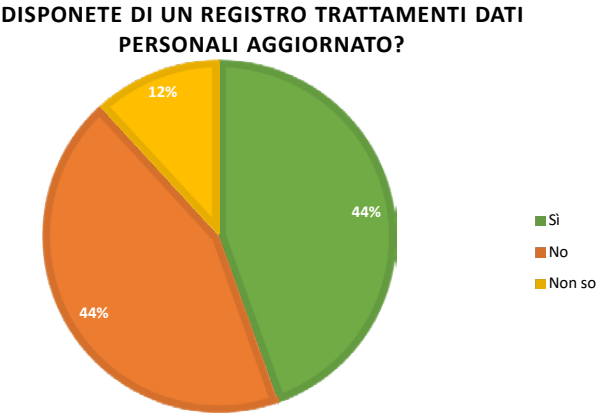


Figura 10: *Registro trattamento dati personali in azienda* (© Clusit - CNA Milano Survey 2022-23)

Apparentemente le questioni inerenti la privacy sembrano in generale ben indirizzate, almeno nella maggior parte delle aziende campione.

Non si può dire la stessa cosa per la Cybersecurity: solo il 21% dispone di una procedura scritta per la gestione di un data breach.

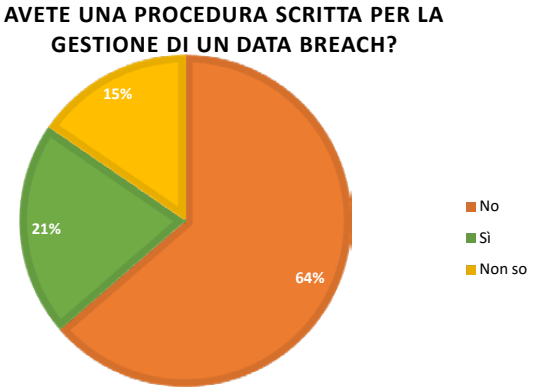


Figura 11: *Procedura scritta per la gestione dei data breach* (© Clusit - CNA Milano Survey 2022-23)

Le risposte inerenti alla formazione in materia di privacy e cybersecurity sono un'ulteriore riprova di quanto si investa ancora poco in questo ambito: solo l'11% delle aziende organizza sessioni di training per il personale che comprendano anche tematiche di Cybersecurity. Un ulteriore 11% organizza formazione in materia di privacy, mentre il 73% non se ne occupa interamente.

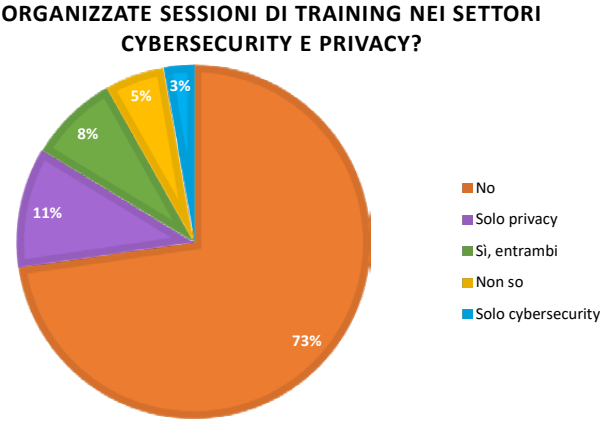


Figura 12: *Formazione in materia di privacy e cybersecurity* (© Clusit - CNA Milano Survey 2022-23)

Policy e procedure sono pubblicate e conosciute da dipendenti e collaboratori solo in un terzo (33%) delle aziende rispondenti.

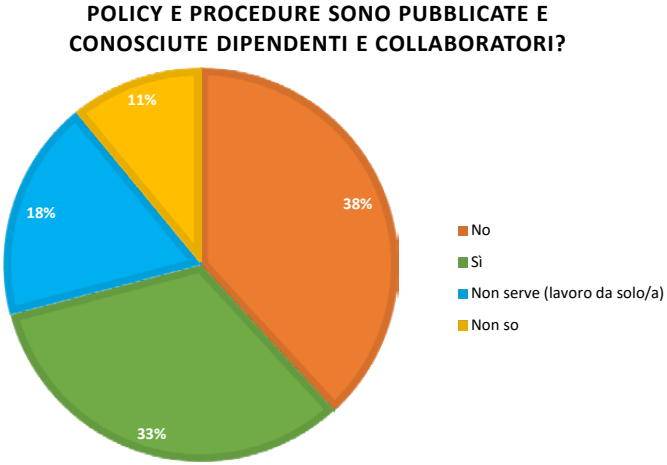


Figura 13: *Pubblicazione in azienda di policy e procedure* (© Clusit - CNA Milano Survey 2022-23)

Il numero di dispositivi informatici utilizzati in azienda è relativamente basso, nella maggior parte dei casi inferiore a 100.

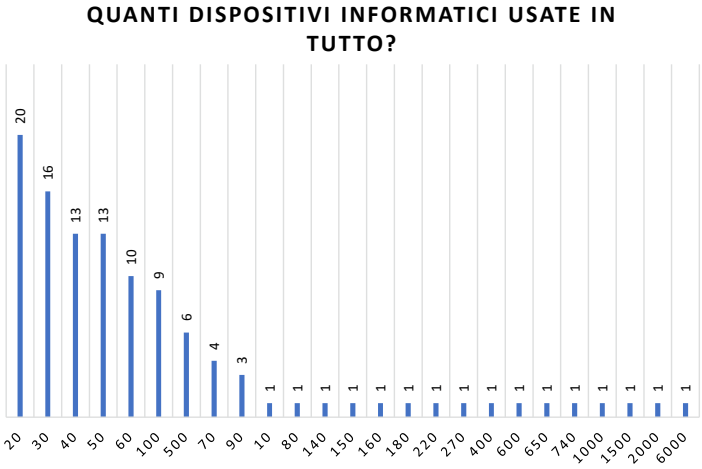


Figura 14: *Dispositivi informatici in azienda* (© Clusit - CNA Milano Survey 2022-23)

In generale (76%) però il collegamento ad Internet dell'azienda è protetto da un firewall. Solo l'11% delle aziende rispondenti non utilizza alcuna protezione.

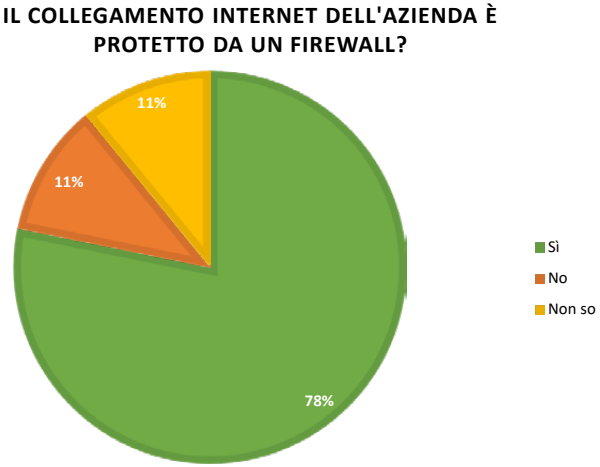


Figura 15: *Protezione da firewall del collegamento internet dell'azienda*
(© Clusit - CNA Milano Survey 2022-23)

In prevalenza l'accesso ai sistemi aziendali dall'esterno non è concesso (47%) o previsto solo eccezionalmente (37%).

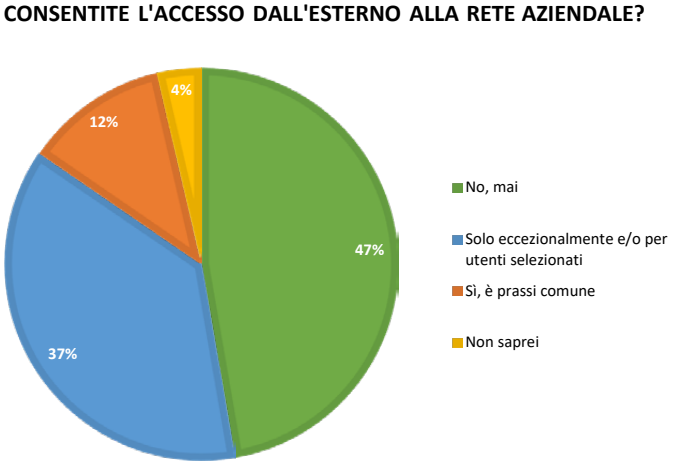


Figura 16: *Accesso dall'esterno ai sistemi aziendali* (© Clusit - CNA Milano Survey 2022-23)

I dispositivi personali sono invece generalmente ben accetti e ne viene concessa la connessione alla rete aziendale come prassi comune (36%) o occasionalmente (32%).

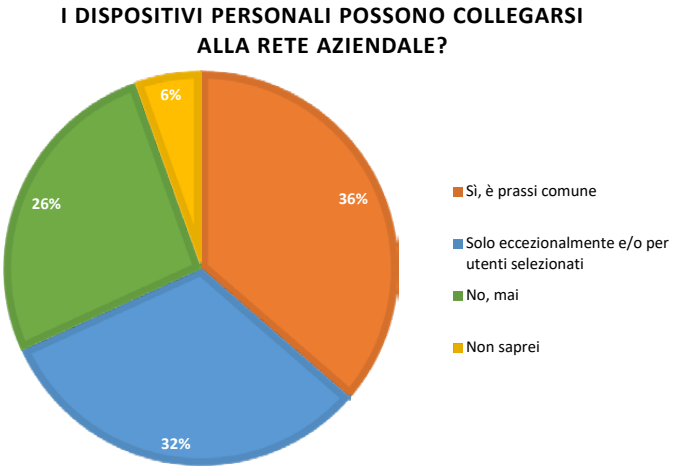


Figura 17: *Gestione in azienda dei dispositivi personali* (© Clusit - CNA Milano Survey 2022-23)

Strumenti e procedure utilizzate

La prevalenza delle aziende rispondenti (69%) dispone di un sito web.

Figura 18: *Sito web aziendale* (© Clusit - CNA Milano Survey 2022-23)

Ma solo il 9% dispone anche di e-commerce

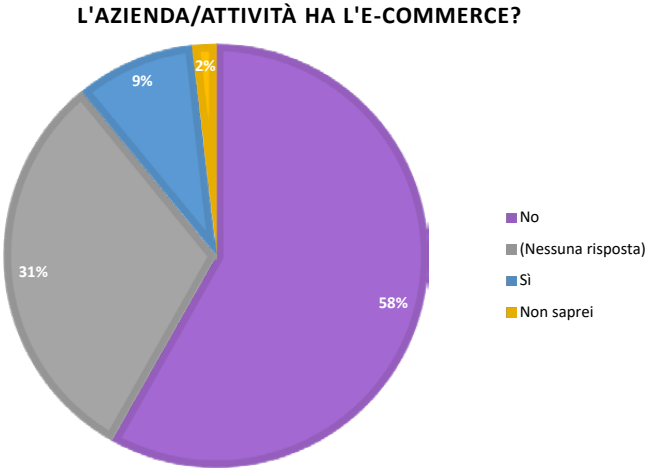


Figura 19: *E-commerce aziendale* (© Clusit - CNA Milano Survey 2022-23)

Per la posta elettronica vengono utilizzate soluzioni variegate, che in prevalenza fanno affidamento su servizi in cloud, business o consumer.

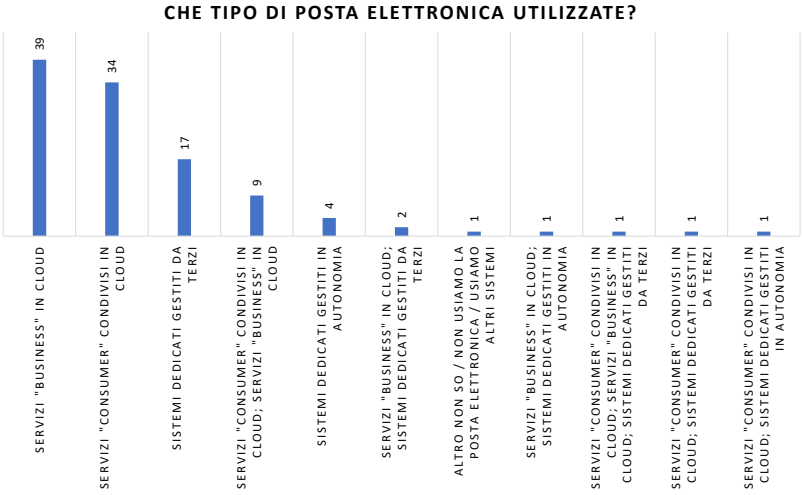


Figura 20: *Sistemi di posta elettronica* (© Clusit - CNA Milano Survey 2022-23)

I computer aziendali sono in generale dotati almeno di soluzioni di backup (anche su cloud) e antivirus.
Solo in pochi adottano soluzioni più avanzate come il disco fisso cifrato o l'assenza di privilegi amministrativi per l'utente.

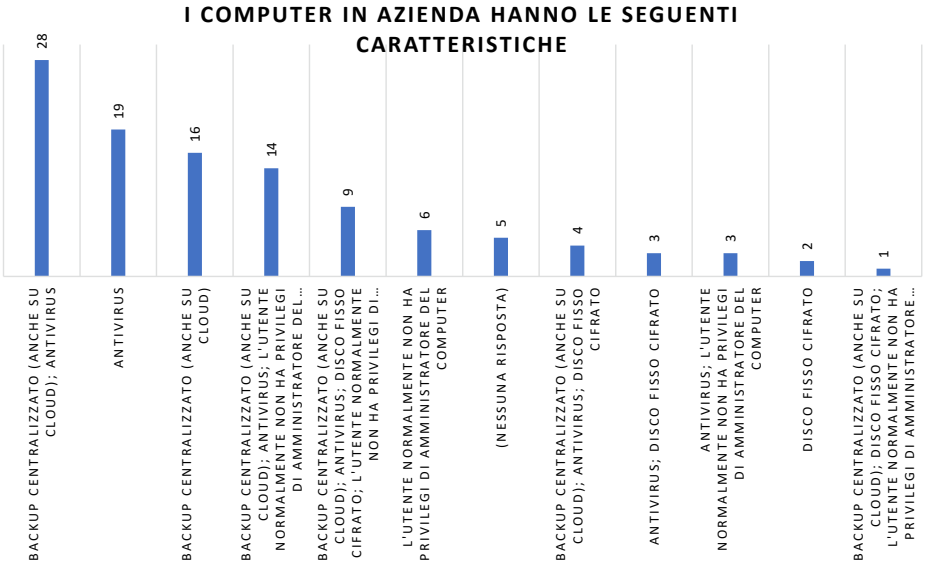


Figura 21: *Sistemi di protezione client* (© Clusit - CNA Milano Survey 2022-23)

La gestione dell'autenticazione è un argomento ancora poco maturo per le aziende rispondenti: la metà del campione utilizza infatti password generiche e solo un terzo password con una scadenza regolare.
L'autenticazione multi-fattore viene utilizzata in una minoranza ancora troppo ristretta di casi (**Figura 22**), dimostrando quanto ci sia ancora molto da fare in questo ambito.

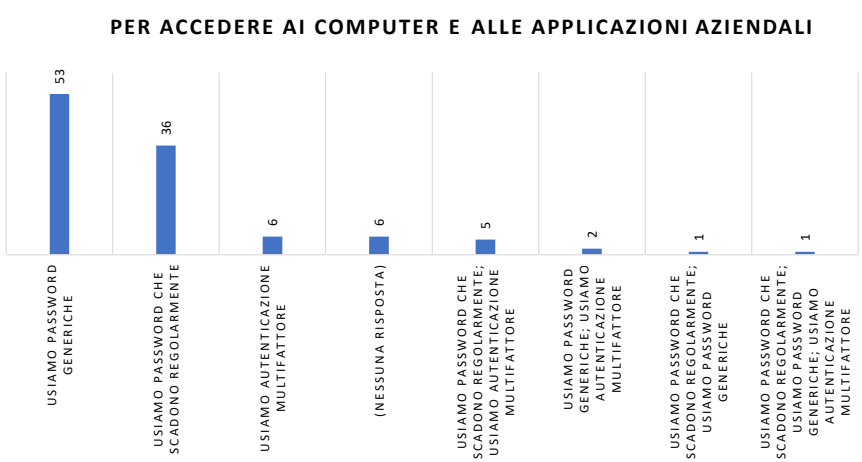


Figura 22: *Tipologia di autenticazione per i dispositivi client* (© Clusit - CNA Milano Survey 2022-23)

Anche le politiche per la gestione dei dispositivi mobili in azienda sono in maggioranza (60%) assenti. Dove le policy sono presenti la gestione può essere automatizzata o manuale. Ma ciò che può fare la differenza è che le politiche di gestione siano ben definite o meno

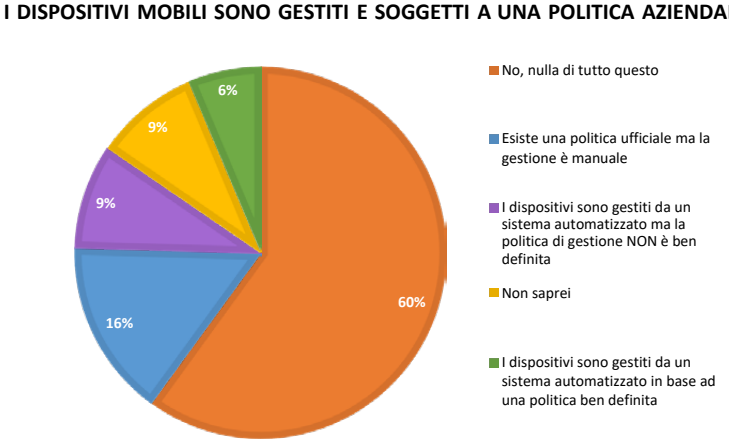


Figura 23: *Politiche per la gestione dei dispositivi mobili in azienda*
(© Clusit - CNA Milano Survey 2022-23)

I servizi di archiviazione di file e documenti sul Cloud sono in generale molto diffusi ma con una predilezione per i sistemi consumer.

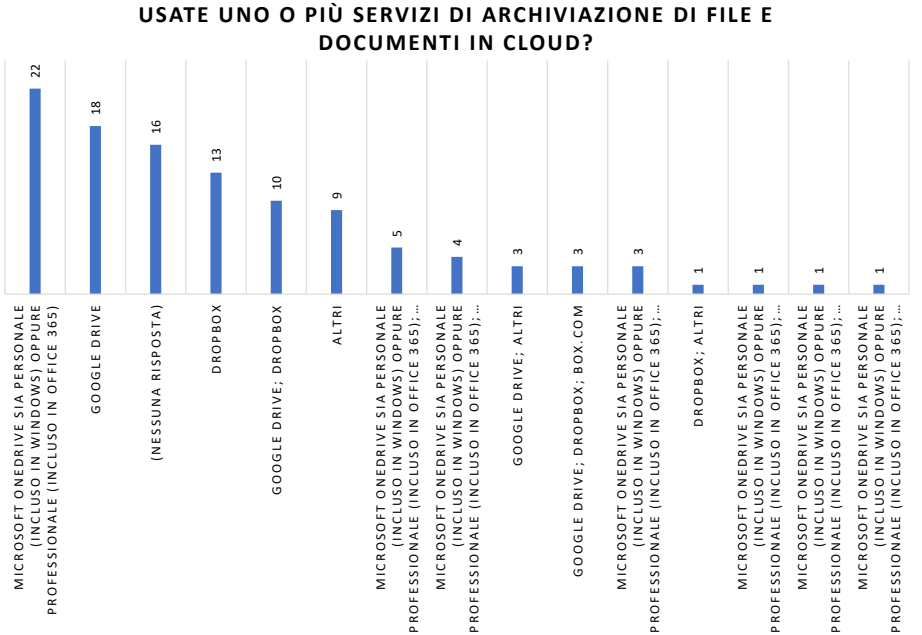


Figura 24: *Sistemi di archiviazione in cloud* (© Clusit - CNA Milano Survey 2022-23)

Conclusioni

- Le aziende sono in prevalenza piccole e con un fatturato non elevato.
- L'IT non è in prevalenza gestito in azienda.
- I responsabili della Cybersecurity sono carenti e la funzione stessa non è gestita in azienda: in caso di problemi ci si rivolge all'esterno.
- Si fa ancora poco affidamento sul regolamento sulla strumentazione informatica e sul registro per il trattamento dei dati personali.
- Manca una procedura ben definita per la gestione dei data breach.
- Non si investe in formazione in materia di privacy e Cybersecurity (soprattutto!)
- Ai dispositivi personali è concessa la connessione alla rete aziendale (e questo dovrebbe essere regolamentato).
- I dispositivi mobili non sono soggetti ad una politica aziendale.

La consapevolezza in termini di sicurezza informatica ci appare, in conclusione, ancora insufficiente rispetto alle sfide che il mondo di oggi pone alle imprese.
Ulteriore dato da registrare è il numero ristretto di adesione alla compilazione da parte delle imprese, che è da leggere come poca disponibilità delle imprese a leggersi sotto il punto della sicurezza informatica e che ci permette di sostenere che se aumentasse la risposta emergerebbe in modo più marcato, l'impreparazione delle imprese.
Da una parte ci si dice poco esposti al problema; ci si sente forse del tutto protetti, avendo adottato alcune contromisure tecnologiche minimali, come un antivirus ed un firewall. Purtroppo, la gravità e la persistenza delle minacce odierne richiedono ben altra preparazione: affidarsi soltanto ad alcune protezioni tecnologiche davvero di base, oggi, significa in realtà prestare inconsapevolmente il fianco a praticamente tutti gli attacchi che vengono realmente portati.

Si vive forse nell'illusione di poter confinare il problema, come testimonia la domanda a proposito del collegamento di dispositivi estranei alla rete, che in generale (almeno a parole) non sono assolutamente permessi. Nei fatti, questa posizione di principio viene, nei fatti, contraddetta immediatamente, poiché la grande maggioranza dichiara che naturalmente è consentito ai telefoni personali di collegarsi alla rete aziendale. Evidentemente i dispositivi dei dipendenti non sono vissuti come "estranei". Ma d'altra parte, nemmeno i dispositivi aziendali ad uso personale vengono gestiti centralmente, nella maggioranza dei casi; cosa che, in pratica, implica l'affidarsi sostanzialmente alla propria buona fortuna.

Peraltro, non solo le responsabilità di cybersecurity, ma addirittura quelle IT sono in prevalenza vissute come un qualcosa di esterno all'azienda, da delegare ad altri ogniqualvolta ciò sia percepito come possibile. Insomma, l'informatica è un male necessario, e la cybersecurity a maggior ragione. Altre risposte, tuttavia, indicano come questa delega sia operata con superficialità, e senza realmente indagare se davvero sia efficace. Si spera insomma di poter delegare ad altri il problema, quando si presentasse, ma, come testimonia ad esempio

la domanda relativa alla gestione dei data breach, non c'è alcuna preparazione a monte: il modello è forse quello del pompiere. Come però ben sa chi ha subìto davvero un incendio, per l'azienda questo non basta: i Vigili del Fuoco (quelli veri) sono i primi ad insistere sull'importanza della prevenzione.

Purtroppo anche la prevenzione non sembra particolarmente curata, come viene evidenziato dalle domande a proposito di politiche e procedure, e soprattutto a proposito di consapevolezza e formazione di tutti i collaboratori.
Gli unici punti dove la situazione sembra un poco più sotto controllo sono quelli legati alla privacy, dove la consapevolezza e l'organizzazione appaiono ad un livello di maturità più elevato, grazie probabilmente alla forte spinta che il legislatore ha ritenuto di imporre. I primi interventi in questo ambito risalgono però ormai al 1996, e dopo più di un quarto di secolo di lavoro, è ragionevole che ormai ci si possa attendere qualche risultato concreto.
Servirebbe probabilmente da parte del legislatore una spinta simile anche in ambito cybersecurity, che in qualche modo "forzasse" la maturazione di questa consapevolezza, agevolando la crescita di quel certo interesse che comunque le imprese denotano per il problema.
In questo modo il tessuto produttivo nazionale e della UE potrebbe finalmente, anche se in grande ritardo, acquisire una maggiore robustezza e resilienza, a fronte di antagonisti che evolvono velocemente e non hanno scrupoli ad usare qualsiasi mezzo per impadronirsi di nostre risorse ed arricchirsi a nostro discapito.
Il legislatore Europeo sta già intervenendo con effetti normativi che dovrebbero essere recepiti, nei prossimi anni, anche al nostro livello nazionale.

Access Broker e attacchi basati sull'identità: tendenze e protezione

[A cura di Luca Nilo Livrieri, CrowdStrike]

Quando parliamo di un sistema di Threat Actors, in relazione soprattutto all'Ecrime, dobbiamo pensare ad un'organizzazione criminale che si comporta ed agisce come una vera e propria azienda. Come in ogni azienda, ci sono dipartimenti e divisioni, ognuno con le proprie responsabilità: c'è chi si occupa delle risorse umane, chi del rapporto con i clienti nei servizi pre e post vendita, chi con i fornitori ecc. La tendenza degli ultimi anni, anche per gli attaccanti, è di comprare e fornire tutto "as a service". A livello macro possiamo identificare fra i threat actor "as a service", tre principali tipologie di settori: servizi, distribuzione e monetizzazione. Il settore dei servizi è quello che ha il compito di "armare" i cyber criminali fornendo tutto quello di cui i diversi gruppi di threat actors hanno bisogno per produrre la minaccia. All'interno di questa divisione ci sono coloro che forniscono i malware, gli accessi, le piattaforme e i server dove ospitare i server di command & control, i tool per effettuare attacchi denial of service e molto altro.

Il secondo settore è quello della distribuzione che, come dice la parola stessa, si occupa di "distribuire" l'attacco, facendo in modo che la minaccia arrivi al maggior numero di target possibile. In questo settore ci sono gruppi che si occupano di creare le pagine social per attirare le vittime, i messaggi di phishing o le campagne di spam personalizzate sui bersagli da colpire (spear phishing, ecc.).

Il terzo settore, infine, è quello dedicato alla monetizzazione e si occupa di trasformare gli attacchi informatici in denaro, ovvero di capitalizzarli. In questo settore ci sono gruppi specializzati nel riciclaggio di denaro, in riscatti ed estorsioni (ransom), in cryptovalute e altro. L'obiettivo è quello di trasformare l'attacco in denaro vero e proprio che poi deve essere a sua volta riciclato e spostato su conti correnti che sono utilizzati dai criminali in maniera rapida e veloce.

Figura 1: *Principali settori dell'ecosistema criminale*

Focalizzandosi sull'ambito dei servizi, è di particolare interesse l'analisi del fenomeno degli Access Broker, ossia quei gruppi criminali che sono specializzati nel fornire accesso alle aziende o a risorse utilizzate dalle aziende (third part o supply chain). Come vediamo dall'immagine di seguito (Fig.2), nell'analisi CrowdStrike della telemetria del 2022, mappando il framework Mitre sui dati raccolti, l'utilizzo di account validi è una delle tecniche più popolari e utilizzate dai Threat Actors, insieme ad un aumento nel targeting dei servizi remoti, anch'essi spesso vittime degli attacchi tramite l'utilizzo di credenziali rubate.

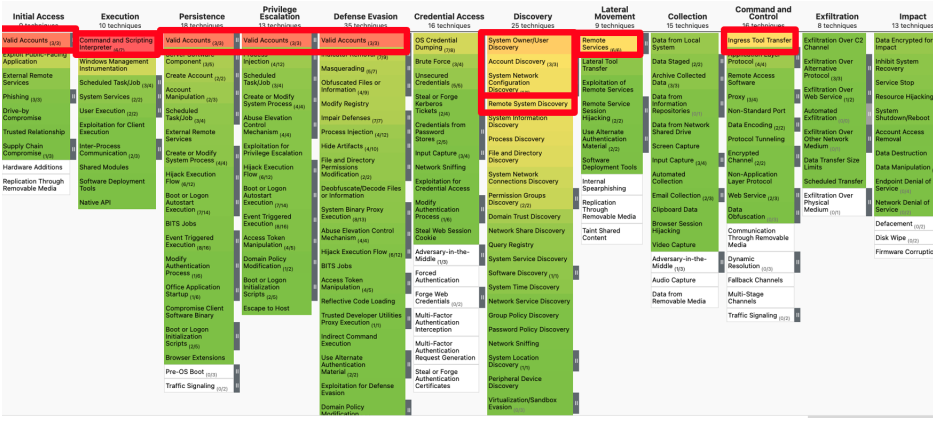


Figura 2: *Tecniche più popolari nel 2022*

Il boom degli Access Broker

Il "boom" degli Access Broker è esploso nel 2022. Gli Access Broker sono Threat Actors che acquisiscono l'accesso alle organizzazioni e forniscono o vendono queste informazioni ad altri Threat Actors, inclusi gli operatori di ransomware, per velocizzare le fasi di accesso iniziale in un attacco informatico. Potremmo dire che forniscono un "initial access" as a service.
La popolarità e la diffusione di questi servizi è aumentata nel 2022, con più di 2.500 annunci pubblicitari di vendita di credenziali identificati, segnando un aumento del 121% rispetto al 2021.
Moltissimi broker hanno pubblicizzato la vendita di "pacchetti" di credenziali in blocco durante il 2022, mentre altri hanno continuato a utilizzare la tecnica "one-access one-auction" con vere e proprie aste singole per vendere le credenziali più gettonate e preziose a cifre maggiori.

Perché questo boom nelle vendite di credenziali? I Threat Actors, così come le aziende stesse, sono consapevoli che qualsiasi utente, sia esso un amministratore IT, un dipendente, un lavoratore da remoto, un fornitore di terze parti o un cliente, può essere compromesso ed esporre il fianco ad un potenziale attacco degli avversari. In questo contesto, sono proprio le aziende a dover autenticare ogni identità e autorizzare ogni richiesta per mantenere la sicurezza e prevenire un'ampia gamma di minacce informatiche, tra cui gli attacchi ransomware e gli attacchi alla supply-chain, in modo tale da evitare di incorrere in potenziali danni dai costi elevati.
Che l'autenticazione sia a uno o più fattori (2FA o MFA), gli Access Broker si occupano di fornire il servizio di accesso per "entrare" all'interno della rete target con tecniche dedicate per bypassare l'autenticazione (Clickjacking, iFrame on 2FA page, Response Maniputation, Status Code Manipulation, SIM Swap e social engineer). Gli avversari informatici stanno infatti continuando ad attaccare l'identità nella sua definizione più ampia, non limitandosi solo al furto di credenziali, bensì usando tecniche come il pass-the-cookie, il golden SAML e l'ingegneria sociale con MFA fatigue per compromettere le identità stesse.

Come lavora un Access Broker? L'Access Broker lavora alla costante ricerca di aziende dai sistemi informatici vulnerabili. Trovata la vulnerabilità sfruttabile, l'Access Broker tenterà l'accesso al sistema e verificherà la portata dei dati a disposizione: più importante sarà la tipologia di dati rilevati, maggiore sarà il valore dell'informazione.

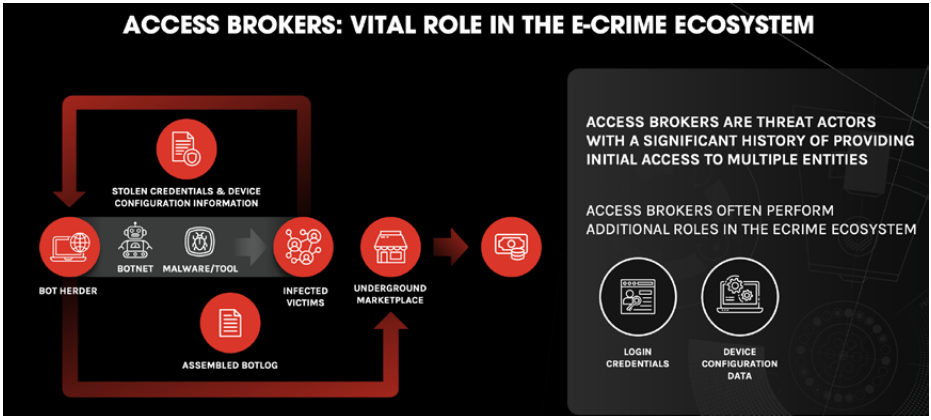


Figura 3: *Come funziona un Access Broker*

Una volta verificata la portata dell'accesso, l'Access Broker rivende l'informazione sulle piattaforme deep (in particolare nei forum) in attesa del miglior offerente. Di seguito i settori maggiormente "pubblicizzati" nel 2022.

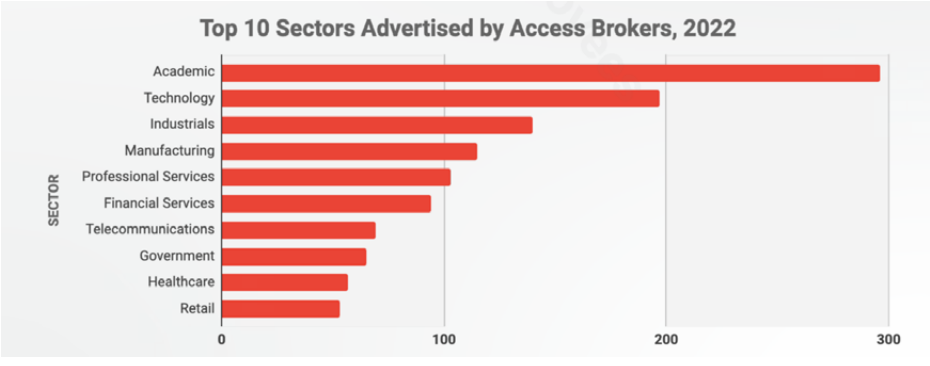


Figura 4: *CrowdStrike Global Threat Report*

Uno degli Access Broker più famosi a livello mondiale, secondo i report CrowdStrike, è Percussion Spider, attivo da Maggio 2020 e basato nell'Est Europa. Percussion Spider ha fra le sue caratteristiche, quella di colpire principalmente organizzazioni enterprise governative, energetiche e tecnologiche.

L'intelligence di CrowdStrike mappa anche una forte relazione tra questo Access Broker con il gruppo criminale responsabile del malware Tanos, a cui vende in maniera seriale credenziali di accesso a livello mondiale. Il connubio "Access-Broker" con i gruppi specia-

lizzati nella creazione di ransomware, sia esso o meno in modalità Ransomware as a Service, permette di velocizzare ancora di più le operazioni di movimento laterale all'interno della rete, creando un pacchetto completo che al suo interno ha già le credenziali per effettuare il movimento e che quindi, una volta scaricato sulla macchina, è in grado di propagarsi velocemente. Quando viene eseguito, il ransomware non si limita a colpire la macchina su cui è atterrato e non deve cercare credenziali per effettuare la "privileged escalation", ma le ha già incluse nel binario stesso ed è quindi molto rapido nella sua azione.

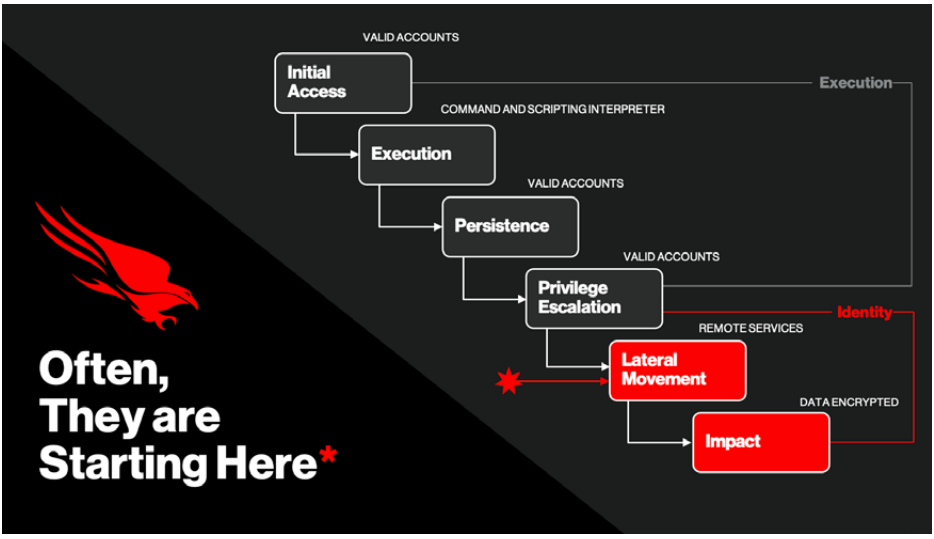


Figura 5: *Fasi di un attacco ransomware già in possesso di credenziali*

Di seguito vediamo alcuni esempi di annunci rilevati sul deep web dove vengono pubblicizzati accessi a diverse reti e organizzazioni in diversi settori, come una società di energia elettrica, un ospedale o una società di calcio. Non viene quasi mai menzionato il nome dell'organizzazione, se non, in qualche caso e solo dopo la prima negoziazione, al fine di evitare che eventuali strumenti di brand monitoring nel deep web facciano scattare un avviso. Ci sono però altre informazioni che possono aiutare ad identificare l'azienda, come il numero di dipendenti o il fatturato dell'azienda stessa e, a volte, viene fornita anche una descrizione dell'organizzazione copiata da Wikipedia. Strumenti avanzati di Threat Intelligence, grazie ad opportune regole di monitoraggio, possono consentire la protezione di questo tipo di annunci.

I prezzi delle vendite di credenziali variano molto ed oscillano fra i 1000 e i 5000 dollari a seconda delle dimensioni e dell'importanza dell'organizzazione, ma ci sono stati casi di vendita di credenziali a centinaia di migliaia di dollari. Tramite Access Broker è anche possibile

cercare credenziali in vendita specificando quelle che dovrebbero essere le caratteristiche dell'azienda target, mettendo un vero e proprio annuncio di quello che si sta cercando.

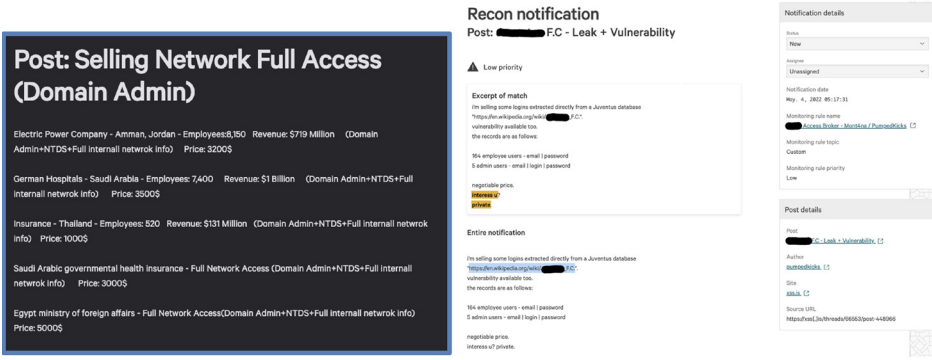


Figura 6: *Esempi di annunci di vendita di credenziali e monitoraggio con sistemi di Threat Intelligence*

Access Broker e fileless attack

Come si legano i temi di Access Broker e attacchi privi di malware? Va da sè che, nel momento in cui si è già in possesso delle credenziali per accedere ad una rete, non è necessario un malware da distribuire per garantire l'accesso iniziale e "rubare" le credenziali per effettuare il movimento laterale all'interno della rete diminuendo quindi il breakout time (ovvero il tempo medio per effettuare il movimento laterale).

Gli attacchi prive di malware (fileless attack) rappresentano il 71% di tutti i rilevamenti nel 2022 (rispetto al 62% nel 2021). Il 71% delle violazioni evita del tutto l'utilizzo di malware, per eludere i software antivirus legacy basati sull'identificazione di firme di malware noti. Questo dato è certamente correlato alla crescita degli Access Broker e all'abuso di credenziali valide da parte degli avversari per agevolare l'accesso e la persistenza in ambienti target. Un altro fattore che contribuisce all'aumento degli attacchi fileless è la velocità con cui vengono rilevate e divulgate nuove vulnerabilità e la velocità con cui gli avversari sono in grado di rendere operativi gli exploit.

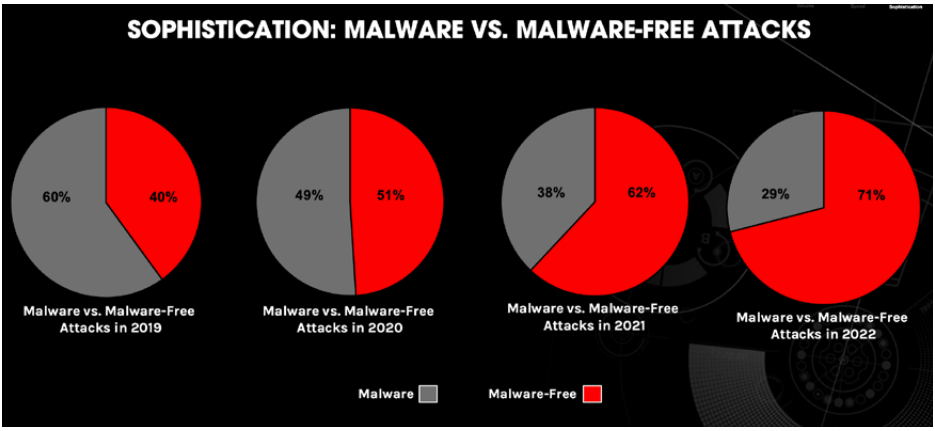


Figura 7: *Tendenza degli attacchi Malware-free*

Questi attacchi malware-free vengono anche definiti LOTL (Living Off the Land), perché usano strumenti e tool già presenti all'interno della macchina. La motivazione dietro all'utilizzo di queste tecniche è duplice: grazie a tali funzionalità e strumenti, gli aggressori sperano di mimetizzarsi nella rete della vittima e nascondere la propria attività all'interno dei processi legittimi. In secondo luogo, anche se viene rilevata un'attività dannosa che coinvolge questi strumenti, è molto più difficile attribuire gli attacchi. Se tutti utilizzano strumenti simili, è più difficile distinguere un Threat Actor da un altro. Le tecniche più comuni utilizzate dagli attacchi LOTOL sono elencate nella tabella di seguito.

Technique name	**Technique Description**
Use of Compromised Credentials	The use of legitimate compromised credentials found via web-scraping or in underground forums; used to gain legitimate network access.
Exploitation of Internet-Facing Assets	The exploitation of Internet-facing items such as web servers, email servers, web apps, IoT, etc.
PSExec	A lightweight telnet replacement that lets you execute processes on other systems, complete with full interactivity for console.
Remote Desktop Protocol (RDP)	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.

Native Binaries	The use of on-system native binary assets on the machine, examples include wscript.exe, cscript.exe, mshta.exe, etc.
PowerShell	A task-centric command-line shell and shell scripting language that helps system admins automate tasks and execution processes

Attacchi basati sull'identità: come prevenire e difendersi

L'evoluzione del panorama delle minacce rende la protezione dell'identità all'interno delle aziende una priorità assoluta. Quasi l'80% dei cyberattacchi sfrutta attacchi basati sull'identità per compromettere le credenziali legittime e utilizza tecniche come il movimento laterale per eludere rapidamente il rilevamento. La realtà è che gli attacchi basati sull'identità sono difficili da rilevare, soprattutto perché la superficie di attacco, per molte imprese, continua ad aumentare.

Ogni azienda deve autenticare ogni identità e autorizzare ogni richiesta per mantenere una solida postura di sicurezza. Appare semplice, ma in verità questo è ancora un punto critico per molte imprese.

Gli avversari sono diventati più abili nell'ottenere credenziali rubate per aprirsi un varco in un'azienda. L'identità è diventata il nuovo perimetro, poiché gli aggressori prendono sempre più di mira le credenziali per infiltrarsi all'interno di un ambiente aziendale. Purtroppo, le imprese continuano a essere compromesse da attacchi basati sull'identità e non hanno la consapevolezza necessaria per prevenirli. Anche le terze parti o un cliente possono essere compromessi e offrire un percorso di attacco agli avversari. In questo contesto, sono proprio le aziende a dover autenticare ogni identità e autorizzare ogni richiesta per mantenere la sicurezza e prevenire un'ampia gamma di minacce informatiche, tra cui gli attacchi ransomware e gli attacchi alla supply-chain, così da prevenire potenziali danni dai costi elevati.

L'approccio zero-trust per contenere gli avversari

La protezione dell'identità non può essere un tassello a sé stante: è solo un aspetto di una strategia di sicurezza efficace, che funziona al meglio insieme ad un sistema di sicurezza zero trust. L'approccio zero trust prevede che tutti gli utenti, sia all'interno che all'esterno della rete dell'organizzazione, siano autenticati, autorizzati e continuamente convalidati prima che venga concesso o mantenuto l'accesso alle applicazioni e ai dati. In poche parole, non esiste una fonte affidabile in un modello zero trust. Il fatto che un utente sia autenticato per accedere a un determinato livello o area di una rete non garantisce necessariamente l'accesso a tutti i livelli e aree. Ogni movimento viene monitorato e ogni punto di accesso e di richiesta di accesso vengono analizzati. Sempre. Questo è il motivo per cui le imprese con le difese di sicurezza più solide utilizzano una soluzione di protezione dell'identità insieme ad un sistema di sicurezza zero trust.

Come proteggere l'identità

Negli ultimi due anni, l'adozione da parte delle imprese di tecnologie basate sul cloud, atte a consentire alle persone di lavorare da qualunque luogo, ha creato una "crisi di identità" che deve essere risolta. Una soluzione completa per la protezione dell'identità deve offrire all'organizzazione una serie di vantaggi e funzionalità avanzate.
Queste includono la capacità di:

- bloccare gli attacchi moderni come il ransomware o gli attacchi supply-chain;
- superare i test Red Team / Audit;
- migliorare la visibilità delle credenziali in un ambiente ibrido (comprese le identità, gli utenti privilegiati e gli account di servizio);
- migliorare il rilevamento dei movimenti laterali e la difesa;
- estendere l'autenticazione a più fattori (MFA) ai sistemi legacy e a quelli non gestiti;
- rafforzare la sicurezza degli utenti privilegiati;
- proteggere le identità dall'acquisizione di account;
- rilevare gli strumenti d'attacco.

La protezione dell'identità è talvolta vista come l'ultima linea di difesa per le organizzazioni, ed è per questo che dovrebbe essere una componente chiave dell'approccio alla sicurezza delle aziende. Le imprese che rinnovano il loro approccio alla sicurezza delle identità si troveranno nella posizione ideale per bloccare le violazioni e mantenere la continuità aziendale, specialmente in un periodo caratterizzato dall'aumento di minacce basate sullo sfruttamento di credenziali compromesse. Ecco di seguito alcune best practice che possono avere un forte impatto sul livello di difesa delle aziende di piccole e medie dimensioni:

- **Educare i dipendenti**: l'intera forza lavoro dovrebbe essere consapevole dei diversi tipi di minacce alla sicurezza informatica e degli attacchi di ingegneria sociale che potrebbero trovarsi ad affrontare durante le attività lavorative, di cui il phishing, lo smishing e l'honey trapping ne sono solo un esempio.
- **Rafforzare l'autenticazione multi-fattore (MFA):** l'identità è una componente critica degli attacchi informatici e la MFA fornisce un ulteriore livello di difesa che rafforza la sicurezza, assicurandosi che si tratti del dipendente e non di un attaccante informatico che tenta di accedere ai sistemi e alle risorse.
- **Eseguire backup regolari dei dati critici**: è importante eseguire back up dei dati in cloud, soprattutto nel caso in cui si verifichi una violazione a danno di una piccola azienda. Il cloud fornisce migliore accessibilità e visibilità dei back up dei dati, insieme ad una più rapida esecuzione che riduce ulteriormente i tempi di inattività. È importante sapere che i cyber criminali possono crittografare i back up qualora dovessero ottenere l'accesso ai sistemi, pertanto è necessario mettere in atto una solida strategia di difesa.

- **Mantenere aggiornate le patch del software**: le violazioni dei dati spesso hanno inizio quando un attaccante informatico sfrutta una vulnerabilità priva di patch, soprattutto in ambito fileless.
- **Bloccare gli ambienti cloud**: proteggere i drive cloud come Box o Google Drive implementando la MFA e aderendo al principio del "minimo privilegio" garantisce ai dipendenti di avere accesso soltanto alle risorse necessarie a compiere le proprie attività lavorative.
- **Implementare e testare la rilevazione e la risposta alle minacce:** prendersi del tempo per analizzare gli ambienti e i comportamenti degli utenti in caso di attività malevole o anormali. Essere aggiornati sugli autori delle minacce, sulle tecniche e sugli indicatori di attacco. Definire, documentare e testare come si verifica una risposta agli incidenti. Pianificare il "quando", non il "se".

Nel momento in cui questi elementi base sono stati soddisfatti, è bene considerare la difesa "intel-driven" per supportare il rilevamento e la risposta. Comprendere gli autori delle minacce non è necessariamente complesso o dispendioso in termini di tempo, purché alla base ci sia un'adeguata threat intelligence. L'attribuzione consente ai team di sicurezza di comprendere la loro reale posizione di rischio, definendo chi potrebbe attaccarli e come, oltre ad adattare la strategia di sicurezza. La cybersecurity rappresenta una grande sfida, ma è possibile costruire una solida postura di sicurezza e proteggere l'ambiente dalle minacce odierne, anche con risorse limitate. Ripensare la propria strategia di sicurezza e aggiornare le proprie difese può fare una grande differenza nella capacità di superare un attacco informatico se, o più probabilmente quando, saremo costretti ad affrontare un incidente.

Infrastrutture critiche Italiane

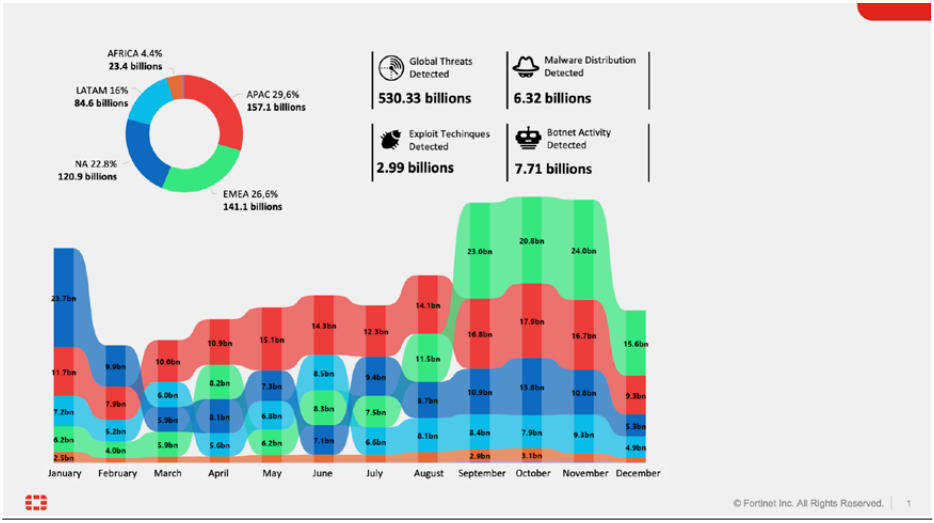
(A cura di Aldo Di Mattia, Fortinet)

Nel corso del 2022 le infrastrutture critiche italiane e mondiali sono state fortemente prese di mira da parte dei criminali informatici. La pandemia ha contribuito a intensificare le minacce cyber, in particolar modo quelle dirette al settore "**Healthcare**", che ha visto maggiormente aumentare la numerosità delle **minacce** negli ultimi anni e che a livello globale ha registrato, nel corso del 2022, un numero pari a **80.44 miliardi** a livello globale (il 15,16% di quelle identificate in totale). Emergono altri dati preoccupanti, di minore intensità ma di maggiore complessità, come l'individuazione di malware "ransomware" costruito per le infrastrutture OT (Operation Technology) e la ricomparsa di malware di tipo "wiper", cioè di virus che hanno come unico scopo quello di distruggere il sistema target, diretti a sistemi IT e OT. Entrambi i dati sembrano essere legati all'invasione dell'Ucraina e alle attuali tensioni geo politiche. I virus "wiper" erano stati sostituiti infatti dai malware "ransomware", che permettevano di remunerare l'attaccante. Nello scenario geo politico attuale, gli attacchi "state sponsored", ideati per destabilizzare i governi target paralizzando i servizi essenziali erogati dalle infrastrutture critiche, sono senza alcun dubbio i più preoccupanti, anche se in numero esiguo rispetto agli attacchi generati dal "cybercrime".
I dati indicati di seguito sono stati estratti dai FortiGuard Labs, l'organizzazione globale di threat intelligence e ricerca di Fortinet sulle minacce. I FortiGuard Labs monitorano la superficie di attacco mondiale e utilizzano l'intelligenza artificiale per estrarre i dati relativi. Nei seguenti grafici è possibile vedere il nome di molte minacce, individuate da Fortinet, nel sito web https://www.fortiguard.com, nel campo di ricerca "search threats advisories", dove può essere inserito il nome delle firme mostrate così da avere dettagli aggiornati in tempo reale.

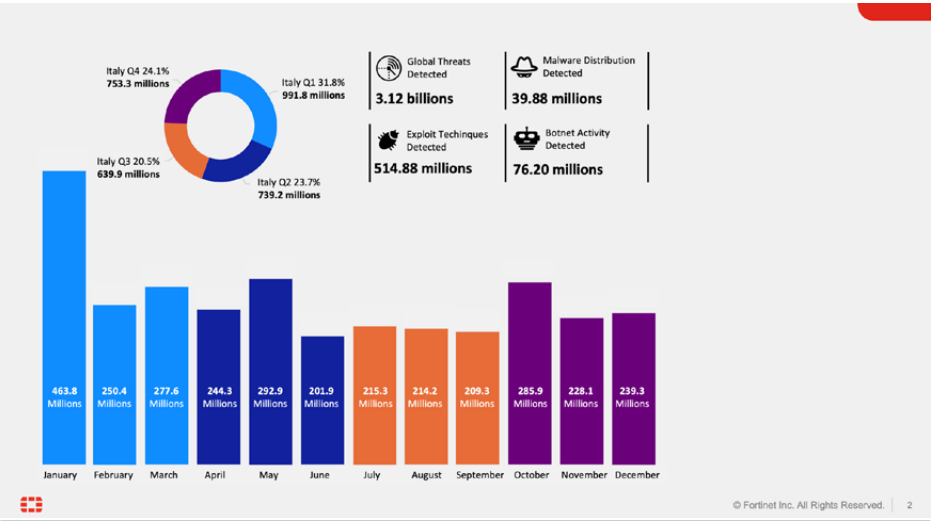
Le minacce più riscontrate in Italia

Di seguito le minacce più individuate, in termini di Exploit, Botnet e Malware, dirette alle infrastrutture critiche di tutto il mondo e italiane. I FortiGuard Labs hanno individuato nel corso del 2022 un totale di **530,33 miliardi di minacce** in tutto il mondo. Di queste **l'Italia** rappresenta lo **0,58%**, con **3,12 miliardi di minacce** identificate. Nel mondo sono stati individuati 6,32 miliardi di malware, 2.99 miliardi di Exploit, 7.71 miliardi di Botnet, con dei picchi nei mesi di gennaio e ottobre, gli stessi avuti in Italia.
In termini di "**Exploit Attempts**" l'Italia ha registrato nel corso del 2022 un totale di **514,88 milioni**, pari al **17,22% dei totali (2,99 miliardi)**, di cui 69 milioni riguardanti "Log4Shell" (pari al 0,08% dei totali) e 10 milioni riguardanti "IoT Remote Code Execution" (pari al 0,06% dei totali).
Il numero totali di **malware** individuati in Italia è stato pari a **39,88 milioni**, con il **0,63% degli attacchi globali (6,32 miliardi)**. Di questi i malware "Cripto Miner" sono stati 4 milioni (1,91% di quelli globali pari a 209 milioni) mentre i "trojans" si sono attestati a 35

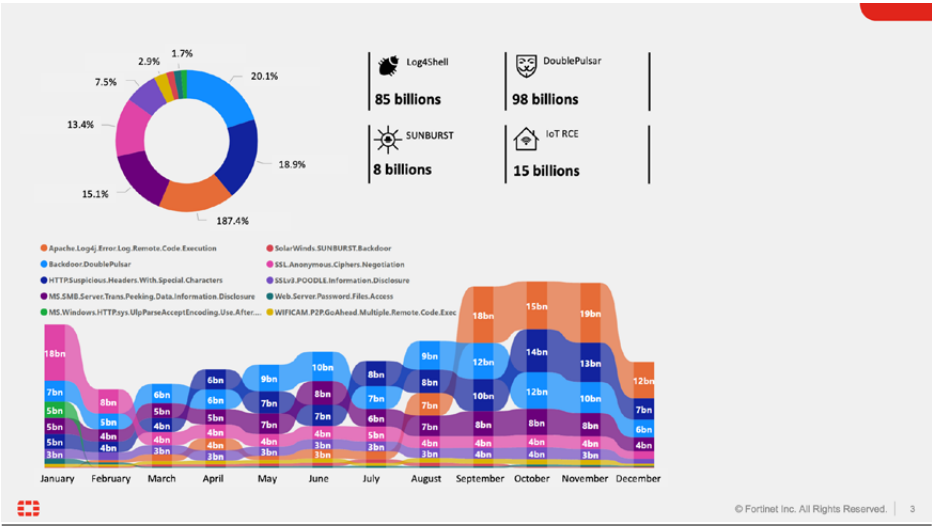
milioni (0,7% di quelli globali pari a 5 miliardi) e i virus "drive by download" sono stati 3 milioni (1,16% di quelli globali pari a 258 milioni).
In ultimo, in termini di "Endpoint vulnerability" in Italia sono stati identificati dei picchi di tentativi di utilizzo delle stesse nei mesi di febbraio e giugno, di cui la maggior parte relativa a "JAVA" (diversi CVE nuovi 2022) ma anche "Log4Net" (CVE datato 2018).



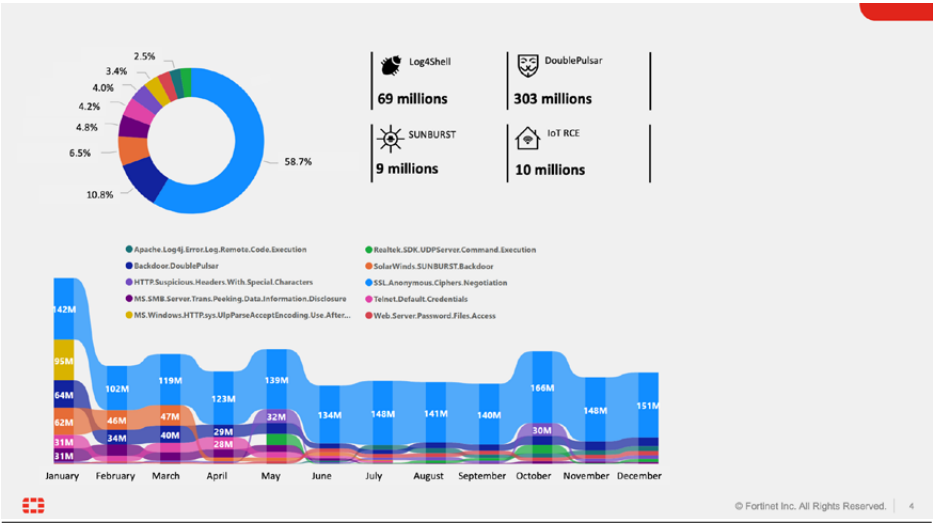
Global Threats Landscape worldwide



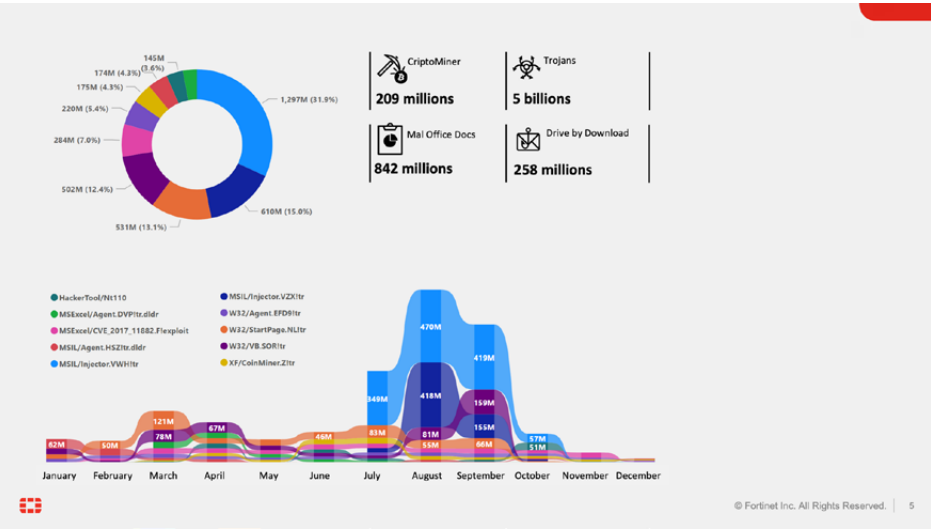
Global Threats Landscape Italy



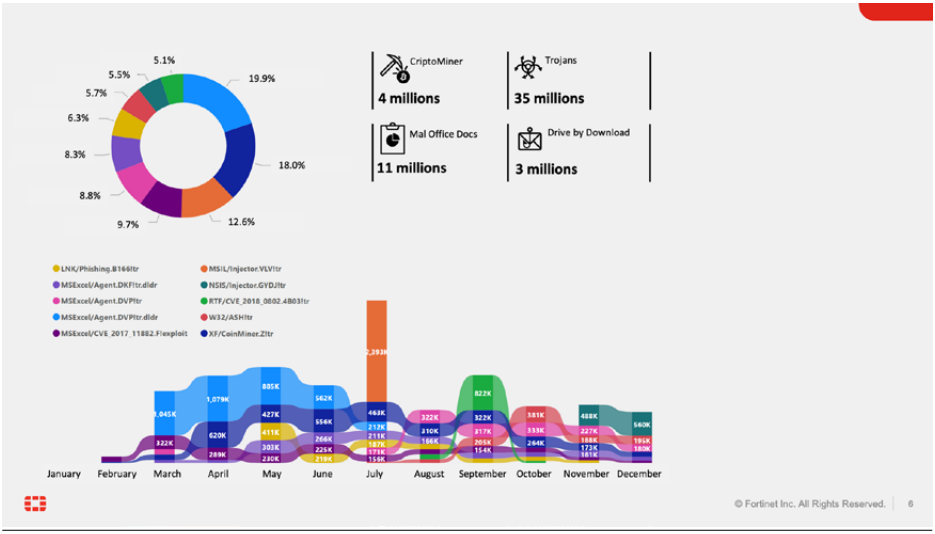
Exploit attempts worldwide



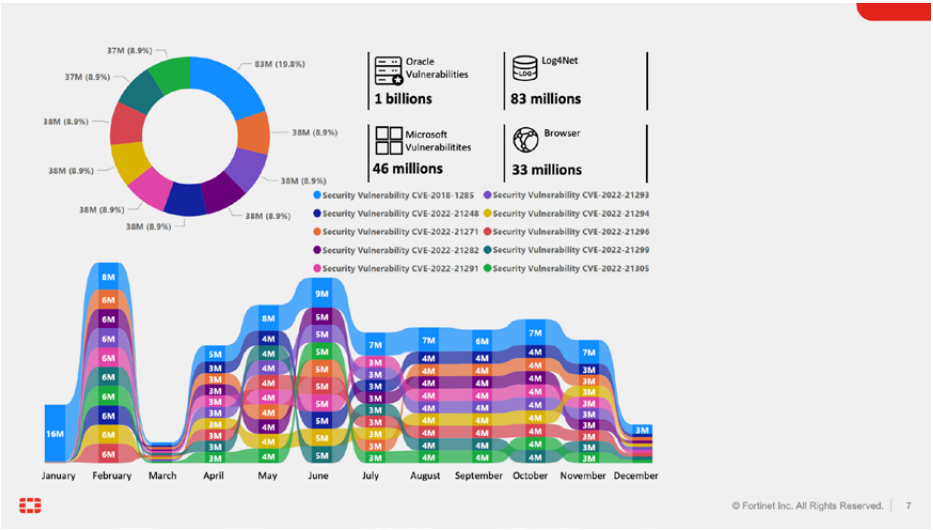
Exploit attempts Italy



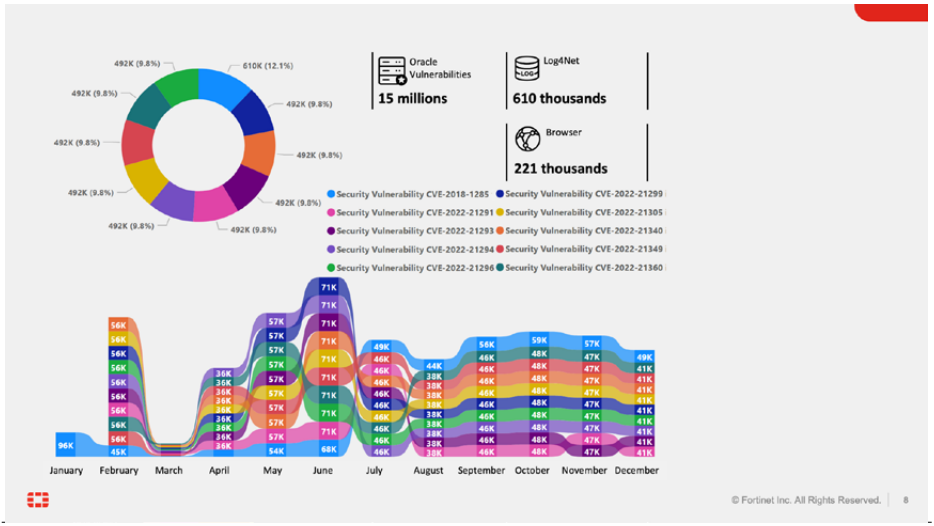
Malware detection worldwide



Malware detection Italy



Endpoint vulnerability worldwide



Endpoint vulnerability Italy

Le minacce globali nei mercati delle infrastrutture critiche

L'analisi dei dati inerenti alle minacce e gli attacchi specifici alle infrastrutture critiche su scala globale, secondo quanto rilevato dai FortiGuard Labs, evidenzia uno scenario fortemente influenzato dal contesto macroeconomico mondiale.
L'alterazione dell'equilibrio geopolitico causata dall'invasione Russa in Ucraina ha rappresentato indubbiamente un elemento di innesco ed amplificazione per le attività di cybercrime nell'ambito delle Infrastrutture Critiche. L'Europa nel 2022 è stato infatti il teatro più significativo, con il **60,5%** del totale, per quanto concerne il volume delle attività del Cybercrime verso le Infrastrutture Critiche, ed il fenomeno appare correlato su scala temporale al conflitto in corso.

Il settore **Healthcare**, già oggetto di numerosi attacchi nel corso del periodo pandemico, ha fatto registrare un volume totale di **80.44 miliardi di minacce** rilevate, di cui il **90,8%** ha interessato la regione **Europa e Middle East** (da qui in avanti **EME**). Da segnalare un picco significativo durante il terzo e quarto trimestre del 2022, dove "Exploit Attempts" della nota vulnerabilità "Log4Shell" hanno rappresentato il 95,5% del totale degli attacchi all'industria Healthcare in EME.

Il comparto del **Transportation** ha fatto registrare un volume totale di **2,86 miliardi di minacce** rilevate, di cui il **47,4%** in **EME**. L'exploit maggiormente registrato è stato il "SolarWinds Sunburst Backdoor", con il 66.2% del totale.

L'industria **Energy & Utilities** è stata oggetto di **7,65 miliardi di minacceg** rilevate, di cui l'**86,6%** in **EME**. L'exploit dominante in questo mercato appartiene alla famiglia delle vulnerabilità SSL, in particolare "SSL Anonymous Ciphers Negotiation" con il 92,4% del totale. In particolare, le infrastrutture legate alla produzione ed al trasporto del gas hanno fatto registrare un significativo aumento di attacchi rispetto al periodo precedente.

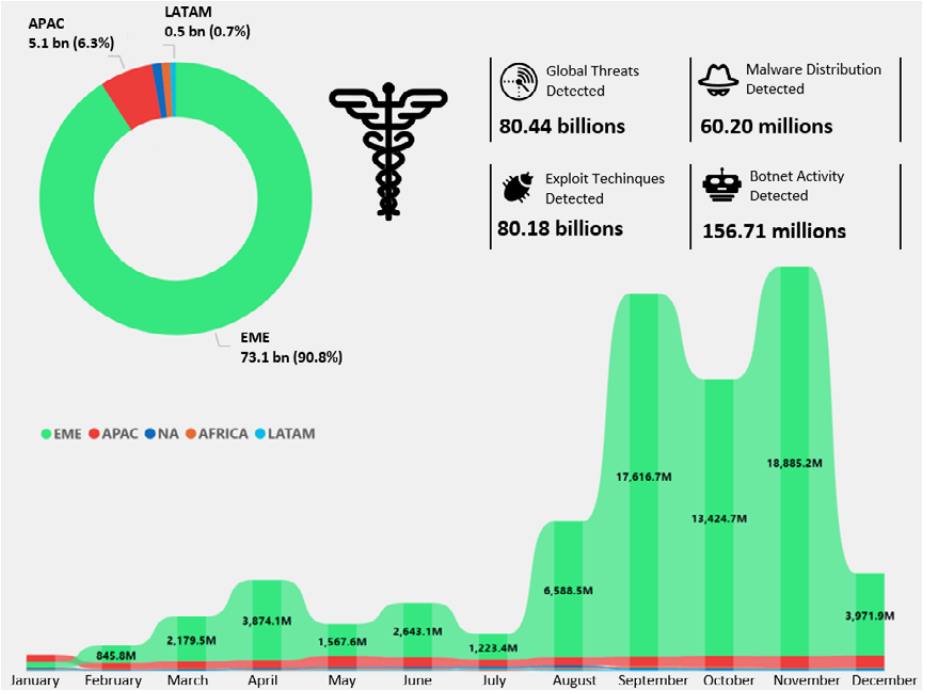
L'industria **Telco & Carrier**, infrastruttura critica per eccellenza quale vettore principale del flusso informativo, è stata protagonista di un volume crescente di attacchi mirati, in concomitanza delle prime fasi del conflitto in Est Europa. Il comparto è stato interessato da **17.82 miliardi di minacce** rilevate, di cui il **55,7%** nella regione **EME**. L'exploit maggiormente registrato è stato il "SolarWinds Sunburst Backdoor", con il 70,9% del totale.

L'ambito **Government** ha risentito della stessa fenomenologia geopolitica per le implicazioni politiche, diplomatiche e militari che un conflitto in corso presuppone. Il mondo Governativo ha fatto registrare **7.44 miliardi di minacce** rilevate, di cui il **24,4%** in **EME** ed il **41,9%** in **APAC**.

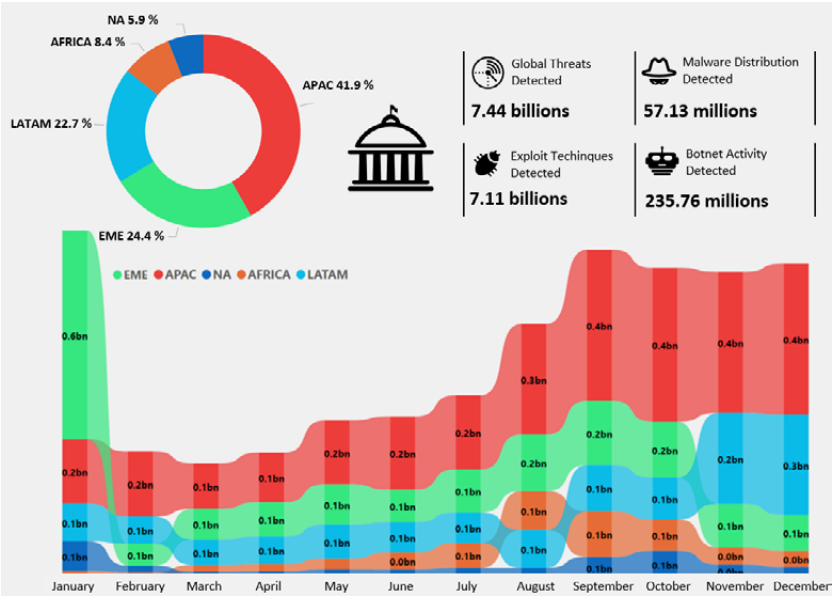
L'industria **Finance**, pur riconfermandosi un costante obiettivo di Cybercrime, ha anch'essa subìto un volume di attacchi crescente nel corso del 2022. Il comparto ha fatto registrare

un totale di **10.30 miliardi di minacce** rilevate, di cui il **57,9 %** in **EME**. L'exploit dominante in questo mercato appartiene alla famiglia delle vulnerabilità SSL, in particolare "SSL Anonymous Ciphers Negotiation" con l'86,6% del totale.

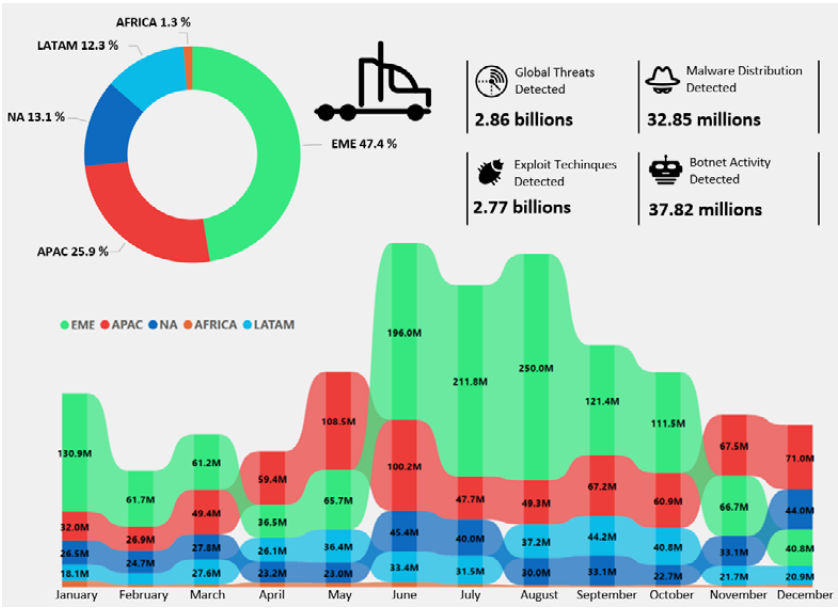
I grafici seguenti cristallizzano ed evidenziano nei numeri quanto il 2022 ha rappresentato in termini di "Threat Landscape" per le infrastrutture critiche su scala globale.



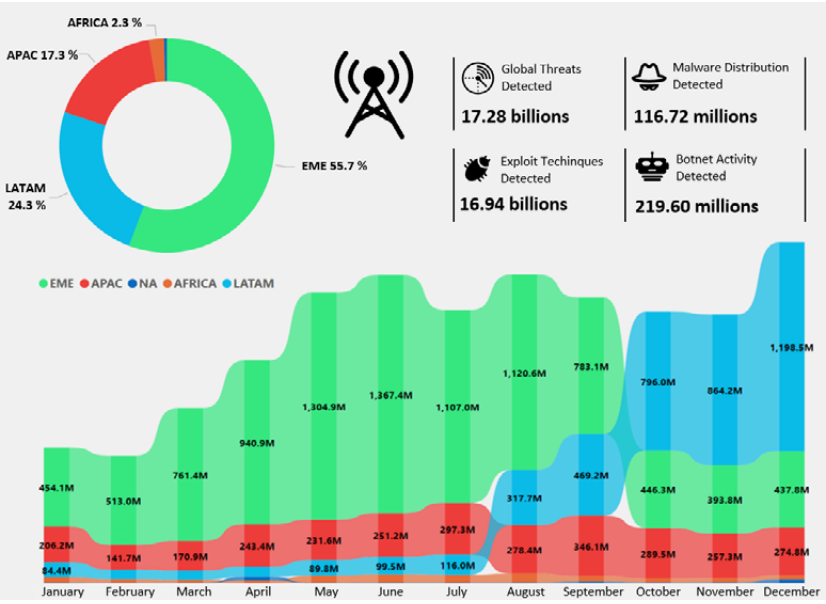
Healthcare Threat Landscape



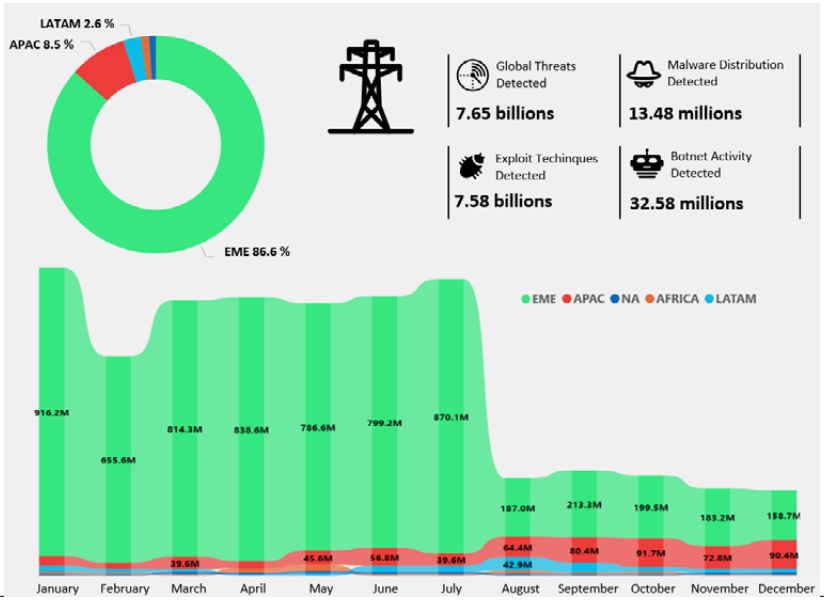
Government Threat Landscape



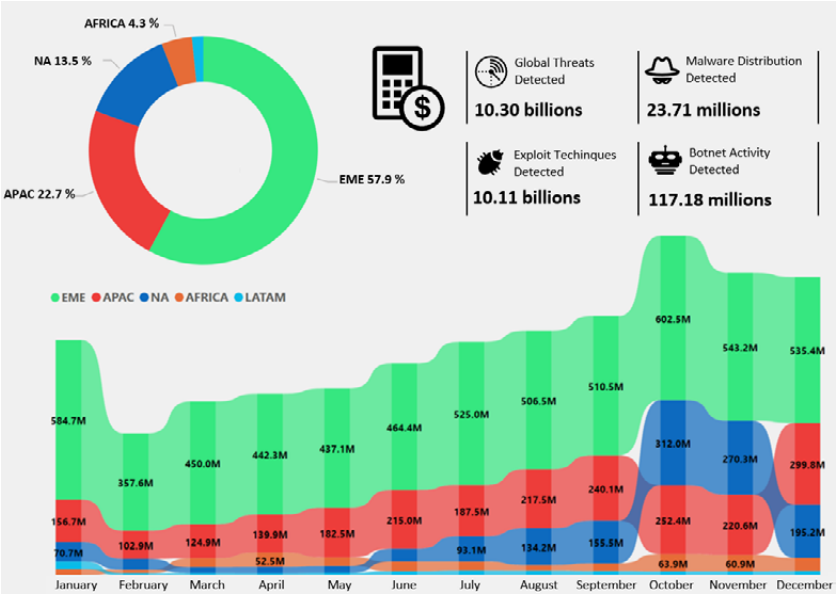
Transportation Threat Landscape



Telco Threat Landscape



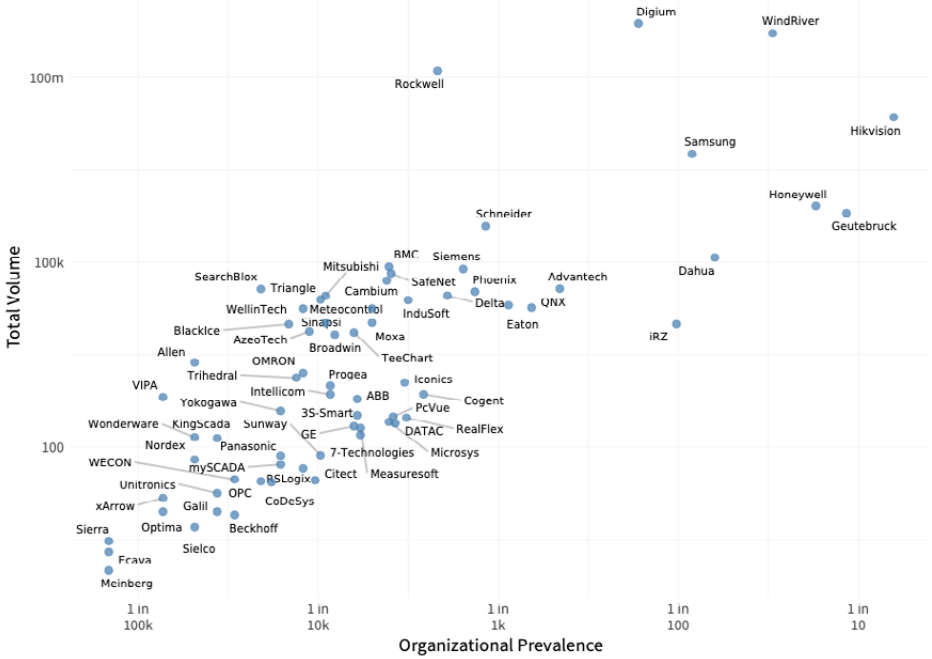
Energy & Utilities Threat Landscape



Finance Threat Landscape

Le minacce diretta alle infrastrutture di Operation Technology

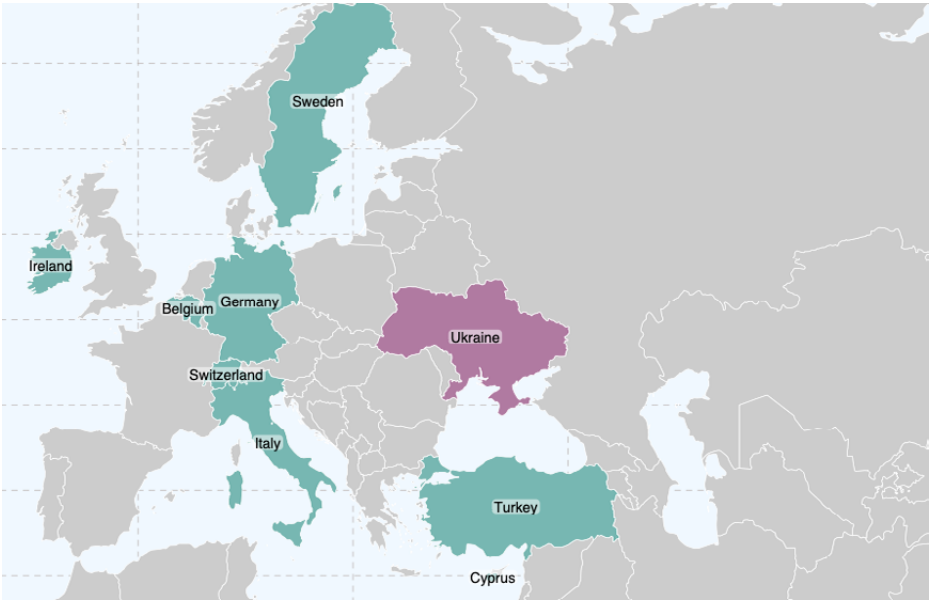
I sistemi appartenenti alla categoria Operational Technology (**OT**) rappresentano indubbiamente un obiettivo sensibile per attacchi di matrice sia politica che finanziaria. La gran parte dei dispositivi OT è considerata non sicura "by design", poiché la loro progettazione parte dal presupposto che questi sistemi lavorino in ambienti protetti quali reti "air-gaped" (completamente disconnesse). Partendo da questo assunto, i progettisti tendono quindi a privilegiare funzionalità ed efficienza, spesso a discapito della sicurezza. Non è più possibile basare la sicurezza dei sistemi OT solo sulla rete entro la quale operano. È quantomai importante considerare il mondo OT un elemento indipendente da proteggere in termini di vulnerabilità e "zero-days".



Diffusione e volume di "exploits" su OT nei primi 6 mesi del 2022

L'immagine sopra rappresenta il volume e la diffusione di vulnerabilità rilevate su sistemi OT. Mentre la maggior parte dei vendor risulta essere raggruppata in un'area contigua, nel primo semestre 2022 risultano anche due evidenti picchi a carico di Hikvision e Geutebruck. Utilizzando la mappatura ed i volumi rappresentati, si vuole fornire al lettore un elemento di riflessione rispetto alla presenza nella propria realtà di quei sistemi OT, che potrebbero richiedere una specifica attenzione in termini di sicurezza e visibilità, oltre che la gestione di vulnerabilità e contromisure.

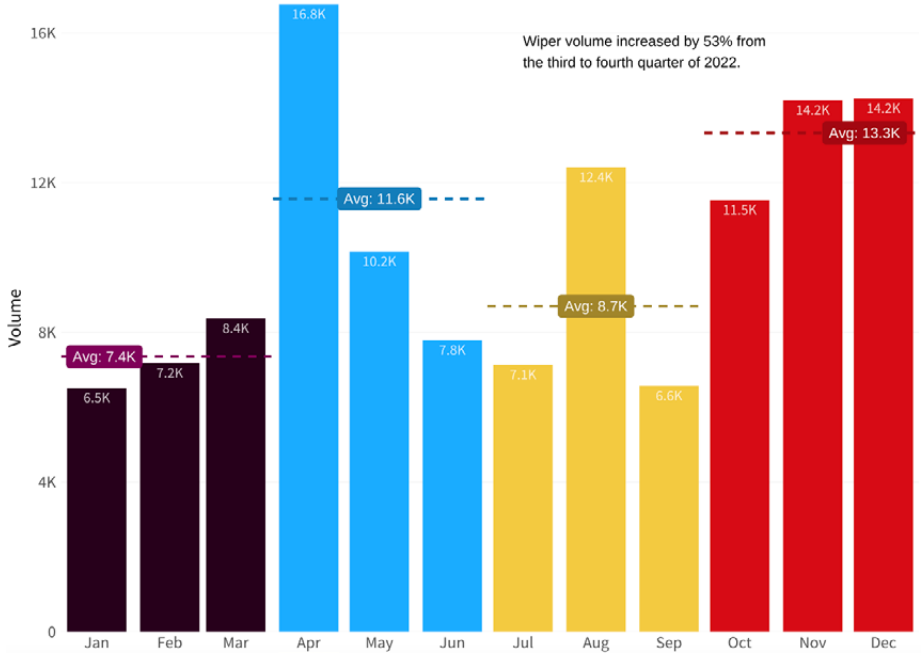
Il conflitto in Ucraina ha fatto registrare un sostanziale incremento nell'utilizzo di "Wiper" ovvero malware finalizzato alla cancellazione totale di dati su disco. Fortinet ha identificato ben sette nuove varianti di wiper nel corso della prima metà del 2022, principalmente utilizzati in campagne contro entità Governative, Private e Militari in Ucraina. Si tratta di un numero molto significativo di varianti in un periodo così breve, poiché circa sette ne erano state identificate in totale nell'ultimo decennio, a partire dalla variante **Shamoon** del 2012 utilizzata contro *Saudi Aramco* e *RasGas in Quatar*. I numeri rilevati nella prima metà del 2022 indicano con ottima approssimazione che gruppi criminali allineati agli obiettivi russi nel conflitto in corso siano gli artefici di tale incremento di varianti wiper, ai danni di infrastrutture principalmente, ma non limitatamente, Ucraine.



Identificazione di "wiper" inerenti il conflitto in corso nei primi 6 mesi del 2022

Nell'immagine sono evidenziate le nazioni europee che hanno riscontrato attacchi di tipo wiper nel corso dei primi sei mesi del 2022 e tra queste è presente l'Italia. È interessante notare che nonostante l'Ucraina abbia rappresentato nel 2022 il principale obiettivo di tali attacchi, essi sono stati tuttavia rilevati in ben altri 24 paesi. Un esempio importante è rappresentato dal wiper **AcidRain**, utilizzato inizialmente per colpire Service Provider Satellitari ucraini, poi utilizzato anche per un attacco ad un campo eolico in Germania, che ha messo offline circa **6000 turbine eoliche**. Queste dinamiche indicano un chiaro rischio che tali attacchi possano facilmente travalicare confini, che siano essi di Nazioni o di reti IT ed OT.

In sintesi, quanto rilevato in Ucraina suggerisce che questa famiglia di malware può essere utilizzata, in funzione del contesto, sia per generare danni ad infrastrutture critiche che per perseguire obiettivi militari. Inoltre i wiper sono stati utilizzati sia come strumento di "cyber sabotage" come Shamoon già nel 2012, ma anche come ransomware "improprio" finalizzato all'estorsione di denaro alle vittime come **NotPetya** e **GermanWiper** a partire dal 2017.



Mapping CVEs Reveals Vulnerability Red Zone to Help CISOs Prioritize

In ultimo, questo grafico rappresenta il volume di malware "wiper" individuati nei diversi mesi del 2022 e mostra un aumento del 53% dell'attività dal terzo al quarto trimestre.

Cyber Resilienza

[A cura di Carlo Mauceli, Microsoft]

PNRR è una sigla che sta per *Piano nazionale di ripresa e resilienza*. Si tratta del programma stilato dal governo Conte, presentato alle Camere e ora al vaglio del Comitato Tecnico di Valutazione, per ottenere i finanziamenti messi a disposizione dall'Europa nell'ottica del Recovery Fund. Il documento presenta diversi ambiti di intervento in cui si citano **digitalizzazione**, rafforzamento del sistema sanitario, transizione ecologica, economia circolare. Obiettivi virtuosi, racchiusi in una cornice in cui il termine *resilienza* spicca come un evento favolistico in un mondo ordinario come quello del linguaggio tecnico-istituzionale. *Resilienza* è tutt'altro che una parola nuova, ma gode oggi di una diffusa simpatia e una altrettanto più recente antipatia. Nuovo è comunque il ruolo che l'attuale governo le sta attribuendo, a conferma dell'ampliamento del ventaglio dei settori di utilizzo del termine anche se, personalmente, ritengo che venga troppo spesso abusata e, soprattutto, nell'ambito tecnologico sia molto lontana dall'essere realtà. Nei dizionari se ne contano solitamente non più di due o tre, di cui i primi sono settori strettamente tecnologici.

resilienza [re-si-lièn-za] n.f.
1. (fis.) proprietà dei materiali di resistere agli urti senza spezzarsi, rappresentata dal rapporto tra il lavoro necessario per rompere una barretta di un materiale e la sezione della barretta stessa
2. capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi ecc.: resilienza sociale (cfr. garzantilinguistica.it)

Noi ci concentreremo sulla seconda in particolare sulla resilienza informatica.
I leader odierni dovrebbero considerare la resilienza informatica come una parte essenziale della resilienza aziendale. Dovrebbero gestire le interruzioni informatiche con le stesse modalità con cui si affrontano i disastri naturali o altri eventi imprevisti, riunendo stakeholder interni dei settori delle operation, delle comunicazioni, delle questioni legali e altro ancora al fine di creare delle strategie adeguate. In questo modo, le organizzazioni possono riportare rapidamente online i sistemi aziendali critici e riprendere le normali operazioni aziendali. Ma non è tutto. Poiché molte organizzazioni si affidano a fornitori e service provider di terze parti, i leader decisionali dovrebbero estendere la pianificazione della resilienza informatica alla catena del valore end-to-end per garantire, appunto, la business continuity e la resilienza.

La resilienza informatica è la capacità di reagire ad un evento tecnico avverso. Ovvero, la capacità di un sistema di resistere ad un cyber attacco o ad un evento catastrofico.
Un sistema tecnologico dovrebbe essere resiliente anche verso altre tipologie di avversità, soprattutto a tutto ciò che è legato all'evoluzione e al cambiamento dei materiali. Inoltre,

utilizzare un approccio legato alla resilienza, riduce l'impatto di attacchi informatici, poiché protegge i dati e ripristina rapidamente il sistema.
La strategia di resilienza informatica richiede un cambiamento. Pertanto l'organizzazione dovrebbe adottare la sicurezza come lavoro a tempo pieno e con l'integrazione delle migliori pratiche di resilienza nelle operazioni quotidiane. Attraverso la resilienza un'azienda diventa intelligente e agile per gestire attacchi reali o potenziali. **Cyber security e cyber resilience sono si diverse ma lavorano in simbiosi**. Nonostante siano trattate come due elementi separati e correlati, viene dato più valore quando la sicurezza informatica costituisce un elemento della resilienza globale.
Nello scenario digitale attuale, quasi il 60% delle aziende subisce una violazione dei dati e le difese utilizzate si rivelano inefficienti a proteggere l'azienda dalle violazioni. È importante sapere che le intrusioni informatiche sono inevitabili. La resilienza informatica aiuta le aziende a difendersi da crimini informatici, riducendo i rischi e la gravità degli attacchi, consentendo la continuità aziendale. Un'azienda cyber resilience è preparata per affrontare gli attacchi e può rispondere in modo efficace agli stessi, ripartendo rapidamente quando si verificano questi eventi.
La sicurezza informatica è un fattore chiave per il successo tecnologico. Innovazione e miglioramento della produttività possono essere solo ottenute con l'introduzione delle misure di sicurezza che permettono alle organizzazioni di essere resilienti il più possibile contro i moderni attacchi.

Le minacce digitali e il grado di sofisticazione degli attacchi informatici aumentano di giorno in giorno. Oggi, molti attacchi complessi si concentrano sulla compromissione dei sistemi d'identità, delle supply chain e di terze parti sfruttando, molto spesso, i laschi sistemi di controllo della sicurezza. In particolare, gli attacchi di phishing mirati alle identità sono una minaccia definita e presente. Tuttavia, questi tipi di attacchi, in genere, non hanno esito positivo se sono implementate procedure efficaci di gestione delle identità, controllo del phishing e gestione degli endpoint. Di conseguenza è utile ricordare una nozione di base: **il 98% degli attacchi può essere fermato con una protezione della sicurezza di base**.
La gestione dell'identità e dei dispositivi nel segno di un approccio Zero Trust, che include l'accesso con privilegi minimi e credenziali a prova di phishing per fermare efficacemente gli autori delle minacce e proteggere i dati, rappresentano il punto di partenza per innalzare la propria postura di sicurezza. Oggi anche i criminali informatici privi di competenze tecniche sofisticate possono lanciare attacchi incredibilmente distruttivi perché l'accesso a tattiche, tecniche e procedure avanzate è praticamente aperto a tutti nell'economia della criminalità informatica. Con la guerra in Ucraina, per citare una situazione sotto gli occhi del mondo intero, i cosiddetti "nations state actors" hanno intensificato le loro operazioni informatiche offensive ricorrendo sempre più spesso al ransomware. Il ransomware ora è diventato, per così dire, un settore sofisticato, nel quale i threat actors usano tattiche di estorsione doppia o tripla per ottenere il pagamento di un riscatto e dove gli sviluppatori offrono il ransomware come servizio (RaaS). Con RaaS, i threat actors usano una rete di

affiliazione per eseguire gli attacchi, abbassando le barriere di ingresso per i criminali informatici meno qualificati e, di conseguenza, espandendo il bacino di utenti malintenzionati. I recenti attacchi alla supply chain e ai fornitori di terze parti indicano un importante punto di svolta nel settore. I blocchi che questi attacchi causano a clienti, partner, enti pubblici, ecc. continuano ad aumentare, testimoniando quanto sia importante dedicare attenzione alla resilienza informatica e alla collaborazione tra i vari stakeholder della sicurezza. Gli avversari prendono di mira anche i sistemi locali, confermando quanto sia necessario che le organizzazioni gestiscano le vulnerabilità prodotte dai sistemi legacy, modernizzando e spostando l'infrastruttura nel cloud, dove la sicurezza è più solida e, soprattutto, è condivisa. Viviamo in un'era in cui la sicurezza è un fattore chiave del successo tecnologico. L'innovazione e il miglioramento della produttività possono essere raggiunti solo introducendo misure di sicurezza in grado di rafforzare il più possibile la resilienza delle organizzazioni rispetto agli attacchi moderni. Con l'aumento e l'evoluzione delle minacce digitali, è essenziale integrare la resilienza informatica nel tessuto di ogni organizzazione.

Resilienza informatica: le fondamenta essenziali di una società connessa

La rivoluzione nella tecnologia digitale ha trasformato le organizzazioni, sempre più connesse sia nel modo di operare che nei servizi offerti. Con l'aumento delle minacce in ambito informatico, è fondamentale integrare anche la resilienza informatica nel tessuto dell'organizzazione, oltre alla resilienza finanziaria e operativa. La trasformazione digitale ha alterato per sempre il modo in cui le organizzazioni interagiscono con clienti, partner, dipendenti e altri stakeholder. Le nuove tecnologie offrono enormi opportunità di interagire con le persone, trasformare i prodotti e ottimizzare le operazioni. La pandemia ha accelerato la trasformazione digitale promuovendo tecnologie innovative che consentono alle persone di collaborare in modi inediti e da qualsiasi luogo. Man mano che le minacce informatiche diventano endemiche, nel nostro mondo "sempre connesso" diventa sempre più difficile evitare che compromettano un'organizzazione. Come dicevamo all'inizio di questo scritto, la resilienza informatica rappresenta la capacità di un'organizzazione di continuare le operazioni e di promuovere l'accelerazione della crescita nonostante i continui attacchi. La prevenzione deve essere bilanciata con funzionalità di sopravvivenza e ripristino. A tal fine, enti pubblici e aziende stanno sviluppando modelli completi che vanno oltre la sicurezza e la privacy per proteggere dati e risorse nell'ambito della resilienza informatica.

La resilienza informatica richiede un approccio olistico, adattivo e globale in grado di resistere alle minacce in continua evoluzione, indirizzate a servizi e a infrastrutture di base, tra cui:

- Protezione informatica di base, come illustrato nella curva a campana della resilienza informatica.
- Comprensione e gestione del rapporto rischio rendimento della trasformazione digitale.
- Funzionalità di risposta in tempo reale che consentono il rilevamento proattivo di minacce e vulnerabilità.

- Protezione contro gli attacchi noti e attività preventive contro i vettori di attacco nuovi e previsti, inclusa la funzionalità di correzione automatica.
- Impatto ridotto di attacchi e disastri grazie all'isolamento dei problemi e alla segmentazione.
- Ripristino e ridondanza automatizzati in caso di interruzione.
- Priorità ai test operativi per individuare eventuali lacune e comprendere responsabilità condivise e dipendenze da risorse esterne, come le soluzioni di sicurezza basate sul cloud.

Un programma efficace di resilienza informatica inizia dalle nozioni di base sulle risorse, ad esempio la conoscenza dei servizi disponibili e la presenza di un catalogo affidabile delle risorse a cui si può ricorrere in caso di interruzione. Partendo da queste informazioni, il programma deve essere in grado di valutare la propria efficacia, misurare le performance dei servizi critici e delle relative dipendenze, testare e convalidare le funzionalità nei servizi locali e cloud e promuovere un'ottimizzazione continua del ciclo di vita digitale dell'organizzazione.

Per offrire un approccio olistico, è necessario identificare i servizi, i processi aziendali, le dipendenze, il personale, i vendor e i fornitori locali e online più importanti. Bisogna, inoltre, identificare le risorse associate alle aspettative dei clienti e del mercato, agli obblighi normativi e contrattuali e alle operazioni interne. Una volta trovate queste risorse critiche, può partire un'attività parallela volta a rilevare e monitorare le minacce, le interruzioni, i potenziali vettori di attacco e le vulnerabilità dei sistemi e dei processi. Completare questo processo con le attuali carenze di competenze richiede una rigorosa definizione delle priorità, basata sul rischio complessivo specifico per l'organizzazione.

Questo tipo di approccio olistico deve essere adattabile in un contesto di minacce in continua evoluzione e deve avere come obiettivi un miglioramento misurabile delle performance, la riduzione dei tempi di rilevamento, risposta e ripristino e la limitazione dell'impatto in caso di interruzione. L'approccio deve anche riconoscere la crescente connessione delle minacce. Ad esempio, un incidente di sicurezza potrebbe comportare una violazione dei dati con implicazioni per la privacy e richiedere la collaborazione di diversi team interni ed esterni per rispondere rapidamente e ridurre al minimo l'impatto.

L'importanza della modernizzazione dei sistemi e dell'architettura

Oltre l'80% degli incidenti di sicurezza può essere ricondotto alla mancanza di pochi elementi, che potrebbe essere risolta ricorrendo ai moderni approcci alla sicurezza.

I sistemi legacy, sviluppati prima dell'avvento dei moderni strumenti di connettività come smartphone, tablet e servizi cloud, rappresentano un rischio per le organizzazioni che ancora li impiegano. Questa esposizione al rischio è confermata dai risultati delle ricerche che, come *Microsoft Security Services for Incident Response*, abbiamo condotto nell'ambito del

supporto ai clienti che hanno l'esigenza di reagire e di ripristinare i sistemi dopo gli attacchi.

Nell'ultimo anno, i problemi riscontrati dai clienti in seguito al ripristino dopo un attacco hanno riguardato sei categorie, come illustrato in **Figura 1**. Nei paragrafi successivi vengono descritte le azioni concrete per migliorare la resilienza.

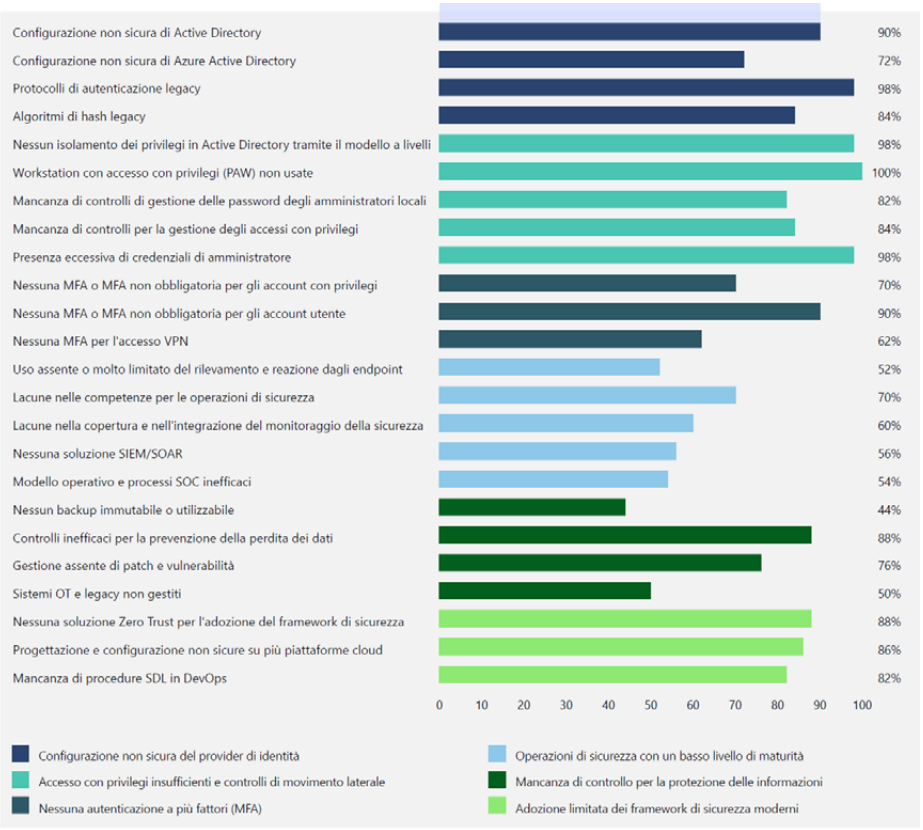


Figura 1: *Percentuale di clienti colpiti da attacchi che non ha eseguito i controlli di sicurezza di base*

L'importanza della modernizzazione dei sistemi e dell'architettura

Ci sono aree chiaramente identificate sulle quali le organizzazioni possono intervenire per modernizzare il proprio approccio e proteggersi dalle minacce:

Problema	Azioni concrete
Configurazione non sicura del provider di identità L'errata configurazione e l'esposizione delle piattaforme di identità e dei relativi componenti sono un vettore usato di frequente per ottenere l'accesso non autorizzato a privilegi elevati.	Segui le linee guida e le procedure consigliate per la configurazione della sicurezza quando distribuisci e gestisci i sistemi di identità come Active Directory e l'infrastruttura Azure Active Directory. Implementa le restrizioni di accesso applicando la separazione dei privilegi e l'accesso con privilegi minimi, nonché usando workstation con accesso con privilegi (PAW) per la gestione dei sistemi di identità.
Accesso con privilegi insufficienti e controlli di movimento laterale. Gli amministratori dispongono di autorizzazioni eccessive all'interno dell'ambiente digitale e spesso espongono le credenziali amministrative su workstation soggette a rischi legati a Internet e alla produttività.	Proteggi e limita gli accessi amministrativi per rendere l'ambiente più resiliente e depotenziare gli attacchi. Impiega controlli per la gestione degli accessi con privilegi, ad esempio l'accesso JIT (Just-in-Time) e l'accesso per amministratori JEA (Just-Enough Access).
Nessuna autenticazione a più fattori (MFA) Gli utenti malintenzionati odierni non irrompono ma accedono.	MFA è un controllo di accesso utente critico e fondamentale che tutte le organizzazioni dovrebbero implementare. Insieme all'accesso condizionale, MFA rappresenta uno strumento prezioso per la lotta alle minacce informatiche.
Operazioni di sicurezza con un basso livello di maturità. La maggior parte delle organizzazioni colpite dagli attacchi usava strumenti di rilevamento delle minacce tradizionali e non disponeva di insights rilevanti, utili per rispondere e correggere tempestivamente i problemi.	Una strategia di rilevamento delle minacce completa richiede investimenti in funzionalità di rilevamento e reazione estese (XDR) e in moderni strumenti nativi per il cloud che usano l'apprendimento automatico per separare il rumore di fondo dai segnali. Modernizza gli strumenti per le operazioni di sicurezza incorporando XDR, che offre insights approfonditi sulla sicurezza nell'intero panorama digitale.
Mancanza di controllo per la protezione delle informazioni. Le organizzazioni hanno ancora enormi difficoltà a organizzare controlli olistici per la protezione delle informazioni, in grado di coprire completamente tutte le posizioni dei dati, di restare efficaci durante l'intero ciclo di vita delle informazioni e di adattarsi al livello di criticità aziendale dei dati.	Identifica i dati aziendali critici e la loro posizione. Rivedi i processi del ciclo di vita delle informazioni e applica la protezione dei dati, garantendo al contempo la business continuity.
Adozione limitata dei framework di sicurezza moderni. L'identità è il nuovo perimetro di sicurezza che consente l'accesso a numerosi servizi digitali e ambienti di elaborazione. L'integrazione dei principi Zero Trust, della sicurezza delle applicazioni e di altri framework informatici moderni consente alle organizzazioni di gestire in modo proattivo rischi che altrimenti non prenderebbero neanche in considerazione.	I framework Zero Trust applicano concetti di privilegio minimo, la verifica esplicita di tutti gli accessi e la supposizione continua della violazione. Le organizzazioni dovrebbero anche implementare controlli e procedure di sicurezza in DevOps e nei processi del ciclo di vita delle applicazioni per garantire maggiori livelli di sicurezza dei sistemi aziendali.

Un profilo di sicurezza di base è un fattore determinante per l'efficacia delle soluzioni avanzate

In molti casi, l'esito di un attacco informatico viene determinato assai prima del suo inizio effettivo. Gli utenti malintenzionati sfruttano gli ambienti vulnerabili per ottenere l'accesso iniziale, condurre attività di sorveglianza e creare scompiglio attraverso il movimento laterale, la crittografia o l'esfiltrazione. Fermare un aggressore in queste fasi preliminari aumenta notevolmente la probabilità di ridurre l'impatto complessivo.
Attraverso lo studio delle configurazioni specifiche nei profili di sicurezza per identificare le carenze più comuni nelle procedure reali di questi ambienti si è in grado di osservare le vulnerabilità più comuni durante gli attacchi ransomware gestiti da persone, grazie alle quali i threat actors sono riusciti ad accedere e a spostarsi nella rete senza essere individuati.

Le configurazioni di sicurezza di base devono essere attivate

I dispositivi di un'organizzazione non integrati oppure obsoleti possono essere sfruttati dagli attaccanti come punti di ingresso e percorsi per ottenere l'accesso. Abbiamo scoperto che, pur essendo un passaggio importante, l'onboarding dei dispositivi aziendali con una soluzione aggiornata di rilevamento e reazione dagli endpoint (EDR) e una piattaforma di protezione degli endpoint (EPP) non garantisce il blocco del ransomware.
Soluzioni avanzate come EDR ed EPP sono essenziali per rilevare un utente malintenzionato nelle prime fasi del flusso di attacco e per attivare le funzionalità automatiche di correzione e protezione. Tuttavia, poiché essenzialmente si basano sulla capacità di rilevamento di un attacco, queste soluzioni avanzate richiedono l'attivazione delle configurazioni di sicurezza di base. Abbiamo osservato infatti diversi scenari in cui erano implementate delle soluzioni avanzate che sono stati compromessi dall'assenza di configurazioni di sicurezza di base.

Le procedure consigliate per le configurazioni di sicurezza rappresentano un indicatore di resilienza più importante dei tempi di risposta degli analisti del centro operazioni per la sicurezza (SOC).

Osservando la popolazione di clienti e partner per un periodo di sei mesi, abbiamo rilevato una riduzione del 70% del tempo impiegato da un analista SOC per individuare e reagire a un determinato avviso. Questa maggiore consapevolezza è un buon segno. Tuttavia, sebbene la visibilità sulla configurazione di sicurezza abbia migliorato le performance degli analisti SOC, la visibilità sui prodotti grazie all'integrazione e all'aggiornamento dei dispositivi dell'organizzazione si è dimostrata un indicatore di previsione molto più efficace in termini di prevenzione.

Rischi associati ai dispositivi sconosciuti

A differenza delle reti cloud, dove i clienti sanno quali risorse sono in esecuzione e su quali sistemi operativi, le reti locali possono contenere una vasta gamma di dispositivi non monitorati o gestiti dall'organizzazione, ad esempio IoT, desktop, server e dispositivi di rete.

Una rete aziendale include in media oltre 3.500 dispositivi connessi non protetti da un agente EDR, che potrebbero avere accesso a risorse aziendali o persino a risorse di alto valore.
Nello scenario attuale, i sistemi EDR sono fondamentali per rilevare i dispositivi e fornire informazioni sulle classificazioni dei dispositivi connessi alla rete; ad esempio il nome del dispositivo, la distribuzione del sistema operativo e il tipo di dispositivo.
Per i dispositivi non supportati da un agente EDR, è necessario essere almeno consapevoli della loro esistenza, adottando delle misure per proteggerli in base alle vulnerabilità e limitando l'accesso alla rete.

Garantire l'integrità delle identità è fondamentale per l'equilibrio organizzativo

La difesa dell'identità è più importante che mai. Anche se gli attacchi basati su password restano lo strumento principale di compromissione dell'identità, stanno emergendo altri tipi di aggressioni. Il volume degli attacchi sofisticati continua ad aumentare rispetto agli attacchi di tipo replay e password spraying, finora prevalenti.

Gli attacchi basati su password sono ancora frequenti e oltre il 90% degli account compromessi con questi metodi non è protetto con l'autenticazione avanzata, che si basa su più fattori di autenticazione quali, ad esempio, password + SMS e chiavi di sicurezza FIDO2.

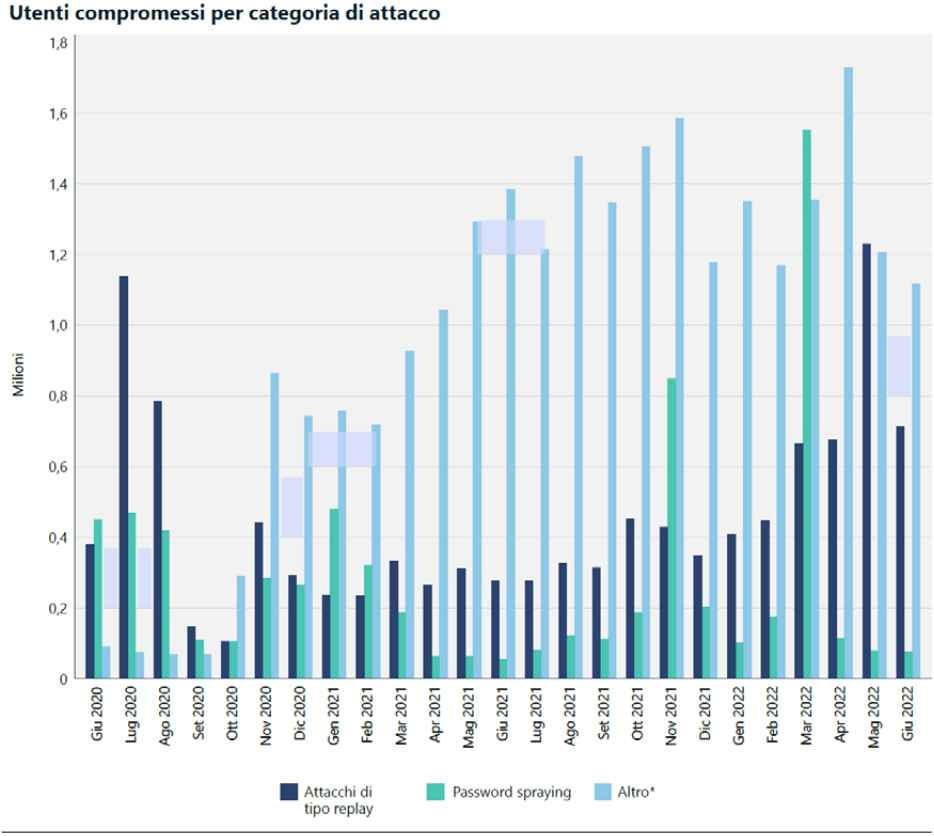


Figura 2: *Utenti compromessi al mese per categoria di attacco*

Il grafico di Figura 2 evidenzia come negli ultimi due anni si sia verificato un aumento degli attacchi di password spraying mirati, con picchi molto elevati nel volume di traffico degli attaccanti distribuiti tra migliaia di indirizzi IP.

Garantire l'integrità delle identità è fondamentale per l'equilibrio organizzativo

Adozione dell'autenticazione avanzata

Una tendenza positiva che abbiamo rilevato è l'adozione in costante aumento dell'autenticazione avanzata come, ad esempio, l'utilizzo di Azure Active Directory (Azure AD). Per Azure AD, la percentuale di utenti attivi ogni mese (MAU) dell'autenticazione avanzata è passata dal 19% al 26% nell'ultimo anno, mentre per gli account amministrativi i MAU sono aumentati dal 30% a circa il 33%.

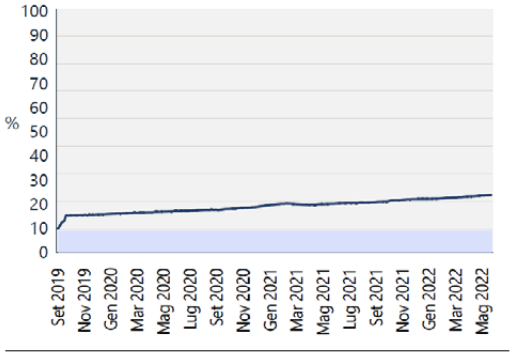


Figura 3: *Uso dell'autenticazione avanzata*

Questa tendenza è positiva ma c'è ancora molta strada da fare per raggiungere una copertura consistente con l'autenticazione avanzata. I clienti che non la usano ancora nei propri ambienti dovrebbero avviare la pianificazione e la distribuzione dell'autenticazione avanzata per proteggere gli utenti. Quando si progetta una distribuzione con autenticazione avanzata, è opportuno valutare un'autenticazione senza password perché offre un'esperienza di utilizzo più sicura, eliminando il rischio di attacchi alle password.

Anche se l'adozione dell'autenticazione avanzata è raddoppiata dal 2019, solo il 26% degli utenti e il 33% degli amministratori la usa.

Aumento costante degli attacchi di tipo token replay

Nel 2022 abbiamo registrato un aumento della percentuale di altri tipo di attacco. Abbiamo rilevato una crescita degli attacchi che evitano specificamente l'autenticazione basata su password per ridurre le possibilità di rilevamento. Questi attacchi sfruttano i cookie Single Sign-On (SSO) del browser o i token di aggiornamento ottenuti tramite malware, phishing e altri metodi. In alcuni casi, gli attaccanti scelgono un'infrastruttura nelle vicinanze della posizione geografica del bersaglio per ridurre ulteriormente le possibilità di rilevamento. Abbiamo assistito ad un aumento costante degli attacchi di tipo token replay, con oltre 40.000 rilevamenti al mese in Azure AD Identity Protection. Gli attacchi token replay usano token rilasciati a un utente legittimo da un malintenzionato in possesso di tali token. I token vengono in genere ottenuti tramite malware, ad esempio esfiltrando i cookie dal browser dell'utente o mediante metodi di phishing avanzati.

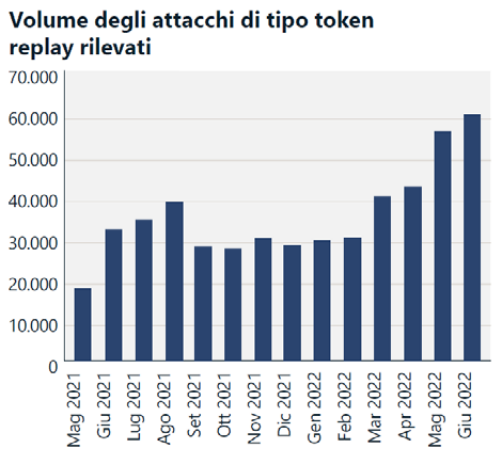


Figura 4: *Volume degli attacchi di tipo token*

Estrazione di token

Più che del malware, gli attaccanti hanno bisogno delle credenziali per raggiungere i loro obiettivi. Infatti, il 100% degli attacchi ransomware gestiti da persone si basa su credenziali rubate. Molte intrusioni sofisticate usano credenziali acquistate sul dark Web, sottratte in origine tramite malware per il furto di credenziali non sofisticati e ampiamente distribuiti. Questa classe di malware si è evoluta passando al furto di token, tra cui informazioni sulla sessione e attestazioni MFA. Ciò significa che le infezioni nei sistemi domestici, da cui gli utenti accedono alle risorse aziendali, possono causare incidenti gravi nelle reti aziendali.

Gli attaccanti possono estrarre i token dai dispositivi delle vittime anche con attacchi man-in-the-middle, in cui la vittima fa clic su un collegamento dannoso in un'e-mail di phishing o in un messaggio istantaneo e viene indirizzata a un sito Web che assomiglia alla pagina di accesso autentica del provider di identità. In realtà, si tratta di un servizio Web attivato dal criminale che inoltra e intercetta tutto il traffico tra l'utente e il provider di identità. L'attaccante riesce a intercettare il nome utente e la password e inoltrare anche le richieste MFA. I token risultanti emessi dal provider di identità e intercettati dall'attaccante potrebbero contenere attestazioni MFA che possono essere usate dall'aggressore per soddisfare i requisiti MFA.

Come Microsoft, abbiamo rilevato una media di 895 attacchi al mese di questo tipo dall'inizio del 2022. Questa forma di attacco può essere prevenuta usando fattori MFA resistenti al phishing, come l'autenticazione basata su certificati, Windows Hello for Business o le chiavi di sicurezza FIDO2.

Sovraccarico di MFA

Sfruttando il concetto di "sovraccarico di MFA", gli aggressori inviano più richieste MFA al dispositivo della vittima, nella speranza che la vittima accetti la richiesta inavvertitamente o per stanchezza. Questo attacco può essere prevenuto usando app di autenticazione moderne come Microsoft Authenticator, unite a funzionalità come la corrispondenza dei numeri. Azure AD Identity Protection stima che ogni mese vengano sferrati 30.000 attacchi di sovraccarico MFA.

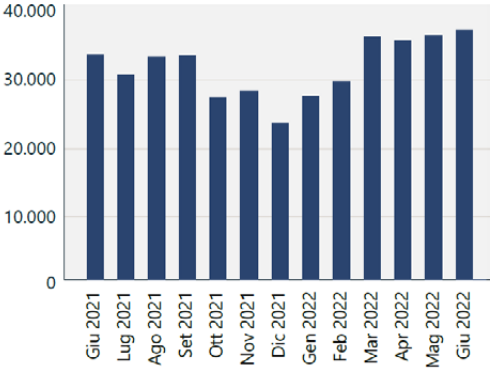


Figura 5: *Numero stimato di attacchi di sovraccarico*

Resilienza alle operazioni di influenza informatica: la dimensione umana

Quando parliamo di eventi riportati tramite testo, audio e contenuti visivi, siamo arrivati a un punto in cui né gli esseri umani né gli algoritmi riescono più a distinguere in modo affidabile la realtà dalla finzione. La proliferazione di questi strumenti e dei loro prodotti intacca l'affidabilità di tutti i media digitali e pregiudica la nostra interpretazione degli eventi locali e mondiali. Le nuove forme delle operazioni di influenza, rese possibili dai progressi tecnologici, hanno serie ripercussioni sui processi democratici.

Molti si chiedono come possiamo prepararci per un futuro più resiliente a queste operazioni di influenza informatica. La tecnologia è solo una parte del puzzle. Per completarlo, è necessario il contributo di tutti. Serve una formazione finalizzata all'alfabetizzazione mediatica, alla consapevolezza e alla vigilanza, investimenti nel giornalismo di qualità, con reporter affidabili che seguono le notizie a livello locale, nazionale e internazionale, reti per condividere e segnalare le operazioni di influenza e nuovi tipi di normative che perseguano i criminali che generano o manipolano i media digitali con obiettivi fraudolenti.

Bisogna essere consapevoli che ristabilire la fiducia nei contenuti digitali è un obiettivo ambizioso che richiederà approcci e contributi diversi. Non esiste un'azienda, un istituto o un governo in grado di risolvere queste minacce autonomamente. **Il nostro superpotere come esseri umani è la capacità di collaborare e cooperare**. Questo aspetto è particolarmente importante ora perché tutti, ovvero governi mondiali, settori industriali, mondo accademico e, soprattutto, organi di stampa, mass media e social media, dovranno lavorare insieme per il miglioramento e la salute della nostra società

La curva a campana della resilienza informatica

Come abbiamo visto, molti attacchi informatici vanno a buon fine semplicemente perché non è stata usata la sicurezza di base. Gli standard minimi che ogni organizzazione dovrebbe adottare sono:

- **Abilitare l'autenticazione a più fattori (MFA):** fornisce protezione contro le password utente compromesse e aiuta ad aumentare la resilienza per le identità.
- **Applicare i principi Zero Trust:** il fondamento di qualsiasi piano di resilienza per limitare l'impatto su un'organizzazione. Questi principi sono:

  Verifica esplicita: verifica lo stato di utenti e dispositivi prima di consentire l'accesso alle risorse.

  Uso dell'accesso con privilegi minimi: concedi solo i privilegi strettamente necessari per accedere a una risorsa.

  Ipotesi di violazione: parti dalla supposizione che le difese siano state violate e che i sistemi possano essere compromessi. Questo approccio si traduce in un monitoraggio costante dell'ambiente per rilevare possibili attacchi.

- **Usare le funzionalità di rilevamento e reazione estese antimalware:** implementa un software per rilevare e bloccare automaticamente gli attacchi e fornisci insights alle operazioni di sicurezza. Il monitoraggio degli insights ricavati dai sistemi di rilevamento delle minacce è essenziale per poter rispondere alle minacce in modo tempestivo.
- **Aggiornare regolarmente i sistemi:** i sistemi obsoleti e senza patch rappresentano la causa principale per cui molte organizzazioni cadono vittima di un attacco. Verifica che tutti i sistemi siano mantenuti aggiornati, inclusi il firmware, il sistema operativo e le applicazioni.
- **Proteggere i dati:** sapere quali sono i dati importanti, dove si trovano e se sono implementati i sistemi giusti è fondamentale per applicare le misure di protezione appropriate.

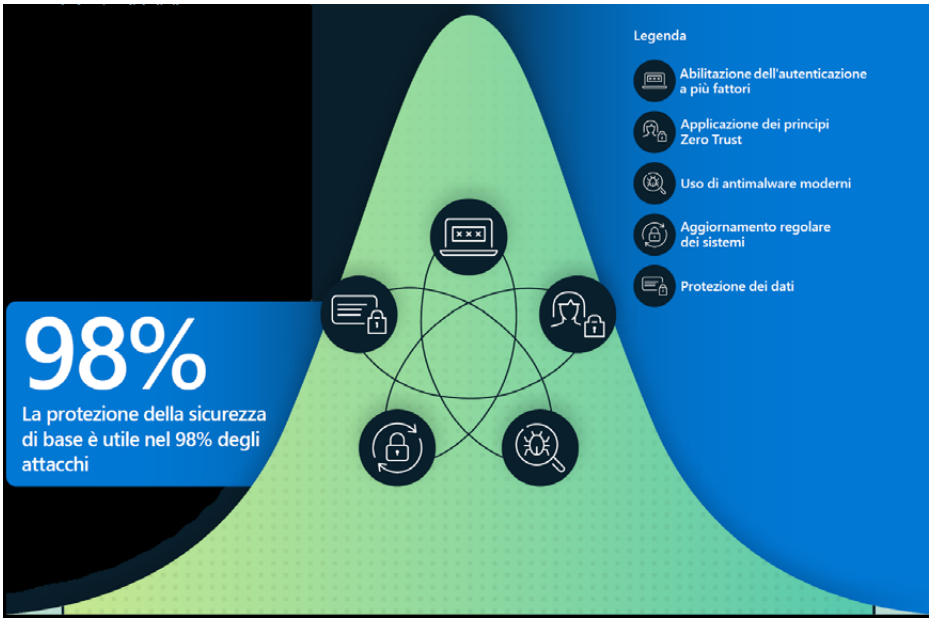


Figura 6: *La curva della resilienza informatica*

Referenze

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

https://www.kaspersky.com/blog/the-human-factor-in-it-security/

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

La nuova direttiva NIS 2 tra obbligo normativo e opportunità di migliorare la resilienza

[A cura di Enzo M Tieghi e Mario Testino, ServiTecno]

Introduzione

Nel 2018 con il DL 520/2018, come molti Stati della UE anche l'Italia ha ratificato la direttiva europea NIS (1148/2016 e RE 2018/151, EU NIS Network and Information Systems) che ha finalmente reso obbligatorie le misure necessarie per elevare il livello di sicurezza comune delle reti e dei sistemi degli Operatori di Servizi Essenziali e Fornitori di Servizi Digitali all'interno dell'Unione Europea.

Al di là degli aspetti generali ed organizzativi è risultato subito evidente come il focus della normativa fosse orientato alla riduzione di impatti negativi sulle attività economiche e sociali di potenziali incidenti informatici, ovvero garantire la continuità operativa degli Operatori di Servizi Essenziali, quali le istituzioni finanziarie, bancarie, sanitarie, le reti di telecomunicazione (in particolare gli Internet Service Provider), e tutte le Infrastrutture Critiche.

Nell'elaborare le strategie di mitigazione di pericolosi e costosissimi downtime non bisognava quindi sottovalutare l'impatto dei cyber incidenti su reti ed impianti e sulle tecnologie utilizzate sia Informative (IT) che Operazionali, la cosiddetta OT (Operational Technology, l'hardware e il software dedicati a rilevare o causare cambiamenti nei processi fisici attraverso il monitoraggio e / o il controllo diretto di dispositivi fisici, impianti e macchinari come generatori, compressori, trasformatori, valvole, pompe, ecc.).

Nel mese di febbraio 2019, 465 organizzazioni italiane sono state destinatarie di una "lettera speciale": la comunicazione dell'inserimento del loro nome nella lista di OSE Nazionali "attenzionati".

Infatti, il MISE, Ministero dello Sviluppo Economico, d'accordo con il Ministero delle infrastrutture e dei Trasporti, il Ministero dell'Economia e delle Finanze, il Ministero della Salute e il Ministero dell'Ambiente e della Tutela del Territorio e del Mare, in collaborazione con le Regioni e Province autonome di Trento e di Bolzano, ha identificato a livello nazionale 465 Operatori di Servizi Essenziali e FSD Fornitori di Servizi Digitali.

Si tratta di organizzazioni, sia pubbliche che private, appartenenti ai settori previsti dalla Direttiva Europea "NIS", Network and Information Security, che per la prima volta a livello continentale affrontava in modo organico e trasversale il tema della cybersecurity, con lo scopo di incrementare il livello comune di sicurezza e resilienza in tutti i Paesi UE.

L'Italia, assieme a Germania e Gran Bretagna, è stata nel gruppo di testa degli Stati membri

dell'Unione Europea che hanno dato seguito agli adempimenti della Direttiva NIS. La nomina di questi 465 OSE nazionali è stata definita dai Ministeri coinvolti come uno step in avanti decisivo per aumentare il livello di resilienza rispetto a minacce che già oggi sempre di più insidiano la sicurezza nazionale e la crescita del Paese: infatti le strategie di trasformazione digitale con i piani lanciati dal Governo (Industria4.0 e Transizione4.0) ed il panorama sociale possono moltiplicare i rischi, minacce e danni causati da incidenti "cyber".

Nella "prima NIS" del 2018 i settori strategici identificati e chiamati ad agire erano otto: energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali.

Tralasciando i settori bancario, infrastruttura dei mercati finanziari, il sanitario e le infrastrutture tipicamente digitali, notiamo come nei rimanenti settori quali energia, trasporti ed acqua potabile siano da anni presenti ed operanti sistemi di controllo e telecontrollo (SCADA) per la gestione di impianti ed infrastrutture fisiche, che necessitano di attenzione particolare riguardo agli aspetti della continuità operativa e protezione da rischi cyber.

Si può facilmente intuire come i sistemi OT a presidio delle infrastrutture fisiche (stiamo parlando di PLC, SCADA, RTU, DCS, ecc.), vista anche la progressiva convergenza tra IT-OT, siano elementi fondamentali per garantire la sicurezza fisica e la continuità del servizio. Proviamo solo per un istante ad immaginare il danno che potrebbe provocare un cyber-incidente (accidentale o malevolo che sia) ad un sistema di controllo di un impianto di generazione di energia o a un sistema di segnalamento ferroviario, aeroportuale o altro.

Come recitava il documento del MISE: "Gli obiettivi della NIS prevedono, in particolare, la promozione della cultura della prevenzione del rischio e le misure tecnico-organizzative per limitare l'impatto di incidenti informatici; il potenziamento delle capacità nazionali di cybersecurity; il rafforzamento della cooperazione – sia in ambito nazionale che europeo; e, ancora, la salvaguardia della business continuity per gli Operatori di servizi essenziali e i Fornitori di servizi digitali."

Ed ancora: "Spetta a loro (gli OSE) l'obbligo di adottare misure tecniche ed organizzative adeguate alla gestione dei rischi e alla prevenzione degli incidenti informatici. La notifica di incidenti con impatto rilevante sui servizi forniti andrà fatta al Computer Security Incident Response Team (CSIRT) e alle Autorità competenti NIS, ossia i vari Ministeri. A questi ultimi è assegnato il compito di vigilare sull'applicazione della direttiva a livello nazionale, ed irrogare sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti."

Il perché della nuova Direttiva

La nuova direttiva NIS2, DIRETTIVA (UE) 2022/2555, licenziata il 14 dicembre 2022, pubblicata sulla Gazzetta ufficiale dell'Unione europea del 27.12.2022 relativa a misure per

un livello comune elevato di cibersicurezza nell'Unione (con modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148) è disponibile a questo link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&from=IT

La Direttiva NIS2 rientra nel piano di miglioramento della precedente NIS (direttiva 2016/1148), a seguito di valutazioni complessive, ed è indirizzata ad aumentare le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità competenti e dell'Unione nel campo della cibersicurezza e della protezione delle Infrastrutture Critiche. Questo anche a causa all'intensificarsi degli attacchi informatici durante la pandemia di COVID-19 che hanno mostrato la vulnerabilità delle organizzazioni che operano in maniera sempre più interdipendente.

Peraltro, la precedente direttiva aveva mostrato alcuni limiti, ulteriormente amplificati dai vari recepimenti nazionali, quali:

- Il limitatissimo numero di soggetti coinvolti dall'attuale direttiva legato ai criteri adottati dai singoli stati, responsabili per l'identificazione dei criteri per qualificare gli operatori di servizi essenziali.
- L'elevata discrezionalità delegata ai singoli Stati nello stabilire i requisiti di sicurezza e di segnalazione di incidenti per gli operatori di servizi essenziali che hanno portato gli Stati membri ad implementare i requisiti in modi significativamente diversi, provocando problemi alle società operanti a livello transnazionale.
- L'inefficacia del regime di vigilanza ed esecuzione della direttiva NIS da parte degli Stati membri che ha portato ad una scarsa applicazione delle sanzioni ai soggetti che omettevano di adottare requisiti di sicurezza o di segnalare incidenti.
- La grande difformità di risorse finanziarie e umane accantonate dagli Stati membri per adempiere ai requisiti richiesti per affrontare i rischi di cibersicurezza, accentuando le differenze in termini di resilienza tra i vari Stati membri.
- La scarsa condivisione delle informazioni tra gli Stati membri che porta conseguenze negative sull'efficacia delle misure di cybersicurezza e sul livello di consapevolezza situazionale comune a livello dell'UE.

Per quanto riguarda l'attuazione pratica: entro il 17 ottobre 2024, gli Stati membri devono recepire la Direttiva NIS2, adottare e pubblicare le misure necessarie per conformarsi alla direttiva NIS2, e devono comunicare immediatamente alla Commissione il testo di tali disposizioni che dovranno essere applicate a decorrere dal 18 ottobre 2024.

Soggetti essenziali e importanti

Dalla nuova direttiva scompaiono gli OSE (Operatori dei Servizi Essenziali) e gli FSD (Fornitori dei Servizi Digitali) e vengono introdotte due nuove tipologie di soggetti: Essenziali e Importanti.

Sono considerati Soggetti Essenziali i seguenti:

a. soggetti indicati nelle tabelle allegate (allegato I) il cui fatturato annuo supera i 50 milioni di EUR oppure il cui totale di bilancio supera i 43 milioni di EUR[1].

b. prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;

c. fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese, ovvero, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio non supera i 43 milioni di EUR[2].

d. i soggetti della pubblica amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale;

e. qualsiasi altro soggetto presente nelle tabelle allegate (allegati I e II) che uno Stato membro identifica come soggetti essenziali, ovvero:
   - il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali
   - il soggetto sia critico in ragione della sua particolare importanza a livello nazionale, regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

f. soggetti identificati come soggetti critici[3];

g. se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali[4]

1 Articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE

2 Articolo 2 dell'allegato della raccomandazione 2003/361/CE

3 Ai sensi della direttiva (UE) 2022/2557

4 A norma della direttiva (UE) 2016/1148 o del diritto nazionale.

Sono invece considerati soggetti importanti i soggetti di una tipologia elencata nelle tabelle allegate (allegati I e II) che non sono considerati soggetti essenziali come indicato del precedentemente. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti, ovvero:

- il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
- il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro

Elenco dei Soggetti essenziali e importanti

Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Successivamente, gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

Ai fini della compilazione dell'elenco, gli Stati membri impongono alle entità indicate di presentare alle autorità competenti almeno le informazioni seguenti:

a. il proprio nome;

b. l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail, le serie di IP e i numeri di telefono;

c. se del caso, i settori e sottosettori pertinenti, vedere tabelle allegate; e

d. se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della presente direttiva.

I soggetti indicati nell'elenco notificano tempestivamente qualsiasi modifica delle informazioni trasmesse e in ogni caso entro due settimane dalla data della modifica.

La Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornisce senza indebito ritardo orientamenti e modelli relativi agli obblighi di cui al presente paragrafo.

Gli Stati membri possono istituire meccanismi nazionali che consentano alle entità di registrarsi.
Entro il 17 aprile 2025 e successivamente ogni due anni, le autorità competenti notificano:

a. alla Commissione e al gruppo di coordinamento, il numero dei soggetti essenziali e importanti presenti nell'elenco per ciascun settore e sottosettore;

b. e alla Commissione informazioni pertinenti sul numero di soggetti essenziali e importanti individuati sul settore e il sottosettore secondo le tabelle allegate (allegato I o II) cui appartengono, sul tipo di servizio che forniscono e sulla tipologia di fornitura, tra quelle stabilite.

Sino al 17 aprile 2025 e su richiesta della Commissione, gli Stati membri possono notificare alla Commissione i nomi dei soggetti essenziali e importanti quali gli istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.

Organi di Gestione e Vigilanza

La Direttiva NIS 2 prevede che siano i membri degli "organi di gestione" dei soggetti interessati alla normativa ad approvare le misure, sovraintendendo alla loro implementazione e corretta attuazione.
In aggiunta a quanto sopra, i soggetti saranno obbligati a notificare all'autorità competente, senza indebito ritardo, eventuali incidenti che abbiano un impatto significativo sulla fornitura dei loro servizi.

In ultimo, si segnala che alla luce della Direttiva NIS 2 gli operatori inclusi potranno essere soggetti ad attività di vigilanza, tra cui ispezioni *in loco* e vigilanza a distanza, nonché *audit* sulla sicurezza periodici e mirati, effettuati da organismi indipendenti o dall'autorità competente.

Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione

Misure di gestione dei rischi di cibersicurezza

Tra le misure di gestione dei rischi di cibersicurezza la nuova normativa identifica:

1. politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
2. gestione degli incidenti;
3. continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
4. sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
5. sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informa-

tici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
6. strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;
7. pratiche di igiene informatica di base e formazione in materia di cibersicurezza;
8. politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
9. sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
10. uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi TIC, sistemi TIC o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, nonché, ove necessario, dei pertinenti portatori di interessi, identifica i servizi TIC, i sistemi TIC o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata del rischio per la sicurezza di cui al paragrafo 1.

Obblighi di Segnalazione

Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi.

Un incidente è considerato significativo se:

a. ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b. si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Gli Stati membri provvedono affinché, ai fini della notifica, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

a. senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi

se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b. senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c. su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d. una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:
   - una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;
   - il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;
   - le misure di attenuazione adottate e in corso;
   - se opportuno, l'impatto transfrontaliero dell'incidente;

e. in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

Sanzioni

Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti essenziali siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti importanti siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

Allegati I e II

ALLEGATO I

SETTORI AD ALTA CRITICITÀ

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio (1) che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio (2)
		— Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944
		— Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio (3)
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio (4)
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio (5)
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE
		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno

Settore	Sottosettore	Tipo di soggetto
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio [6], aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio [7], e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio [8]
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio [9]
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio [10], escluse le singole navi gestite da tale compagnia
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio [11], compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio [12]
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione [13] responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio [14]
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio [15]
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio [16]
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio [17]

Settore	Sottosettore	Tipo di soggetto
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio [18]
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio [19]
		— 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] — 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]
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio [22], ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio [23], escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale
8. Infrastrutture digitali		— Fornitori di punti di interscambio internet
		— Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice
		— Registri dei nomi di dominio di primo livello (TLD)
		— Fornitori di servizi di cloud computing
		— Fornitori di servizi di data center
		— Fornitori di reti di distribuzione dei contenuti (content delivery network)
		— Fornitori di servizi fiduciari
		— Fornitori di reti pubbliche di comunicazione
		— Fornitori di servizi di comunicazione elettronica accessibili al pubblico
9. Gestione dei servizi TIC (business-to-business)		— Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti

Settore	Sottosettore	Tipo di soggetto
10. Pubblica amministrazione		— Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale
		— Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale
11. Spazio		Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

(1) Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (GU L 158 del 14.6.2019, pag. 125).
(2) Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (GU L 158 del 14.6.2019, pag. 54).
(3) Direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili (GU L 328 del 21.12.2018, pag. 82).
(4) Direttiva 2009/119/CE del Consiglio, del 14 settembre 2009, che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (GU L 265 del 9.10.2009, pag. 9).
(5) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
(6) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
(7) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
(8) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
(9) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
(10) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).
(11) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).
(12) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10)
(13) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
(14) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
(15) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).
(16) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).
(17) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
(18) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

(19) Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).
(20) Direttiva 2001/83/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali per uso umano (GU L 311 del 28.11.2001, pag. 67).
(21) Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici (GU L 20 del 31.1.2022, pag. 1).
(22) Direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio del 16 dicembre 2020 concernente la qualità delle acque destinate al consumo umano (GU L 435 del 23.12.2020, pag. 1).
(23) Direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, concernente il trattamento delle acque reflue urbane (GU L 135 del 30.5.1991, pag. 40).

ALLEGATO II

ALTRI SETTORI CRITICI

Settore	Sottosettore	Tipo di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 *bis*), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio [1], escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio [2] e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio [3] che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	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
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2
	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2

Settore	Sottosettore	Tipo di soggetto
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di servizi di social network
7. Ricerca		Organizzazioni di ricerca

(1) Direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, relativa ai rifiuti e che abroga alcune direttive (GU L 312 del 22.11.2008, pag. 3).

(2) Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE (GU L 396 del 30.12.2006, pag. 1).

(3) Regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare (GU L 31 del 1.2.2002, pag. 1).

(4) Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

(5) Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

La Supply Chain come Kill Chain
La sicurezza nell'epoca Zero Trust

[A cura di Salvatore Marcis, Trend Micro Italia]

Zero Trust è un approccio alla sicurezza "sempre e ovunque". Un modello, in contrasto con quelli tradizionali, in cui la sicurezza è presente "in alcuni casi e in alcuni momenti". Questi modelli sono stati un approccio a basso costo e valore elevato, adatti a rendere difficile il lavoro dei cybercriminali ma, in un'epoca di automazione degli attacchi e violazioni delle supply chain, sono diventati inefficaci.

Questo documento si focalizza soprattutto sui seguenti temi:

1. **Igiene dei Dati**. Zero Trust evidenzia le fonti di dati a bassa credibilità, fornendo indicazioni su dove investire per ridurre i costi di automazione e del lavoro. L'igiene dei dati che deriva da Zero Trust riduce i rischi di Contaminazione delle Decisioni (una tipologia di fake news a cui sono esposti sia i dirigenti sia l'AI), e consente di prendere decisioni più accurate con meno dati, riducendo i costi di archiviazione e di elaborazione nel cloud.

2. **Sicurezza della supply chain**. Conoscendo i rischi che corrono le identità delle risorse interne, esterne, umane e dei dispositivi, le supply chain di dati "interni" ed "esterni" possono essere gestite in modo identico e trasparente. Il vantaggio secondario di questo approccio è che l'impiego di identificatori globali comuni (identità federate) ne agevola l'adozione da parte di realtà molto estese (l'interoperabilità risulta più economica quando si utilizzano identificatori comuni) come, per esempio, le Pubbliche Amministrazioni e i relativi fornitori.

3. **Omnichannel e Retail di nuova generazione**. L'omnichannel equivale al concetto di "tutti i canali, un'unica esperienza". I clienti si rapportano con l'azienda nel suo complesso anziché con singoli servizi o uffici specifici. Unendo questi canali, emergono molte opportunità di risparmio ma anche di frodi e attività cybercriminali. Queste falle possono essere protette usando Zero Trust per gli acquisti tradizionali e per l'online shopping da mobile, indipendentemente dal fatto che gli acquisti siano eseguiti da esseri umani attraverso lo smartphone o da automobili autonome in roaming, con una configurazione che soddisfi requisiti di integrità unificati tra reti dati e fatturazione. Questa unità omnichannel può essere utilizzata anche per soddisfare i requisiti di conformità.

Zero Trust può essere pensato come l'opposto dei tradizionali modelli di sicurezza manuale. È un approccio "simil opt-out" anziché "simil opt-in". Nei modelli tradizionali, il rischio di sicurezza enterprise viene assegnato dal personale con un supporto scarso o nullo da parte degli architetti di identità. La registrazione delle identità, l'assegnazione di diritti e

privilegi, la gestione dell'inventario e quella degli incidenti e analisi vengono normalmente effettuate senza alcuna guida da parte del business aziendale, dell'identità, della sicurezza e degli architetti, risultando frammentate. Spesso il personale incaricato di queste funzioni non ha alcuna percezione della rilevanza dal punto di vista del business, del rischio d'impresa o della potenziale perdita di fatturato legata ai poteri che vengono conferiti a queste identità. Quando si attiva un blocco, le funzioni di sicurezza tradizionali lo fanno in linea con un approccio di tipo "best effort", aumentando di fatto il rischio all'interno dell'azienda tanto quanto la possibilità di falsi positivi che possono avere un impatto sui ricavi (come, per esempio, l'abbandono dei carrelli degli acquisti). Questi falsi positivi aumentano o la possibilità di interruzioni della rete di produzione (e altri malfunzionamenti) o la quantità di personale esperto necessario per valutare e risolvere tali casi.

Al contrario, Zero Trust prevede la gestione del rischio di identità e la sua valutazione su base continuativa. Ciò significa che gli insight sulla sicurezza forniti sono molto più precisi rispetto a quelli dei modelli di sicurezza IT tradizionali. Essendo più accurati, possono essere maggiormente automatizzati, con meno lavoro manuale e meno personale a doversene occupare; inoltre, hanno meno probabilità di interrompere i flussi di ricavi. Poiché la fiducia nella precisione dei dati si traduce nella possibilità di aver bisogno di meno dati per arrivare alla medesima decisione, i costi di elaborazione e storage legati al cloud possono essere ridotti. Il metodo di valutazione continuativa always-on di Zero Trust può essere considerato come un modello "simil opt-out" obbligatorio.

Da questa inversione di approccio derivano conseguenze profonde e vantaggi importanti.

Potendo stabilire un contesto di sicurezza sempre e ovunque, la qualità complessiva dei dati e delle relative transazioni (Data Hygiene) è attendibile. Avendo una maggiore consapevolezza dell'integrità aziendale e dei suoi rischi, è possibile assegnare maggiori responsabilità alle funzioni di automazione che vanno slegate dalla supervisione umana, normalmente necessaria per "risolvere", "controllare" e "approvare" le funzioni automatizzate (che in questi casi tornano ovviamente a essere manuali). Di conseguenza aumentando la precisione dei processi automatizzati; la quantità di personale qualificato necessario si riduce, così come lo sforzo che occorre per trovarlo e trattenerlo.

La capacità di assicurare l'Igiene dei Dati si riflette sulla capacità di gestire il rischio di identità su vasta scala. Il rischio di identità è la capacità di determinare che una certa identità (che potrebbe non essere mai stata osservata prima, come nel caso di un nuovo cliente) e i relativi comportamenti abbiano il permesso di effettuare una specifica transazione entro il perimetro di rischio accettato del contesto business. Questi contesti business sono quelli in cui l'azienda considera un rischio accettabile, per esempio un piccolo rischio legato a un grande cliente (un'importante fonte di fatturato). Questa applicazione del rischio di identità nella sicurezza business dimostra che gli insight forniti da Zero Trust sono rilevanti anche

da questo punto di vista e ciò risolve la tradizionale differenza tra il rischio in ottica CISO (Chief Information Security Officer), basato sulla prevenzione, e quello in ottica CRO (Chief Risk Officer), basato sull'enablement dei ricavi. In questo modo, l'applicazione degli insight Zero Trust permette ai CISO di ottenere visibilità a livello del CdA.

In un sistema basato sull'Igiene dei Dati, i costi diminuiscono poiché si immagazzinano e si elaborano meno informazioni ma di qualità superiore. I vantaggi relativi all'igiene dei dati derivano da segnali di identità più precisi (le "storie" dei contesti business), che a loro volta riducono la quantità di informazioni necessarie per prendere decisioni accurate tanto quanto quelle prese con più dati ma meno precisi. Queste decisioni richiedono meno tempo e meno – se non nessuna – supervisione umana. Quando si utilizzano le analisi del rischio Zero Trust, i costi del cloud aziendale si riducono sia per l'elaborazione sia per l'archiviazione; la conseguente riduzione del carico sulla rete rende necessario meno hardware e, di conseguenza, minori spese di capitale.

Disponendo di dati più puliti e rigorosamente controllati si può prevenire una categoria di attacchi altrimenti non rilevabili come la Contaminazione delle Decisioni, ovvero la messa a frutto delle falle nel controllo dei dati ("dati sporchi") per manipolarne i risultati. Esempi sono le frodi, gli attacchi di tipo "low-and-slow" o "boiling-the-frog", la contaminazione delle telemetrie, le truffe delle sottoscrizioni iniziali, gli attacchi roaming, le minacce interne, il rischio di uscita dei dirigenti e altri ancora.

Le decisioni che coinvolgono dati sporchi possono essere manipolate e con un numero sufficiente di dati sporchi persino le decisioni dei CdA possono esserlo in modo quasi impercettibile per anni.

Fra le applicazioni di Zero Trust si trova la mappatura delle superfici di attacco (Attack Surface Mapping, ASM). Questi casi ASM possono essere considerati come uno dei seguenti.

1. Colpiti. In questo caso bisogna calcolare rapidamente l'estensione del danno arrecato dal cyberattacco.
2. Mancati per poco. Cosa avremmo rischiato se fossimo stati colpiti? Dobbiamo aggiungere questa casistica ai nostri piani?
3. Alto impatto. Identificare i primi 10 rischi per cui pianificare appositi investimenti.
4. Previsione. La mappatura proattiva dei rischi per nuove casistiche di business (se facciamo questo, cosa rischieremmo se venissimo colpiti?).
5. Scansione ASM. Di tutte le potenziali superfici di attacco esistenti ora e nel prevedibile futuro, quali sono quelle che dobbiamo monitorare?

La prevenzione della Contaminazione delle Decisioni (se effettuata all'interno di un deployment Zero Trust) può essere applicata a intere classi di business e di abilitatori di

business come mezzo per aumentare le potenzialità di automazione e ridurre i costi del cloud. Al crescere della fiducia nei confronti delle attività di Attack Surface Management è possibile automatizzare, esternalizzare o assegnare in outsourcing ulteriori servizi con conseguenti abbattimenti dei costi. Proteggere le decisioni è uno dei mezzi per rendere sicura la tecnologia emergente chiamata Semantic Computing, che si affida a un'automazione estremamente scalabile e all'intelligenza artificiale operativa. Essendo priva delle capacità di giudizio umane, la AI è ovviamente vulnerabile alle manipolazioni effettuate attraverso la Contaminazione delle Decisioni.

A titolo di esempio, le finalità della prevenzione della Contaminazione delle Decisioni con Zero Trust potrebbero comprendere:

1. sicurezza della supply chain collegata alla gestione del rischio fornitore e/o alle SBOM (Software Bill of Materials) governative
2. Minore manipolazione dei CdA attraverso dati falsificati
3. Partecipazione alle alleanze in ambito Identity Federation e alle partnership per ridurre i costi
4. Effetti del retail di nuova generazione e dell'omnichannel sulla riduzione dei carrelli abbandonati
5. Procurement – Confronto tra fornitori e gare virtuali, consolidamento dei vendor
6. Sovranità dei dati – Regole virtuose per i viaggi transfrontalieri dei veicoli autonomi
7. Telecomunicazioni 6G e Zero Trust
8. Prevenzione e controllo delle frodi elettorali
9. Identità nazionale e servizi federati
10. Sicurezza dei veicoli autonomi e gestione delle flotte

Con l'aumento della complessità dei cyberattacchi sferrati a livello statale o semi-statale e la riduzione dei relativi costi, gruppi di cybercriminali sempre più piccoli saranno in grado di lanciare attacchi di questo tipo dall'interno delle supply chain (chi lavora da casa, per esempio) o fingersi dipendenti di fornitori affidabili. Zero Trust permette di ottenere una visibilità delle superfici di attacco enterprise che consente di visualizzare l'intera portata di un attacco su più fronti.

Una nota per manager e dirigenti

Queste necessità potranno essere risolte adottando Zero Trust all'interno dell'ambiente enterprise. L'approccio Zero Trust è particolarmente adatto per trasformare complessi obblighi di reportistica e compliance in una semplice scheda di valutazione automatizzata combinata con insight molto migliorati.

Quando il management rilascia dichiarazioni rivolte agli azionisti, comprese le dichiarazioni al pubblico, l'accuratezza di tali dichiarazioni deve essere inattaccabile. Storicamente, la

veridicità di queste dichiarazioni si basava sulla qualità della supervisione dei dirigenti e, quindi, sulla fiducia nell'integrità dei dati utilizzati nella redazione dei report.

Tale fiducia è sempre più mal riposta.

Con la crescente complessità delle violazioni della sicurezza dei dati, l'accuratezza dei report finanziari è limitata dalla qualità dei dati su cui si basano, che a sua volta è limitata dalla qualità della sicurezza delle informazioni. Questa sicurezza garantisce l'integrità sia dei dati finanziari sia delle attività che essi cercano di misurare. Garantire questa integrità end-to-end è un tipo di responsabilità esecutiva chiamata "dovere fiduciario" e la sicurezza delle informazioni è un requisito essenziale per poterne rispettare gli obblighi. L'incapacità di assicurare in modo credibile la responsabilità fiduciaria è di per sé una "violazione del dovere fiduciario", considerata in alcuni Paesi come un tipo di frode.

Molti Paesi hanno riconosciuto che questa integrità è legata alla salute economica della loro nazione e, quindi, alla sicurezza nazionale.

Per queste ragioni, l'amministrazione Biden ha costituito un comitato denominato Cyber Safety Review Board composto da senatori ed esponenti del settore privato che ha il compito di verificare le vulnerabilità di sicurezza delle grandi aziende e delle relative leadership. Questo comitato potrebbe essere un esempio da seguire per altri Paesi.

La relazione tra sicurezza della supply chain e sicurezza nazionale ha effetti internazionali ma un impatto nazionale. Un esempio può essere la diffusione di un certo malware a livello mondiale le cui conseguenze sono, tuttavia, sentite soprattutto da particolari aziende e Paesi. I governi hanno iniziato ad affrontare questo problema della supply chain con una combinazione di governance aziendale (basata sugli insight Zero Trust) e di governance della supply chain (anche in questo caso usando Zero Trust per mappare le superfici di attacco). L'architettura Zero Trust è, quindi, il legame esistente tra la responsabilità del management e la sua capacità di muoversi sulla base di una efficace sicurezza della supply chain.

Per affrontare queste problematiche in modo proattivo, il governo statunitense sta usando il proprio potere d'acquisto per far rafforzare le aziende (e i loro prodotti) interessate a diventare fornitrici statali o federali. Il presidente USA Joe Biden ha firmato un ordine esecutivo presidenziale che impone ai fornitori pubblici di disporre di un piano Zero Trust a supporto delle SBOM, un inventario "nested" delle supply chain. Le aziende che non sono in grado di dichiarare la propria compliance Zero Trust né fornire un elenco SBOM delle varie componenti software non possono vendere al governo statunitense né ai suoi fornitori e così via. A partire dalla sede centrale, i fornitori richiederanno ai loro partner di migliorare la loro posizione verso la sicurezza. Poiché le aziende di molti Paesi vendono al governo degli Stati Uniti e ai suoi fornitori, questi requisiti si estendono anche oltre i confini statunitensi.

L'importanza di questo cambiamento è chiara per molti leader mondiali. Il 24 maggio 2022 i leader di Giappone, India, USA e Australia hanno dichiarato la propria adesione a molti di questi principi:

"Per realizzare la vision dei 'Quad Leader' per un'area Indo-Pacifica libera e aperta, ci impegniamo a rafforzare le difese delle infrastrutture critiche delle nostre nazioni condividendo informazioni relative a minacce, identificando e valutando potenziali rischi nelle supply chain di prodotti e servizi digitali e allineando gli standard di base della sicurezza del software per il procurement pubblico facendo leva sul nostro potere collettivo di acquisto per migliorare l'ecosistema dello sviluppo software affinché tutti gli utilizzatori possano beneficiarne".

Imponendo ai fornitori l'implementazione di un piano Zero Trust, l'opportunità di intercettare gli attacchi all'interno di una rete o di una supply chain risulta maggiore e l'impatto della risposta a questi rischi sul business è decisamente inferiore.

In effetti, la capacità degli Executive di affermare di aver fatto un buon lavoro è esplicitamente collegata a una efficace sicurezza delle informazioni lungo tutta la supply chain. Zero Trust è, quindi, un modo per dimostrare il dovere fiduciario nella gestione della supply chain, nella gestione di rete e nella gestione dei fornitori.

A breve la Securities Exchange Commission (SEC) statunitense valuterà una proposta per il controllo e il reporting degli eventi inerenti alla sicurezza delle informazioni da parte dei CdA. La proposta prevede il reporting al CdA da parte di una funzione competente in materia di cybersicurezza, Inoltre, richiede che il consiglio di amministrazione informi gli azionisti in caso di eventi di sicurezza rilevanti entro quattro giorni. Questa comunicazione agli azionisti avrà un effetto inevitabile sul prezzo delle azioni.

Se approvata, la conformità alla proposta della SEC relativa alla rendicontazione in materia di sicurezza avrà effetti giganteschi sui CdA. Il rischio e la strategia di cybersicurezza diventeranno immediatamente argomento per i vertici aziendali con una forte ricerca delle relative competenze. I CISO avranno, quindi, un posto fisso al tavolo, portando le competenze richieste nell'agenda di ogni consiglio di amministrazione.

Queste necessità potranno essere risolte adottando Zero Trust all'interno dell'ambiente enterprise, essendo particolarmente adatto per trasformare complessi obblighi di reporting e compliance in una semplice scheda di valutazione automatizzata corredata da insight profondamente migliorati.

1. Panoramica della strategia

Il presente documento intende esplorare i vari aspetti dell'approccio Zero Trust con uno sguardo al futuro. Mentre altri documenti si concentrano sulla tecnologia in sé, questo è dedicato al suo utilizzo e valore, focalizzandosi sul "perché" piuttosto che sul "come" di Zero Trust. Considerando la natura del testo, questo documento può essere considerato come un contributo di approfondimento da utilizzare nella pianificazione esecutiva più che un'analisi dello stato attuale del settore o una promozione del prodotto.

Buona parte dell'odierna sicurezza dell'informazione si basa su concetti datati. Un approccio innovativo al contenimento dei danni causati alle aziende è Zero Trust, che è un nuovo livello di maturità nella sicurezza delle informazioni vincolando i risultati a un miglior supporto decisionale basato sul rischio e supportato da una Zero Trust Architecture (ZTA). Questo documento propone quattro raccomandazioni.

- Cambiamenti nelle responsabilità esecutive e nella governance dei CdA che rendono necessaria l'adozione di una ZTA
- Nuovi obblighi imposti da governi e clienti per la resilienza delle supply chain mediante ZTA
- Utilizzo di strumenti Zero Trust come l'automazione della gestione dei rischi operativi per facilitare la gestione della sicurezza riducendo sia i rischi enterprise sia il TCO (Total Cost of Ownership) della sicurezza
- Uso dell'effetto di semplificazione che la ZTA produce sulla gestione della sicurezza per ridurre la necessità di personale esperto che può essere difficile da trattenere. A sua volta ciò riduce il gap di competenze permettendo di ricorrere a personale di minor esperienza e/o offshore anche per il triage di incidenti complessi.

Sebbene la maggior parte dei messaggi su Zero Trust lo descriva come un approccio di tipo "mai fidarsi, sempre verificare", una migliore descrizione sarebbe "colpevole fino a prova contraria". Ogni utente, dispositivo e transazione è sempre considerato sospetto. Non esiste un rifugio sicuro nel quale un hacker o un malintenzionato possano nascondersi dai controlli della rete. Non essendoci fiducia in alcun utente, entità, transazione o dispositivo, non esiste un perimetro da violare. Nessun hacker potrà dire "sono dentro" perché non esiste un "dentro".

Al posto dei perimetri, viene usata una valutazione costante del rischio per determinare il ritardo assegnato all'accesso alle risorse (chiamato "friction").

Al massimo rischio corrisponde il blocco.
A un rischio elevato corrisponde un accesso ridotto alle risorse.
A un basso rischio corrisponde un accesso completo ma monitorato.

Vi è, dunque, un grado variabile di rischio; non esiste una situazione di totale fiducia.

A differenza di un ambiente di trust tradizionale, il contesto Zero Trust consente di prendere decisioni di sicurezza più precise rispetto al tradizionale scenario di "blocco/non blocco", in cui la sicurezza è eccessiva o insufficiente. Se implementato correttamente, Zero Trust non ostacola il business ma ne riduce costi e rischi. In questo modo i veri elementi trainanti della sicurezza (denaro e risorse) vengono tutelati.

1.1 Cos'è ZTA?

Zero Trust Architecture (ZTA) è un approccio all'architettura enterprise per l'implementazione di requisiti di business Zero Trust complessi come la gestione operativa del rischio di identità.

Il rischio operativo creato dalla sicurezza può essere ridotto al minimo applicando un contesto di rischio (gli insight sul rischio di Zero Trust) alla risposta di sicurezza.

In genere questo contesto viene applicato mediante il giudizio umano, richiedendo procedure manuali che vanificano le finalità dell'automazione in questo campo. Zero Trust è in grado di correggere questa situazione, migliorando la qualità dei dati utilizzati per la risposta automatizzata. Ciò crea nuove opportunità per il personale di sicurezza, costoso e difficile da assumere, che può così interrompere le attività ripetitive e tornare a svolgere compiti più importanti per l'azienda, che richiedono una valutazione umana.

La combinazione di rilevamento della superficie di attacco, valutazione del rischio e mitigazione del rischio è adoperata per produrre questi insight. Gartner definisce questa combinazione come CAASM (Cyber Asset Attack Surface Management).

Figura 1: *Il ciclo di vita della gestione del rischio*

Questo approccio contestuale alla riduzione del rischio creato dalla sicurezza può abbattere il costo effettivo complessivo della sicurezza stessa, che comprende il costo dei prodotti necessari e il suo impatto su operazioni e ricavi. L'impatto della sicurezza può essere ulteriormente attenuato ricorrendo alla micro-segmentazione per "circoscrivere il raggio d'impatto" della sicurezza come descritto nel successivo paragrafo 1.2.

Applicando la gestione del rischio operativo alla sicurezza è possibile far corrispondere il più possibile lo sforzo di sicurezza al valore dell'asset. Più la risposta di sicurezza equivale al rischio dell'asset, meno sarà il costo (rischio) inutile dell'azione di sicurezza.

1.2 Circoscrivere il raggio d'impatto della risposta di sicurezza

La sicurezza è di per sé un rischio e senza Zero Trust, lavorando in modo tradizionale, ignorando il contesto, genera costi. Per esempio, le funzioni mission-critical, come quelle di una smart factory, potrebbero essere interrotte a causa di una sicurezza non-Zero Trust con un impatto diretto di milioni di dollari al minuto. Un altro esempio potrebbero essere reti ospedaliere o di telecomunicazione, bloccate da una sicurezza non-Zero Trust, con un impatto immediato sulle vite umane.

Quando il contesto di sicurezza di Zero Trust viene riconosciuto e vi si risponde, il risultato dell'azione di sicurezza è molto più accurato e risponde alle esigenze del business, come i ricavi, la sicurezza della vita e/o la sicurezza della missione. Questo significa che, aggiungendo le priorità relative al rischio aziendale a sistemi in grado di gestire il rischio di sicurezza come Zero Trust, si riduce effettivamente il rischio aziendale attraverso la riduzione del rischio di sicurezza. Si tratta di un profondo miglioramento rispetto ai modelli di sicurezza tradizionali.

Ciò può essere automatizzato traducendo gli algoritmi dei processi aziendale in algoritmi di processi della sicurezza come l'applicazione delle policy. Il contesto di business diventa, quindi, il contesto di sicurezza. L'impatto sui ricavi (cfr. il successivo paragrafo 1.3) può essere, dunque, integrato nella risposta di sicurezza, per esempio attivando una risposta di "blocco" quando c'è un basso impatto sui ricavi e una di "monitoraggio" quando ha un impatto elevato sui ricavi.

Grazie alla possibilità di integrare le priorità di business nelle risposte di sicurezza, i sistemi di sicurezza tradizionalmente ad alto rischio smettono di essere fonte di costo diventandone fonte di riduzione.

1.3 Granularità della risposta e riduzione dell'impatto della sicurezza sul business

Una sicurezza imprecisa o esagerata è di per sé un rischio e la riduzione della portata di una risposta di sicurezza efficace ne riduce le conseguenze negative. Rendendo la risposta di sicurezza il più accurata e il più possibile "calibrata" sullo specifico contesto di sicurezza dell'incidente, si riduce il costo dell'impatto sui ricavi della sicurezza (in termini di blocco e di interruzioni generate dalla sicurezza). L'impatto della sicurezza sull'azienda si riduce.

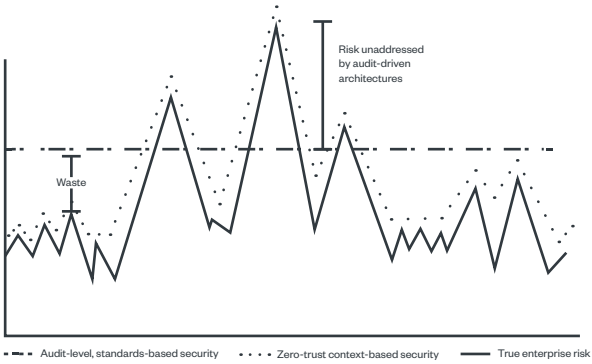


Figura 2: *Zero Trust è un mezzo per applicare il contesto (rischio) alla sicurezza informatica tradizionale.*

Quando la telemetria su cui si basa la risposta all'incidente viene resa più precisa attraverso insight basati sul contesto, inoltre, la risposta è più rapida e si risolve prima con una riduzione complessiva dell'impatto totale sul business.

I costi possono essere ulteriormente ridotti per mezzo della micro-perimetrazione, un altro modo per limitare la diffusione degli incidenti di sicurezza.

1.4 La sicurezza come elemento abilitante del business

Usando il contesto per adattarsi al rischio effettivo in tempo quasi reale, la posizione in termini di sicurezza di un'azienda può reagire dinamicamente a singoli rischi su vasta scala (come quelli inerenti alla supply chain) e ridurre le conseguenze di numerose minacce con effetti simili (gestendo i rischi anziché le vulnerabilità). Questo approccio al rischio basato sul contesto consente anche approcci innovativi per riduzione dei costi, come la gestione del rischio di frode su vasta scala attraverso domini tecnici differenti, la gestione del rischio regolatorio tra giurisdizioni differenti (come la privacy e la sovranità dei dati) e persino la gestione dei rischi locali determinati dalle reti wireless (come il roaming e le reti nomadi).

La combinazione di questi approcci può evolvere in casi di utilizzo per i quali la sicurezza

riduce il rischio legato alle supply chain (SBOM), riduce i costi di gestione dei fornitori e affronta i costi strategici della loro proliferazione. Inoltre, i miglioramenti che Zero Trust apporta sugli inventari degli asset accelera la risposta agli incidenti attenuando l'impatto di eventuali violazioni della sicurezza.

2. Come Zero Trust aiuta le aziende

Zero Trust è un modo per identificare ed eliminare la shadow IT e altre inefficienze. È un modo per ridurre i costi (sia operativi sia di capitale) e, quindi, il rischio aziendale. Pulisce i dati aziendali (igiene dei dati) individuando i sistemi che producono un rischio di dati superiore alla media. Consente di incrementare i ricavi riducendo i rischi di interruzioni di servizio che compromettono il brand e i clienti, come il blocco di funzioni customer-critical quali i robot di Operational Technology presenti nelle fabbriche. Consente un controllo puntuale e dettagliato su elementi come roaming e sovranità dei dati.

Zero Trust consente a più funzioni aziendali di utilizzare un unico metodo di accesso, migliorando la sicurezza e rendendo più semplici gli acquisti da parte dei clienti. Zero Trust può essere sfruttato per molte altre casistiche, alcune delle quali sono riportate in appendice a questo documento.

2.1 Perché mappare la superficie di attacco è importante per proteggere la supply chain

Zero Trust può essere considerato un mezzo per identificare le catene di vulnerabilità dell'azienda che hanno un impatto sui ricavi. Alcune di esse possono sembrare poco impattanti se considerate da sole ma in realtà hanno un effetto valanga sul resto della supply chain che potrebbe portare a un Cascade Failure (una cosa rompe l'altra, a catena). Queste catene possono essere processi aziendali (che rappresentano fatturato e, quindi, impatto sul business), processi di sicurezza (che sono rischio e protezione) e supply chain (rischio e fatturato). L'insieme di tutte queste catene è chiamata superficie di attacco.

Figura 3: *La superficie di attacco digitale*

Nel corso di recenti violazioni globali ad alto impatto, la value chain (che genera ricavi) e la kill chain (che genera rischio) sono spesso identiche. Le supply chain coinvolgono fornitori e processi e le kill chain rappresentano le loro rispettive supply chain. Una gestione efficace delle supply chain mediante Zero Trust è un grande passo avanti verso l'identificazione e la neutralizzazione proattiva delle potenziali kill chain. Conformarsi alla versione NSA-DISA (National Security Agency - Defense Information Systems Agency) di Zero Trust a supporto di una SBOM permette di progredire in questa direzione: non solo è possibile identificare i rischi potenziali delle superfici di attacco ma anche l'effetto dei mancati cyberattacchi.

Il Parlamento Europeo definisce come cyberattacco "mancato" un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o che avrebbe potuto provocare un danno ma che è stato bloccato evitandone l'impatto negativo.

Un approccio completo alla gestione delle supply chain come kill chain è Cyber Asset Attack Surface Mapping (CAASM), che permette di identificare e mitigare a priori gli attacchi effettivi, potenziali e "mancati" ("Kill Chain Mapping").

2.2 Gli attacchi alle supply chain "mancati" e non

Falle impreviste nelle supply chain (di dati o di beni) hanno, in genere, un impatto sui ricavi. Possono essere supply chain di dati, tra cui la connettività a reti o applicazioni. Ridurre il rischio in una rete attiva, rilevare i cyberattacchi "mancati", far entrare in una supply chain prodotti a basso rischio o identificare il rischio in una supply chain esistente sono tutti casi d'uso di Zero Trust che attraversano il perimetro di sicurezza aziendale. (In appendice ulteriori esempi).

Esempi di attacchi alle supply chain sono disponibili nella pagina di MITRE ATT&CK® dedicata alla "Violazione delle supply chain", che recita: "Gli autori degli attacchi potrebbero manipolare le dipendenze software e i tool di sviluppo prima che siano ricevuti dal consumatore finale allo scopo di compromettere dati o sistemi". La pagina "Violazione delle supply chain: compromissione delle dipendenze software e dei tool di sviluppo" aggiunge: "Per funzionare correttamente, le applicazioni dipendono spesso da software esterni. I progetti open source più diffusi, usati come dipendenze in molte applicazioni potrebbero essere colpiti per veicolare codice dannoso verso gli utenti di tali dipendenze". Inoltre, "Il codice pericoloso potrebbe essere rivolto specificamente contro un certo target oppure essere distribuito ai consumatori in generale ma in grado di attivare ulteriori tattiche in presenza di vittime specifiche".

Esempi di attacchi alle supply chain digitali sono Cryptolocker, Petya/NotPetya, SolarWinds e, più di recente, Log4J. Per loro natura questi attacchi compromettono il modello di business dell'azienda colpita e possono costare decine di milioni di dollari all'ora.

Nei deployment Zero Trust avviene una verifica costante dell'inventario degli asset di dati rispetto alle minacce conosciute e a quelle emergenti. A ogni sovrapposizione (per esempio con CVE, Common Vulnerabilities and Exposures, note o emergenti) scatta un allarme. Questa verifica costante può identificare immediatamente la presenza all'interno dell'infrastruttura di moduli esterni ad alto rischio, una volta che il rischio è noto. Si può, quindi, intervenire per eliminare il rischio da tali moduli o prendere decisioni basate sul contesto come l'accettazione del rischio, il throttling dei moduli, l'analisi investigativa o il monitoraggio di intelligence,o altre scelte che salvaguardino la produzione dei ricavi e che le opzioni diverse da Zero Trust non possono offrire.

2.3 L'ordine esecutivo di Biden: Zero Trust e le SBOM

L'amministrazione Biden ha recentemente emanato un ordine esecutivo presidenziale a cui sono stati successivamente aggiunti nuovi obblighi e che si prevede venga ulteriormente aggiornato per innalzare il minimo comune denominatore della sicurezza all'interno della pubblica amministrazione statunitense.

Poiché la macchina federale statunitense deve far rispettare questi obblighi ai fornitori, questi a loro volta dovranno girarli ai rispettivi subfornitori diffondendo il requisito di Zero Trust e SBOM lungo tutta la parte di supply chain che riguarda gli Stati Uniti.

Imponendo ai fornitori di disporre di un piano Zero Trust, l'opportunità di rilevare gli attacchi all'interno di una rete o di una supply chain è maggiore, mentre l'impatto della risposta a questi rischi sul business è minore.

In effetti, la possibilità del management di dichiarare un buon operato è espressamente collegata a una efficace sicurezza delle informazioni lungo tutta la supply chain. Zero Trust nella gestione della supply chain, nella gestione di rete e nella gestione dei fornitori è, quindi, uno strumento per dimostrare il dovere fiduciario.

2.4 Le SBOM, o Software Bill of Materials

Una Software Bill of Materials è un inventario "nested" di tutti i prodotti software e relativi componenti e fornitori presenti all'interno dell'azienda. L'intento dell'ordine esecutivo di Biden è che i produttori forniscano queste informazioni ai loro clienti affinché questi ultimi possano includerle nei tool che correlano le vulnerabilità con i componenti della supply chain a rischio. Questo inventario può essere, quindi, confrontato con le vulnerabilità conosciute e con quelle emergenti per comunicare il livello di rischio esistente su tutti i sistemi di un'azienda.

Quando si rileva uno schema di attività potenzialmente nocivo, la sua identificazione è basata in parte sulla conoscenza delle differenze tra quel che dovrebbe succedere alle informazioni e al software in inventario e quello che invece succede effettivamente.

Per poter far ciò rapidamente, occorre avere un inventario di tutte le SBOM di tutti gli asset software presenti in azienda, siano essi realizzati internamente o da fornitori esterni. Dal momento che potrebbero esserci fornitori che erogano parte dei servizi enterprise, questo inventario deve contenere riferimenti ai componenti, ai prodotti e ai servizi dei singoli fornitori.

Questo inventario (chiamato anche indice dei componenti) è prezioso per chi deve rispondere agli incidenti, poiché può includere informazioni di contatto, livelli di esposizione dei vari sistemi e dati utili per creare una mappatura del rischio rappresentata dalla presenza di componenti violati o violabili. Quando queste informazioni non sono prontamente disponibili, il tempo necessario per procurarle estende la durata, il costo, l'impatto e il rischio di un incidente.

Una gestione efficace del rischio in ambienti multivendor con molteplici profili di rischio non è praticabile da eseguire manualmente su scala. Questo, in combinazione con l'obsolescenza e il patching dei componenti e i crescenti investimenti di tempo da parte degli hacker, rende necessario un sistema automatizzato per la gestione del rischio come Zero Trust.

2.5 Zero Trust negli USA – DISA NSA vs. NIST

Esistono diversi approcci a Zero Trust, uno dei quali è descritto dal NIST e un altro dalla DISA NSA Zero Trust Reference Architecture.

C'è una relazione tra la storia e il background di Zero Trust e le relative linee guida recentemente stilate. Le linee guida pubblicate dal NIST sono state rapidamente adottate su molti prodotti con svariati gradi di successo. Da allora l'amministrazione Biden ha emanato un ordine presidenziale che obbliga i fornitori del governo federale statunitense a possedere un piano Zero Trust. In seguito, è stato chiarito che tale piano debba essere conforme con la DISA-NSA Zero Trust Reference Architecture, un documento che descrive una sicurezza data-centric matura. I due diversi approcci rispondono a differenti requisiti di sicurezza infrastrutturale e rischio di business. L'approccio DISA NSA è più indicato per le grandi infrastrutture critiche, mentre l'approccio NIST è più adatto per innalzare il livello di sicurezza dei soggetti che si trovano ancora all'inizio del percorso di maturazione della loro sicurezza.

L'approccio NIST è un eccellente punto di partenza. L'approccio DISA-NSA è un design complementare che aumenta la precisione della gestione del rischio Zero Trust riducendo il costo dell'infrastruttura.

2.6 L'esigenza di armonizzare Zero Trust in USA, Giappone, Australia e India

I fattori comuni alla base dell'approccio Zero Trust NSA-DISA trovano eco nei leader di molti Paesi. Il 24 maggio 2022 quelli di quattro nazioni in particolare – il primo ministro australiano Anthony Albanese, il primo ministro indiano Narendra Modi, il primo ministro

giapponese Fumio Kishida e il presidente statunitense Joe Biden – hanno rilasciato il seguente comunicato congiunto:

"...Rafforzare le difese delle infrastrutture critiche delle nostre nazioni condividendo informazioni relative a minacce, identificando e valutando potenziali rischi nelle supply chain di prodotti e servizi digitali e allineando gli standard di base della sicurezza del software per il procurement pubblico, facendo leva sul nostro potere collettivo di acquisto per migliorare l'ecosistema dello sviluppo software in generale affinché tutti gli utilizzatori possano beneficiarne".

Se un approccio nordamericano a ZTA enfatizza l'integrità della supply chain dei dati (assegnando doveri e responsabilità), l'approccio giapponese sembra incentrato sulla riduzione delle conseguenze degli incidenti (riduzione dell'impatto). La micro-segmentazione è un modo per "ridurre il raggio d'impatto" degli eventi di sicurezza in segmenti più piccoli. Chiamato anche micro-perimetrizzazione, è un modo per ridurre i rischi riducendo la diffusione delle infezioni (nel caso di malware) o il movimento laterale (nel caso di hacker). È ancora presto per dire se l'approccio giapponese possa allinearsi a quello americano dopo il vertice di cui sopra.

2.7 La protezione della supply chain nell'Unione Europea

Nell'Unione Europea cresce il supporto legislativo all'adozione di Zero Trust. Secondo una proposta, una solida gestione della sicurezza IT, l'impegno ad adottare un'architettura Zero Trust e il rafforzamento dei programmi per la sensibilizzazione del personale sulla cybersicurezza aumenteranno la resilienza nei confronti delle cyberminacce. Occorre, inoltre, spingere due policy: una per promuovere la cybersecurity per gli esperti in materia (PMI), considerare le loro esigenze e fornire loro orientamento e supporto, comprese le linee guida per affrontare i problemi della Supply Chain. L'altra deve promuovere la "cyber igiene" per definire un "insieme base di pratiche e controlli".

Questi tre elementi sono in linea con la dichiarazione congiunta ricordata sopra e dell'approccio ZTA NSA-DISA.

2.8 La Cina e la legislazione sulla protezione delle supply chain

La Cyberspace Administration of China (CAC) ha pubblicato la bozza di un accordo per il trasferimento transfrontaliero dei dati denominato SCC. Questo documento si sovrappone per effetti (ma non ambiti) agli altri temi di Zero Trust richiamati in questo documento. In effetti, molti aspetti nazionali della legislazione Zero Trust non riguardano la sicurezza delle supply chain quanto quella della privacy. Si tratta di un approccio diverso dal solito dal momento che i programmi cinesi per il deployment della sicurezza nazionale attraverso un programma nazionale di identità sono ormai maturi.

Implementando su scala nazionale una versione della sicurezza delle supply chain profondamente basata sull'identità, l'attivazione del programma nazionale di identità da parte della Cina può essere usato come un'applicazione di Zero trust estremamente dinamica e versatile.

Un approccio unificato USA, NSA, DISA e SBOM è estremamente centralizzato e può tagliar fuori rapidamente dalle supply chain statunitensi tutti i fornitori di un certo Paese. L'approccio cinese, fortemente dipendente da identità, sidechain e schede SIM (Subscriber Identity Module), è un modo alternativo per proteggere la supply chain che potrebbe essere decisamente più facile ed efficace rispetto a quello statunitense. Si potrebbe obiettare che l'intera supply chain in 5G/6G ha più elementi in comune con una botnet in rapida evoluzione che non con un tradizionale approccio alla sicurezza delle supply chain basato su elenchi. Gli attacchi automatizzati contro le supply chain possono sconfiggere l'approccio USA NSA DISA essendo più veloci rispetto alla catena di approvazioni burocratiche necessarie per bloccare un attacco estremamente dinamico.

2.9 La complessità come rischio di sicurezza

La complessità è un tipo di caos. Uno dei temi centrali del rischio della supply chain è che il management sperimenta uno o più dei seguenti rischi: proliferazione delle architetture, proliferazione dei fornitori, debito tecnico e dipendenze sconosciute nella supply chain stessa. Ciascuna di queste classi di inefficienza aumenta la complessità di un deployment di tecnologia legata alla generazione dei ricavi e, di conseguenza, la possibilità di violazioni provocate da una difformità nell'applicazione dei controlli sull'architettura di sicurezza. Queste inefficienze sono una sorta di "rumore".

Se un'organizzazione fa abbastanza "rumore" di questo tipo, attirerà sicuramente dei "predatori".

Ciascuno di questi elementi può essere corretto da un deployment Zero Trust maturo. Ogni elemento presenta però alcune sfumature che meritano ulteriori spiegazioni.

Proliferazione delle architetture e debito tecnico

La proliferazione delle architetture equivale al concetto per cui la pianificazione diventa sempre meno rigorosa quanto più un sistema si allontana dalla pianificazione e dal controllo centrale in termini di tempo, spazio, logica, gerarchia business o altre dimensioni. Ciò significa che le capacità di riduzione dei costi dell'architettura enterprise diventano sempre meno efficaci (più costose) meno vengono applicate. Il debito tecnico è un concetto correlato, nel quale le attività di pianificazione vengono "rimandate a domani", a indicare che il lavoro necessario per risolvere un problema architetturale diviene sempre più complesso e costoso più lungo è il tempo che trascorre prima che sia risolto. ZTA evidenzia questi rischi

attirando l'attenzione verso le aree di rischio omogeneo all'interno dell'azienda.

Proliferazione dei fornitori e dipendenze sconosciute nella supply chain

Esiste un altro concetto correlato nel quale più fornitori devono gestire i propri costi e la propria complessità, cosa che alcuni, o tutti, potrebbero fare in modo efficace ma difficilmente coordinandosi a vicenda (il cliente non ha idea di quel che succede all'interno di ogni singolo fornitore). La proliferazione dei fornitori è amplificata da quella delle architetture e dal debito tecnico. La conseguenza è che l'architettura di sicurezza viene rispettata in modo disomogeneo dai vari fornitori. Con una gestione disordinata del rischio di sicurezza dei fornitori si rimane all'oscuro anche dei rischi e delle dipendenze della supply chain. Lo prova il fatto che, combinando ZTA e SBOM, i fornitori ad alto rischio emergono ripetutamente nei report di rischio ZTA in conseguenza dei report SBOM.

Proliferazione delle identità e contaminazione della supply chain

Quello dell'identità è un argomento complesso che molte aziende faticano a gestire, in parte perché il termine "identità" viene spesso usato all'interno di un'azienda in modo impreciso o disomogeneo. Quando l'identità è gestita bene, può rendere molto meno costose le stesse funzioni agendo da filtro per ridurre i volumi (e le tipologie) di dati occorrenti per poter prendere decisioni altamente automatizzate.

Quando si tratta di identità, meno è meglio.

Con un'architettura dati enterprise per l'identità ben funzionante, l'igiene dei dati dell'azienda migliora, il volume totale dei dati immagazzinati ed elaborati dall'azienda si riduce e i costi operativi legati allo storage e all'elaborazione cloud diminuiscono. Quando l'identità non è definita a livello di pianificazione dell'architettura enterprise o di quella business, l'azienda avrà bisogno di quantità assai superiori di dati, elaborazione e valutazioni umane per arrivare alle stesse decisioni. Queste ultime saranno probabilmente meno precise poiché le difformità nel design dell'identità (proliferazione delle identità) permettono a sistemi differenti di applicare significati diversi agli stessi identificatori. Quando all'interno di un sistema si applicano significati diversi al medesimo identificatore, si dice che il sistema soffre di contaminazione semantica, problema che riduce la qualità dei dati dell'intero sistema e di tutti gli altri che da esso dipendono.

Un esempio di tutto ciò può essere Customer_Date, un apparentemente semplice identificatore usato a livello di applicazione. In un'azienda con poca igiene dei dati di identità (molti dati di identità "sporchi"), questo può avere significati diversi come mostrato di seguito. Se tutti questi significati vengono inseriti nel medesimo sistema, sarà difficile interpretare la quantità di contaminazione semantica nei risultati prodotti dal sistema stesso.

System type	Identifier	"Dirty" meaning	Consequence
System One (Retail billing system)	Customer_Date	The day of customer onboarding	No indication of current value as a customer
System Two (Retail marketing communications system)	Customer_Date	Day marketing mailout sent (instances of the same customer across multiple campaigns)	There are multiple instances that could be used in decision support — One? Some? None?
System Three (Corporate security fraud department)	Customer_Date	The day the customer was permanently blocked for performing massive fraud	Potential for decisions weighted toward high-risk and criminal customers

Tabella 1: *Differenti tipologie di sistemi con identificatore Customer_Date e relativo significato*

Identificatori come Customer_ID, Customer_Address, System_ID, Phone_Number e altre fonti ancora possono portare a una contaminazione delle decisioni quando un qualsiasi sistema dovesse essere dotato di una scarsa igiene dei dati e le sue informazioni dovessero fluire all'interno di un sistema comune.

Le conseguenze di questa contaminazione semantica possono ripercuotersi su tutti i sistemi dipendenti a valle nella supply chain dei dati sia interna sia esterna.

I miglioramenti apportati ai dati in una Zero Trust Architecture comprendono l'armonizzazione e la federazione delle identità e dei componenti di identità, il che comporta la garanzia che tutti i componenti di identità e relativi identificatori condividano il medesimo significato su ogni sistema (federazione delle identità e integrità semantica).

Contaminazione delle decisioni e igiene dei dati Zero Trust

Se la contaminazione semantica si verifica in sistemi usati per il supporto decisionale, le decisioni stesse vengono contaminate. Questa è una fonte di inefficienza, di ostacolo all'automazione e di cattivo giudizio per il management che deve basarsi su dati inesatti. La situazione può essere, inoltre, manipolata a fini illeciti da una serie di attacchi a contaminazione dei dati come frodi, violazione dei processi di business e attacchi di tipo "low-and-slow" o "boiling-the-frog".

L'adozione di una Zero Trust Architecture tende a migliorare l'igiene dei dati di un'azienda. Dati di alta qualità sono valutati in modo approfondito e filtrati prima di essere introdotti in un sistema. I controlli non riguardano solo il formato ma anche la garanzia che gli identificatori dei campi di dati abbiano il medesimo significato semantico. Questo è un elemento critico per poter supportare decisioni accurate.

Tutte le decisioni prese usando "dati sporchi" conducono a un supporto decisionale carente e a risultati disomogenei.

2.10 Miglioramenti all'identità e Zero Trust

2.10.1 Mantenere il contesto attraverso reti inattendibili

Zero Trust (specialmente la definizione che ne fa la DISA) si basa su una profonda comprensione delle identità. La definizione DISA di Zero Trust è alla radice dell'ordine esecutivo di Biden riguardante Zero Trust e la sicurezza delle supply chain (SBOM); ciò comprende la capacità di mantenere il contesto di sicurezza anche attraverso reti inattendibili, come quando un'autovettura o un telefono si spostano da una rete all'altra (roaming), quando un laptop si collega a un Wi-Fi sconosciuto ("rete nomade"), o quando arriva un nuovo cliente (omnichannel senza perimetro). Allinearsi a questo requisito rende l'interazione da parte del cliente relativamente priva di frizioni, facilitando la possibilità di acquisire e monetizzare nuovi clienti. Per questo motivo Zero Trust è un elemento basilare delle telecomunicazioni 6G.

Le compagnie di telecomunicazione e gli enti pubblici hanno forti esigenze di protezione end-to-end e, allo stesso tempo, coerente di Dati, Asset, Applicazioni e Servizi (DAAS) in grado di poter affrontare attacchi sferrati da avversari operanti a livello statale o semi-statale. La versione DISA-NSA di Zero Trust è la risposta all'arrivo di una nuova generazione di attacchi APT (Advanced Persistent Threat) da parte di attori statali lanciati contro i dati delle supply chain interne ed esterne al fine di evitare l'attraversamento dei perimetri di sistemi protetti da allarmi. Zero Trust, quando implementato in questo modo, può, quindi, intercettare le violazioni ai processi di business per cui gli operatori dell'intelligence sono famosi. Altre tipologie di deployment Zero Trust come gli approcci application-centric comunemente reperibili oggi sul mercato non possiedono la comprensione approfondita delle identità operazionalizzate necessaria per poter fare lo stesso.

2.10.2 Far leva sulle alleanze tra federazioni di identità e sulle partnership per la riduzione dei costi

Il concetto di federazione di identità come definito da una fonte come la FIDO2 Alliance è un'opzione molto interessante. La capacità di armonizzare le identità di soggetti enterprise e non-enterprise, di soggetti interni e fornitori esterni, di iscritti noti e ignoti e di dipendenti on-site e off-site è notevole. Inoltre, dal momento che FIDO2 viene usata da numerose aziende, il ricorso a questa opzione armonizza le identità non solo tra i sistemi dell'azienda ma anche con quelli dei potenziali clienti che siano a propria volta armonizzati su FIDO2. Questa federazione di aderenti a FIDO2 nelle rispettive supply chain ne riduce i costi. Chi usa FIDO2 rende le proprie identità portabili e interoperabili con i sistemi di altri aderenti all'alleanza, proponendosi come un partner o un fornitore ancora più affidabile. L'adesione a FIDO2 può, dunque, diventare un fattore di abilitazione del business.

2.10.3 Omnichannel, reti senza perimetro e riduzione dei carrelli abbandonati

A causa di costi e scalabilità, si sta diffondendo l'adozione di diversi approcci alla sicurezza dei clienti. Le due tipologie sono l'omnichannel (riuso dei sistemi e dell'interfaccia con il cliente) e le reti senza perimetro (acquisizione del cliente quasi senza frizioni).

Combinando questi due approcci in un ambiente Zero Trust, si ottiene l'effetto di ridurre l'abbandono dei carrelli degli acquisti, una importante fonte di rischio in tutto il retail, dai negozi online fino alle applicazioni per la stipula di mutui online.

Abbandono dei carrelli

L'abbandono dei carrelli riguarda la funzione retail che permette di raggruppare gli acquisti prima di procedere al pagamento. Nel caso dei nuovi clienti (probabilmente la miglior tipologia di cliente), una fonte di abbandono dei carrelli deriva dalla frustrazione che l'utente prova dopo aver dedicato del tempo ad assemblare l'ordine (riempire il carrello) e poi essere sottoposto a un processo di iscrizione lungo e macchinoso.

Il retail di nuova generazione e l'omnichannel

Con l'adozione dei principi omnichannel (a cui Zero Trust è completamente allineato), l'iscrizione può essere effettuata una sola volta per tutti i prodotti e servizi forniti dall'azienda. Poiché gli identificatori comuni dell'omnichannel e di Zero Trust sono condivisi e armonizzati (federati), la prima iscrizione effettuata dal cliente per un singolo servizio ha effetti su tutti gli altri servizi. Ciò funziona egregiamente in combinazione con il concetto delle reti senza perimetro.

Reti senza perimetro

Nell'omnichannel esiste il concetto di iscrizione una tantum. Nelle reti senza perimetro, la sorveglianza basata sul rischio di identità può essere combinata con il rischio derivante dalle tentate attività della persona che ha completato l'iscrizione e con la quantità di sorveglianza già svolta in precedenza (la reputazione effettiva di quella persona).

Nel caso di una persona che abbia già completato l'iscrizione e che intenda acquistare gli stessi prodotti a basso rischio (generi alimentari, per esempio) dallo stesso dispositivo, stesso luogo, con lo stesso indirizzo di consegna e con gli stessi dati di fatturazione, chiedere di digitare una password apporta un vantaggio trascurabile, se non per l'integrità della transazione. Se la stessa persona (di cui si possiedono le stesse informazioni) cerca di acquistare anche un tagliaerba (da consegnare sempre allo stesso indirizzo), la procedura potrebbe richiedere solamente di aggiungere una foto dell'avvenuta consegna scattata dal corriere solamente per definire il momento temporale della consegna stessa.

Questo ulteriore passaggio non serve a ridurre il rischio rappresentato dal cliente, bensì quello rappresentato dalla procedura di consegna. Il cliente in questo caso non ha alcun incentivo ad abbandonare il carrello perché, dal suo punto di vista, l'iscrizione è sempre trasparentemente identica anche se il valore dell'acquisto è di tre o quattro volte superiore.

Riducendo la probabilità di abbandono dei carrelli, evento che produce un rischio, il rischio complessivo della transazione scende fino al punto in cui un costoso tagliaerba può essere consegnato in modo del tutto trasparente. I maggiori ricavi totali della transazione e i maggiori ricavi medi complessivi su tutti i clienti sono il punto vincente del retail di nuova generazione basato su Zero Trust.

2.11 Zero Trust come registro interno

Zero Trust presenta diversi aspetti interessanti. In qualità di registro interno dei componenti software può agire da "fonte esclusiva di verità" per gestire l'integrità dell'intero deployment software di un'azienda. Si tratta di un metodo eccellente per rilevare i casi di shadow IT e ottenere insight di rischio Zero Trust sull'efficacia (e, quindi, sulla convenienza economica) del deployment software dell'azienda.

La complessità organizzativa e il rischio che essa rappresenta possono essere mappati con un registro Software ID (SWID) collegato, sotto forma di contesto di sicurezza, ai relativi rischi di sicurezza e rischi di supply chain. Tale contesto può essere descritto come insight sui rischi di sicurezza.

Gli insight sui rischi di sicurezza basati sul contesto possono essere usati per ridurre notevolmente l'impatto negativo dei controlli di sicurezza ostacolanti.

I sistemi sviluppati internamente possono essere una fonte di rischio all'aumentare dei relativi costi di supporto e dell'obsolescenza. Il report di rischio Zero Trust può essere usato per rilevare e segnalare un rischio inaccettabile producendo elenchi prioritizzati dei prodotti di sicurezza in ordine di efficacia, oltre che identificando i relativi fornitori su cui poter impostare azioni di consolidamento.

2.12 Il registro dei fornitori SBOM e la conformità normativa

Sistemi Zero Trust verificabili e affidabili possono fornire facilmente una prova di conformità rispetto a SBOM, normative di sicurezza e/o controlli di auditing verticali come PCI-DSS (Payment Card Industry Data Security Standard). Sistemi sviluppati esternamente (compresi quelli di sicurezza) possono essere evidenziati come fonti di rischio ma, quando si tratta di prodotti forniti da vendor, il rischio può essere suddiviso per fornitore. L'approccio al rischio di sicurezza dei fornitori identifica il rischio rappresentato da ciascun vendor di prodotti di sicurezza e ne facilita il confronto per identificare quello più efficace.

La tecnologia dedicata alle normative regolamentari (RegTech) è un'area emergente di grande interesse. Più è grande l'organizzazione, più è probabile che sia rigidamente controllata e regolamentata. La capacità di trattare il rischio di supply chain e il rischio regolamentare come rischi di sicurezza rilevabili è un modo eccellente per ridurre la possibilità di sanzioni milionarie, eccezioni di auditing (fallimenti) che possono impattare sui contratti in essere e violazioni alla sovranità dei dati. Le norme applicabili previste da standard, regolamenti e leggi vengono effettivamente trasformate in requisiti di sicurezza rilevabili.
Una nota importante: un report condivisibile che possa agire da prova riduce enormemente il lavoro di auditing e compliance, oltre alle possibilità che i revisori giungano a risultati imprevedibili dopo aver parlato magari con l'ultimo neoassunto. L'uso di report omogenei aiuta l'azienda ad avviare il processo di auditing con fiducia nel risultato.

2.13 La gestione del rischio fornitore e il registro dei fornitori SBOM

Quando si confrontano fornitori di prodotti di sicurezza mediante gli insight di rischio Zero Trust, il vendor meno efficace all'interno di una certa tipologia di prodotto può essere identificato e sostituito con quello più efficace. In questo modo non solo si riduce il rischio di sicurezza enterprise (ottenendo risultati migliori) ma si possono acquistare superiori volumi di licenze da un numero inferiore di fornitori (consolidamento). Questo approccio al consolidamento basato su sconti in blocco ("bulk discount") riduce il rischio totale della sicurezza aziendale, limitando al contempo la complessità e i costi.

3. La gestione del rischio delle identità di macchine ed esseri umani

Il contesto di sicurezza Zero Trust applica una risposta di sicurezza sulla base del rischio. Questa risposta è un approccio molto più business-friendly e pertinente per le aziende riducendo l'impatto negativo che le risposte di sicurezza tradizionali producono sul business.

Tutte le funzioni di sicurezza si riducono a una questione di identità. "Chi ha fatto cosa a cosa, quando" è un enunciato di sicurezza generico che comprende non meno di quattro proposizioni di identità. La precisione e l'integrità dell'intero enunciato dipendono dalla precisione e dall'integrità delle singole proposizioni che lo compongono. La precisione e l'integrità del rischio rappresentato dall'enunciato complessivo si basano sulla precisione e sull'integrità complessiva dell'intero enunciato. Se ogni proposizione di identità è precisa, l'insieme può essere automatizzato con una elevata fiducia nella qualità dei risultati del processo di gestione automatizzata del rischio.

Una parte essenziale della gestione sia del rischio che degli asset fa perno sull'identità. Senza la capacità di identificare le differenze tra asset e/o le differenze tra coloro che vi accedono non può esserci garanzia di protezione delle transazioni o della memorizzazione dei dati.

Buona parte della moderna sicurezza tecnica si basa su un ruolo vecchio di decenni, quello dell'"operatore". I presupposti di questo ruolo derivano dal concetto secondo il quale un

operatore umano è responsabile di tutte le decisioni prese da una macchina, nella forma della responsabilità (assegnata fornendo all'operatore una chiave fisica) dell'insieme di pulsanti e manopole situato sulla console dell'operatore stesso. In origine le macchine erano incapaci di attività senza un operatore umano ma nel tempo la situazione è cambiata. Gli esseri umani e le loro azioni sono spesso l'obiettivo della maggior parte delle attività di rilevamento e applicazione della sicurezza, ma nell'era dei computer ciò non è più una misura dell'essere umano ma solo delle attività effettuate dalla macchina davanti alla quale si presuppone ancora che sia seduto un operatore. Il modello dell'operatore è diventato sempre più una finzione.

L'opportunità di un deployment Zero Trust è di accettare questo contesto di sicurezza di "macchina come essere umano per procura" e applicare la sorveglianza e le regole di sicurezza a tutti i dispositivi come se alla loro tastiera vi fosse un essere umano dotato di una password rubata, o come se un malware (o un hacker in carne e ossa) avesse compromesso la macchina.

Questo approccio di trattare tutte le azioni (umane o meno che siano) come se fossero svolte da macchine o servizi genera parecchia flessibilità architetturale: tutto può essere, infatti, trattato in maniera simile sia che si tratti di un dispositivo sconosciuto, di un utente sconosciuto, di una rete sconosciuta, di un dispositivo conosciuto, di un utente conosciuto, di una rete conosciuta o di una qualsiasi loro combinazione, indipendentemente dalla frequenza con cui può cambiare.

Questo approccio uomo-macchina richiede, tuttavia, una telemetria armonizzata per quanto concerne le identità. Nel 4G e 5G ciò viene comodamente gestito per mezzo delle SIM card (Subscriber Identity Module) e da qualche ulteriore credenziale on-card. In questo modo un dispositivo dotato di SIM come un telefono, un robot, un veicolo autonomo, una smart factory, un drone da carico marittimo o un dispositivo IoT (Internet of Things) possono essere tutti gestiti con Zero Trust come se dietro di essi ci fosse un essere umano con cattive intenzioni. La sorveglianza deve essere sempre attiva per osservare eventuali comportamenti sospetti (contesto di sicurezza) e valutare se possano richiedere un intervento di sicurezza (risposta basata sul rischio).

Fortunatamente questi grossi e costosi rischi enterprise appena descritti possono essere neutralizzati. Quando si implementa una SBOM in una soluzione Zero Trust, i metodi usati per identificare il software si applicano ugualmente ai sistemi creati e customizzati internamente. I sistemi così identificati possono essere analizzati per rilevarne il comportamento normale in modo da poter lanciare l'allarme in caso di comportamenti insoliti. Il concetto di Software ID (SWID) può essere applicato tanto al software interno quanto a quello fornito da produttori esterni creando una mappa dei componenti della supply chain estremamente utile per chi deve intervenire in caso di incidenti e per tutto il team incaricato della gestione del rischio.

4. Conclusioni e suggerimenti

Il concetto di Zero Trust riguarda la sorveglianza. Un sistema "a fortezza" dotato di un proprio perimetro controlla le identità ogni volta che tale perimetro viene attraversato da qualcuno o qualcosa. Una rete Zero Trust lo controlla costantemente, ne incrocia i riferimenti, valuta il rischio comportamentale e lo confronta con le potenzialità di perdite e di ricavi.

In questo documento abbiamo visto:

- quali modifiche alla responsabilità del management e alla governance dei CdA richiedono l'adozione di ZTA
- Quali nuovi requisiti sono imposti da governi e clienti alla resilienza della supply chain usando ZTA
- L'uso di strumenti Zero Trust come l'automazione della gestione del rischio operativo per facilitare la gestione della sicurezza e ridurre sia il rischio enterprise che il TCO (Total Cost of Ownership) della sicurezza
- L'uso dell'effetto di semplificazione che ZTA genera sulla gestione della sicurezza per ridurre la dipendenza da personale esperto che è difficile conservare. A sua volta ciò riduce il gap nelle competenze di sicurezza permettendo di ricorrere a personale junior e/o offshore persino per la diagnosi di incidenti complessi.

Il perno della sorveglianza Zero Trust è l'identità, la cui integrità viene protetta usando Zero Trust in modo da esercitare la massima funzionalità enterprise con il minimo rischio.

Zero Trust basa il proprio accesso sull'autenticazione continua, il che richiede che l'identità sia adeguatamente pianificata e la sua esecuzione elegante – un metodo di design formale e maturo noto come Enterprise Data Architecture, il cui sottoinsieme è la Enterprise Identity Architecture. Sono processi maturi che rendono possibile abbattere i costi attraverso il riuso dell'infrastruttura e la riduzione del lavoro operativo mediante la riduzione della complessità.

In un mondo sempre meno stabile per via di cambiamenti climatici, invecchiamento della popolazione, guerre, interruzioni delle supply chain e conseguente competizione serrata per ottenere risorse che scarseggiano, un approccio alla sicurezza maggiormente sofisticato, articolato ed economicamente conveniente aiuterà le organizzazioni più sane a sopravvivere.

Appendice - CASISTICHE D'USO ZERO TRUST

CASISTICA D'USO A – Miglioramenti alle supply chain – L'antivirus inverso come SBOM Zero Trust

L'antivirus è un elenco di hash di file sospetti la cui esecuzione non è mai consentita.
Si può pensare a un metodo a garanzia della supply chain sottoforma di una lista di hash "buoni" a cui è permessa l'esecuzione.
Questo metodo può essere immaginato come una sorta di "antivirus inverso" ed è un'opportunità per riutilizzare l'infrastruttura esistente in una modalità associabile a Zero Trust.
Percorso di maturità del prodotto. Il metodo proposto è inizialmente un registro di autocertificazioni di conformità SBOM rilasciate dai vari produttori. Questo potrebbe essere sviluppato come un metodo operativo estremamente simile all'antivirus. In questo modo sarebbe scaricabile, aggiornabile, utilizzabile per promuovere la fidelizzazione dei clienti, adatto a valutare altre funzioni di sicurezza ecc.
Il patrimonio dei dati di prima parte. Come operatore di un registro del tipo appena descritto, un antivirus inverso agirebbe da Root of Trust per mettere al sicuro la supply chain. In tale ruolo un antivirus inverso disporrebbe di visibilità sulle attività di tutte le supply chain per tutti i clienti. Applicando machine learning e correlazioni si può derivare il contesto di sicurezza di qualunque elemento della supply chain e, quindi, qualsiasi transazione riguardante la supply chain stessa, dai pagamenti fino alle spedizioni.
Sinergie e best practice per l'architettura business. Da notare che questo processo è estremamente simile al processo Know Your Customer (KYC) vigente nel settore bancario e finanziario per l'antiriciclaggio. Il processo KYC viene usato per affermare la sicurezza delle transazioni nella supply chain finanziaria sottoforma di controlli AML (Anti-Money-Laundering). Il riciclaggio del denaro è una classe di attacchi alla supply chain nella quale la provenienza (la criminalità) di chi fornisce il denaro (il criminale) viene nascosta. In modo simile, gli attacchi alle supply chain dei produttori software nascondono la provenienza dei componenti usati nella supply chain. Si può immaginare per analogia che gli attacchi diretti contro la supply chain software si nascondano attraverso il "riciclaggio dei dati". Il prodotto SBOM-Supply chain visto sopra avrebbe molte sinergie con la pratica ormai matura che garantisce la supply chain finanziaria e un prodotto SBOM come KYC AML rispetterebbe i requisiti di molti standard di auditing del settore bancario (favorendone l'adozione in tale comparto). Si può pensare al processo KYC come a una "sicurezza basata sul contesto".
Sviluppi futuri. Il rapporto tra telecomunicazioni 6G, Zero Trust, sicurezza della supply chain, finanza e reti di distribuzione elettrica non dovrebbe essere sottovalutato. Nell'era del 6G (e nel corso dell'attuale periodo di preparazione), l'implementazione di Zero Trust è resa obbligatoria per diversi settori come previsto dalle compagnie di telecomunicazione. L'uso di blocchi perimetrali non è scalabile negli ambienti 5G e lo si può vedere nell'obbligo di usare Zero Trust nel 6G. La scalabilità dell'approccio Zero Trust senza perimetri DISA-NSA viene promossa ricorrendo a contesti di sicurezza simili a quelli che le compagnie di telecomunicazione usano per il roaming.

Migliorare la sicurezza basata sul contesto per migliorare Zero Trust. Gli insight derivanti da un prodotto SBOM possono essere usati come riferimento per Zero Trust migliorando la sicurezza basata sul contesto di Zero Trust del tipo richiesto dai grandi clienti, per esempio l'architettura di riferimento NSA-DISA.
Consolidamento dei fornitori. Usare le regole per l'orchestrazione della sicurezza SDN all'interno del risk engine Zero Trust e monitorare i fornitori ricercando vulnerabilità pubblicate, fornire alert basati sul contesto di sicurezza (per esempio "alto" potrebbe essere in realtà "basso" per una specifica organizzazione o viceversa). I prodotti come le persone vanno gestiti come minacce interne.
Un'importante casistica di utilizzo di Zero Trust riguarda la gestione della supply chain dei fornitori sia per i lavoratori da remoto che per gli asset in cloud. Il recente attacco Log4j avrebbe potuto essere identificato prima e il suo rischio ridotto attraverso un approccio Zero Trust alla gestione dei fornitori. Le supply chain sono tipiche fonti di rischio dal momento che comportano il "problema del terminale nascosto", ovvero l'impossibilità di osservare quel che accade sul lato più lontano del fornitore più prossimo all'interno della supply chain. Il "fornitore del fornitore" è invisibile rispetto alla governance e alle pratiche di sicurezza pur continuando a generare traffico "affidabile".
Un approccio Zero Trust a questo problema è l'uso di golden image28 verificate tramite hash ripetibili con l'identificatore sidechain29 del fornitore. L'accesso in abbonamento a un database opt-in globale di fornitori costituirebbe una nuova opportunità di prodotto.
Un approccio simile potrebbe riguardare l'uso dell'"antivirus inverso" descritto prima, includendo SWID come elemento di riferimento incrociato contro le vulnerabilità conosciute.

CASISTICA D'UTILIZZO B – eSIM per sistemi nazionali di identità e sovranità dei dati su reti di telecomunicazione 6G globali in roaming

I recenti eventi mondiali hanno evidenziato aspetti come il nazionalismo, l'instabilità di interi Paesi e l'impatto delle attività di disinformazione sulle popolazioni. Diversi Stati lungimiranti pianificano da tempo questi metodi di competizione internazionale che richiamano sempre più alla Guerra Fredda. Questi Paesi – Canada, Cina, Stati Uniti, Russia – hanno iniziato a implementare un modello simile a Zero Trust per la gestione di un sistema Identity-as-a-Service per i cittadini come strumento per rafforzarsi contro le operazioni di disinformazione. Prove concettuali di questo sistema sono già in funzione: il programma nazionale di identità della Cina è in fase di sperimentazione a Shenzhen. Considerato lo scenario politico locale, non è necessario nascondere il programma (che potrebbe incontrare delle resistenze in altri Paesi se venisse reso pubblico). Il programma nazionale cinese di identità è un approccio molto maturo e ben pianificato che può essere implementato in modo efficiente anche a fronte di potenziali perplessità da parte della popolazione. Zero Trust viene implementato sia sugli identificatori IT che su quelli telecom.
Il programma nazionale di identità della Cina può essere considerato come una supply chain di informazioni relative all'Identity Fabric che usa ciascun elemento della catena sia come aggregatore che come sensore di sicurezza.

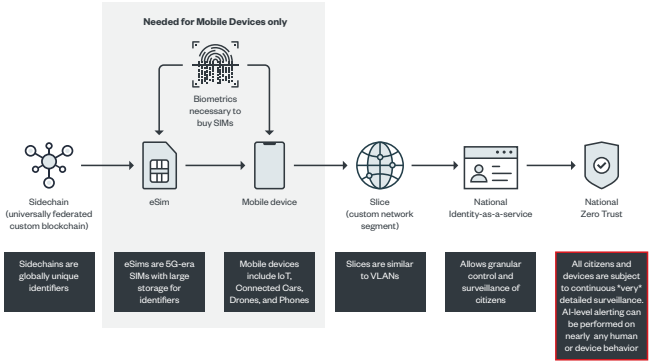


Figura 4: *Il programma nazionale cinese di identità come supply chain di informazioni relative a un fabric delle identità*

Questo approccio permette di arricchire costantemente le fonti di dati offline attraverso i dispositivi mobili. Dal momento che i dati biometrici sono obbligatori per l'acquisto delle SIM e i dispositivi stessi generano telemetria mediante sensori (compresi quelli biometrici), esiste la possibilità di combinare entrambe le tipologie di dati all'interno di graph database di alta qualità per l'intelligenza artificiale. Queste basi di dati possono essere usate, quindi, per creare nuovi alert ancora più precisi basati su attività cybercriminali, attività di attori statali, tracciamento di dissidenti e automazione delle operazioni di vigilanza. Quando il sistema è presente su tutti i cellulari di un Paese, soluzioni come il tracciamento dei contatti COVID possono essere usate trasparentemente per altri scopi come seguire i contatti noti dei criminali.

CASISTICA D'UTILIZZO C – Prevenzione e controllo delle frodi elettorali

Diversi Paesi stanno migliorando il processo elettorale con un maggior livello di tracciabilità che può essere ottenuto con una versione specifica di Zero Trust.
L'applicazione di Zero Trust Primacy (e il relativo subset di Personas) ai sistemi di votazione può offrire:

- integrità dei sistemi elettorali (questa persona è reale, è un cittadino e ha votato una sola volta)
- Collegamento a requisiti come quelli, in vigore in alcuni Paesi, per cui i cittadini che vogliono svolgere servizio pubblico devono avere votato.

Tutto questo può essere fatto in modo anonimo e sicuro sia per l'elettore che per il sistema a monte (una caratteristica di Primacy e Personas).

CASISTICA D'UTILIZZO D – Zero Trust per la compliance 6G

La tecnologia di telecomunicazione 6G comprende già Zero Trust caratteristica fondamen-

tale negli standard emergenti. L'uso di Primacy e Personas con Zero Trust è scalabile (quindi veloce e leggero, con una riduzione dei costi di capitale in termini di carico totale sulla rete delle torri cellulari). Per questa ragione Zero Trust è stato integrato direttamente negli standard 6G proposti.

CASISTICA D'UTILIZZO E – Omnichannel

L'approccio trasformativo "tutti i servizi, un'unica infrastruttura" noto come omnichannel dipende fortemente dalla federazione delle identità, una funzione base di Zero Trust. Quando esistono più mezzi di autenticazione, devono essere presenti funzionalità e registrazioni leggere e condivise. Questo ha come implicazione progettuale una struttura comune di gestione dei che unifica le soluzioni IAM (Identity and Access Management) in una federazione di identità leggera e scalabile (un cosiddetto Idenity Fabric).
Per fornire risultati credibili, l'Idenity Fabric deve fare affidamento sulla federazione. Il concetto di IAM unificato è semplice ma la sua esecuzione è complessa, poiché molte aziende non possiedono un'architettura dati enterprise sufficientemente matura per mettere in collegamento il vecchio con il nuovo.

CASISTICA D'UTILIZZO F – Sovranità dei dati

La sovranità dei dati è un particolare deployment dell'omnichannel con ulteriori requisiti di business definiti dalle normative locali.
Le implementazioni Zero Trust possono applicare filtri basati su telemetria e crittografia usando estratti delle caratteristiche imposte dalle leggi locali. Le tecniche di machine learning hanno dimostrato con successo di riuscire a estrarre i vincoli normativi dai testi legislativi su vasta scala con una precisione superiore a quella degli avvocati in carne e ossa. La sovranità dei dati può quindi essere automatizzata per rispettare i requisiti dei singoli Paesi.

CASISTICA D'UTILIZZO G – Carta d'identità internazionale

Sidechain è un'implementazione della blockchain che può essere utilizzata come identità canonica federata a livello globale (Globally Federated Canonical Identity) usando identità eSIM visibili alle regole di business, dati, applicazioni e reti Zero Trust. Le applicazioni comprendono identificatori globali per passaporti, per prodotti (per contrastare le contraffazioni), per spedizioni (per contrastare contraffazioni e furti) e per transazioni (per contrastare frodi e riciclaggio di denaro), iniziative di anticontraffazione per prodotti retail e tracciamento di asset utilizzabili a scopi illegali (vaccini fasulli, diamanti insanguinati, armi da fuoco, precursori di stupefacenti ecc.).

CASISTICA D'UTILIZZO H – Federazione banche-energia-telecomunicazioni

I consumi elettrici dell'IoT sono elevati e aumenteranno in conseguenza dell'espansione del 5G e dell'IoT. Monetizzare (e fatturare) i maggiori consumi di dispositivi ad alto consumo di energia richiede una visibilità operativa armonizzata tra sistemi di fatturazione, sistemi elettrici e sistemi di telecomunicazione.

Aprire questi sistemi, con i loro requisiti di sicurezza decisamente differenti, richiederà un controllo estremamente granulare sulle modalità di interazione fra tutte le tre famiglie di architetture dati. Serviranno l'autenticazione continua e la sicurezza granulare delle identità di ciascun dispositivo. Da notare che molti dispositivi IoT non possiedono identità univoche ma la natura granulare di Zero Trust e le reti senza perimetro permettono di ricavare le identità effettive con precisione.
Dal momento che ogni sistema potrebbe essere attaccato attraverso gli altri, l'uso di algoritmi di intelligenza artificiale per la sicurezza basati sul gaming può mappare lo "spazio di rischio" di tutti gli altri sistemi coinvolti.
Inoltre, il 6G presenta requisiti elevati in termini di velocità, fatturazione e controllo dell'energia di broadcast. Nell'era del 6G l'unità tra banche, telecomunicazioni e griglia di distribuzione elettrica richiede un'autenticazione incrociata e una profonda dipendenza reciproca tra le rispettive supply chain. L'omnichannel Zero Trust fa parte di questo scenario insieme con gli aspetti legati a open banking, rete elettrica dinamica e machine learning 6G.

CASISTICA D'UTILIZZO I – "Il firewall per fake news" (blocco di operazioni di disinformazione su vasta scala)

La combinazione tra programmi nazionali di identità e Zero Trust produce una profonda visibilità sulle attività di una popolazione. Chiamate, messaggi e uso di Internet possono essere combinati per osservare le attività di un qualsiasi gruppo di persone.
Se una certa narrativa provoca una determinata attività considerata contraria agli interessi dello Stato, può essere implementata una funzione equivalente a una censura automatizzata di massa per evitare che narrative indesiderate arrivino all'attenzione di cittadini vulnerabili. In questo modo anche le attività negative (come la distruzione delle antenne 5G, per esempio) possono essere bloccate.
Il punto di contatto tra la prevenzione delle fake news circolanti e un vero "firewall per fake news" è l'estensione della gestione del rischio di identità verso il campo della Signals Intelligence (SIGINT), in cui i cambiamenti delle attività umane suscitano una risposta automatizzata che produce una censura automatizzata su vasta scala. Ovviamente il tipo di narrativa da censurare dipende dagli specifici interessi di ogni singolo Stato.

CASISTICA D'UTILIZZO J – Confronto dei fornitori e "gare virtuali"

Zero Trust contribuisce molto per riunire metriche di sicurezza armonizzate provenienti da molteplici fonti che possono, quindi, essere usate per identificare e neutralizzare intere classi di rischio in modo proattivo o reattivo, compresi i rischi insiti nei componenti di un produttore.
Molte aziende di grandi dimensioni soffrono di una diffusione incontrollata delle architetture (conseguenza delle varie attività di fusione e acquisizione) che potrebbe risultare in una sovrapposizione delle funzionalità fornite dai diversi produttori presenti all'interno della rete. Cosa accadrebbe se un intero produttore fosse un rischio perché la sua funzionalità, soluzione o linea di prodotti risultasse meno efficace (più rischiosa) rispetto alla

linea di prodotti di un altro vendor già presente nella stessa rete? Confrontare i due per mezzo di audit potrebbe essere inutile, dal momento che nella maggior parte dei casi si tratta di analisi point-in-time e non in tempo reale condotte sulla base delle tendenze delle performance passate. Una gara in questo caso è un confronto tra produttori che dispongono delle medesime caratteristiche, effettuato solitamente nel laboratorio di un vendor prima di decidere un contratto di fornitura. Dal momento che si tratta di un passaggio che rientra nell'acquisizione di nuovo business, i produttori sono disponibili a farlo essendo una normale condizione competitiva in vista di un possibile contratto.
Confronti di questo genere sono incredibilmente difficili da negoziare per i responsabili che si occupano dei rischi di sicurezza una volta che il contratto è stato assegnato. Per questa ragione sarebbe estremamente utile poter svolgere gare virtuali nelle quali i produttori e le rispettive soluzioni siano messi a confronto mediante un report di sicurezza basato sull'affiancamento di dati armonizzati (come Zero Trust). Con questo approccio si possono confrontare le performance (riduzione del rischio) di ciascuna soluzione e ciascun produttore. I vendor possono essere valutati in base al ROI (Return on Investment) dei loro prodotti e i due migliori possono essere consolidati. Due è il numero minimo di fornitori agli effetti pratici, non essendoci leva negoziale sul prezzo in caso contrario.
Questo e altri approcci simili possono essere usati per gestire gli investimenti dedicati alla sicurezza. Una volta acquisita credibilità e ottenuto il successo interno, è possibile allargare le valutazioni anche a fornitori di ambiti diversi dalla sicurezza avvalendosi di criteri di business aggiuntivi. In questo modo la sicurezza delle informazioni, che tradizionalmente è considerata come un centro di costo, può uscire dal suo angolo ed essere riconosciuta come contributo agli obiettivi di business a livello di CdA come quelli dei CRO.
La gestione del rischio di sicurezza Zero Trust può, quindi, diventare un mezzo per gestire anche rischi o persino asset diversi dalla sicurezza; un approccio scalabile e automatizzabile alle esigenze di governance che scaturiscono dalle considerazioni di responsabilità normativa legate a supply chain e SBOM.

CASISTICA D'UTILIZZO K – Zero Trust per la gestione di fornitori, supply chain e lavoro da casa

Dal momento che consulenti e dipendenti che lavorano da casa fanno a tutti gli effetti parte della supply chain e possono essere considerati come "fornitori", si può seguire un approccio simile per loro, i loro prodotti e i loro dispositivi. Questi approcci Zero Trust alla supply chain supportano l'identità decentralizzata e le reti senza perimetro quando vengono implementati con specifiche caratteristiche come Primacy, rendendo porzioni di identità visibili ai soggetti appropriati.

Enterprise Architecture a supporto della Information Security

[A cura di Raffaella D'Alessandro, Sebastiano Paolo Lampignano e Alessandro Pisani, Consulthink]

Premessa

Il ruolo dell'Information Security è quello di coordinare le iniziative di sicurezza rispetto ai programmi aziendali e agli obiettivi di business, assicurando che gli asset informativi e le tecnologie siano adeguatamente protetti rispetto ai rischi proprio in funzione degli obiettivi di business definiti dalla Direzione Aziendale.
Quindi l'esigenza primaria dell'Information Security è quella di conoscere il Business dell'azienda e di conoscere come gli asset informativi e tecnologici contribuiscono ai processi di business, al fine di individuare e contrastare i relativi rischi di Sicurezza che possono impattare il raggiungimento degli obiettivi aziendali. Sembra un tema scontato, ma nella realtà, caratterizzata da dinamiche estreme di digitalizzazione grazie anche all'avvento del Cloud, riscontriamo che uno dei più grandi problemi dei CISO è proprio quello di non avere una conoscenza oggettiva ed aggiornata di quali siano gli asset informativi e tecnologici che supportano ciascun processo di Business. Si tratta dell'ABC: se non si conoscono quali asset supportano quali processi di business, come si fa a valutare il rischio ed a renderli sicuri in funzione degli obiettivi di Business aziendali?

Proviamo a rispondere a questo interrogativo esplorando cosa può fare la Enterprise Architecture (EA) a supporto della Information Security. Cominciamo fornendo la definizione di cosa si intende per Enterprise Architecture e che rapporti ha con la Security Architecture. Vedremo quindi il meta-modello informativo disponibile nell'Enterprise Architecture e come questo possa essere utilizzato in diversi scenari di Information Security, fornendo il supporto sia in fase di valutazione dei rischi e pianificazione strategica in allineamento agli obiettivi di business aziendale, che nel corso della gestione operativa delle misure di sicurezza e delle attività di audit. Gli scenari di Information Security a cui abbiamo applicato il meta-modello informativo dell'Enterprise Architecture sono quelli di: Analisi dei Rischi, Business Impact Assessment (BIA) e Piano di Continuità Operativa e di Disaster Recovery, Supply Chain Security, Identity and Access Management, Gestione degli incidenti di Cybersecurity, Registro dei Trattamenti dei Dati Personali, Classificazione dei dati ai sensi della Sicurezza e della Privacy, EDP Auditing.

Enterprise Architecture e Security Architecture

"Architettura" è una parola affascinante. Nasce per riferirsi alle attività di progettazione e realizzazione tipiche del mondo delle costruzioni, in cui l'uomo costruisce ed organizza gli spazi della sua esistenza, siano essi una casa, un palazzo, un quartiere o un'intera città. Nel tempo, sia nel mondo dell'Information Technology che in quello della Information Security, si è giustamente fatto ricorso per analogia al concetto di "architettura" esattamente con la

stessa finalità, solo contestualizzata alla costruzione di spazi non più fisici, ma anche costituiti da oggetti - per buona parte immateriali - quali sono le informazioni.
Si sente con frequenza parlare di molte tipologie di architetture in questo ambito: "architettura applicativa", "architettura della informazioni", "security architecture", "enterprise architecture"; è il caso quindi di provare come prima cosa a definire che cosa intendiamo specificamente per "Enterprise Architecture", al meglio delle nostre possibilità e per non incorrere in fraintendimenti. Tuttavia, si tenga presente che l'esercizio di dare definizioni è uno dei più difficili, perché nel tentativo di generalizzare si rischia sempre di perdere di vista la realtà di ciò che osserviamo e di ragionare per postulati. Si tenga conto del fatto che l'intento vuol essere tutt'altro che "accademico": sarà l'attività sul campo – tanto nella realizzazione di sistemi di Enterprise Architecture che nel contesto dell'Information Security Management System – l'unica vera fonte delle affermazioni riportate.
L'esperienza operativa fa emergere che le grandi organizzazioni moderne ("enterprise") fanno un uso estensivo e pervasivo della digitalizzazione delle informazioni e del loro trattamento tramite strumenti software, necessitando di infrastrutture informatiche per l'esercizio. Ne consegue che gli investimenti nella digitalizzazione dei processi aziendali, nello sviluppo o nell'acquisizione di software applicativo e di hardware fisico o virtuale sono ormai tra le voci di costo più grandi ed evidenti nei bilanci delle organizzazioni. In questo processo di crescita digitale, qualcosa si perde. La componente tecnologica rischia di essere vista come un fine ultimo e non un mezzo (potentissimo) per raggiungere gli obiettivi strategici dell'organizzazione. A fronte della necessità di mantenere un forte allineamento tra l'Information Technology ed il business aziendale, si è introdotto, per la verità fin dal 1987[1], il concetto di "Enterprise Architecture" cioè quel sistema informativo in cui convergono e si collegano le entità chiave del business e dell'IT. Quindi una possibile definizione pragmatica è la seguente: **l'Enterprise Architecture è il 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**[2].

[1] John A. Zachman, "A Framework for Information Systems Architecture," IBM Systems Journal 26, no. 3 (1987)

[2] Il Gartner Glossary definisce così il termine: "Enterprise architecture (EA) is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. EA delivers value by presenting business and IT leaders with signature-ready recommendations for adjusting policies and projects to achieve targeted business outcomes that capitalize on relevant business disruptions." https://www.gartner.com/en/information-technology/glossary/enterprise-architecture-ea. Per completezza delle fonti, è bene ricordare anche la definizione di TOGAF: ISO/IEC/IEEE 42010:2011 defines "architecture" as: "The fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution." The TOGAF Standard embraces but does not strictly adhere to ISO/IEC/IEEE 42010:2011 terminology. In addition to the ISO/IEC/IEEE 42010:2011 definition of "architecture", the TOGAF Standard defines a second meaning depending upon the context: "The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time." (fonte TOGAF: https://pubs.opengroup.org/togaf-standard/introduction/chap03.html#tag_03_02)

Tutto considerato è una promessa niente male. "Come si fa?" chiederebbe a questo punto il saggio manager. La risposta alla domanda richiede una ulteriore precisazione, sempre frutto dell'esperienza sul campo.

L'Enterprise Architecture (EA da qui in poi,) può essere vista come la stratificazione di **tre** elementi:

- la **capability**, ovvero la capacità dell'organizzazione di vedere sé stessa nei termini sopra descritti- Quindi un elemento di "maturità" dell'impresa;
- il **modello concettuale** che descrive l'EA, il relativo **patrimonio di informazioni** che lo popolano e soprattutto le **relazioni** che vengono definite tra queste ultime. Normalmente si fa riferimento a questo come "meta-modello", ovvero un modello che mette in relazione entità provenienti da altri modelli concettuali. Questo perché, come già accennato, le informazioni provenienti da diverse aree dell'organizzazione e contenute normalmente in modelli dati funzionalmente specifici devono essere rappresentate nel modello EA e poi collegati con quelle provenienti da altri modelli;
- infine, la **soluzione software** (prodotto o insieme di prodotti) che consente di gestire e fruire di queste informazioni.

Ora, solo il terzo elemento può essere trovato ed acquistato sul mercato e purtroppo, è anche l'elemento meno decisivo che non deve assolutamente essere scambiato con l'Enterprise Architecture nel suo significato più ampio; sarebbe come dire di avere messo in sicurezza sotto ogni aspetto la propria azienda solo perché abbiamo acquistato un firewall.
Per acquisire gli altri due elementi occorre:

- acquisire una **metodologia** che guidi nel disegno dell'EA ed in particolare del suo meta-modello informativo;
- intraprendere il **progetto** di costruzione dell'EA in dipendenza dalla struttura informativa che si è immaginata;
- e soprattutto **mantenere e sviluppare nel tempo** la capability acquisita, perché l'EA viva, si aggiorni e cambi, in simbiosi con l'Enterprise, della quale ne è, al massimo livello, la sua Mappa.

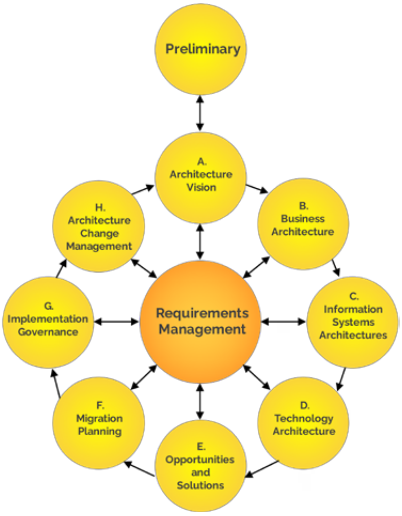


Figura 1: *Fonte Open Group – TOGAF ADM: Architecture Development Method*

A questi fini, ormai da più di trent'anni esistono sul mercato alcuni framework metodologici – normalmente indipendenti da specifici prodotti – che guidano nella definizione del meta-modello, nella implementazione del proprio sistema di EA ed in definitiva nell'acquisizione della *capability*. Uno dei più importanti framework di riferimento è quello mantenuto da The Open Group e denominato **TOGAF** (The Open Group Architecture Framework)[3]. Unitamente al framework metodologico, è stato sviluppato anche il linguaggio di modellazione **Archimate** che può essere efficacemente utilizzato per costruire diagrammi grafici che rappresentano l'Enterprise Architecture o parti specifiche di questa.

Il punto di partenza per la costruzione dell'EA normalmente è la progettazione del meta-modello informativo, la metodologia prescrive solamente una strutturazione di massima, costituita da quattro livelli:

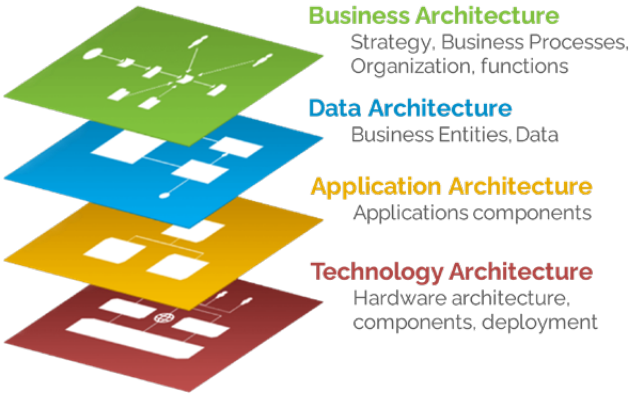


Figura 2: *Architecture Layers*

[3] https://www.opengroup.org/togaf

- **Business (Architecture) Layer**, che racchiude le entità che modellano i processi aziendali ed i servizi erogati, in linea con gli obiettivi strategici dell'organizzazione;
- **Data (Architecture) Layer**: che rappresenta la struttura delle informazioni che l'organizzazione raccoglie, produce e trasforma in valore;
- **Application (Architecture) Layer**: che descrive le applicazioni usate per digitalizzare i processi aziendali e le loro interazioni con utenti ed il business;
- **Technology (Architecture) Layer**: che dà accesso alle informazioni che permettono di disegnare l'insieme di architetture, software di base e tecnologie hardware fisiche e virtuali utilizzate per erogare i servizi dell'organizzazione.

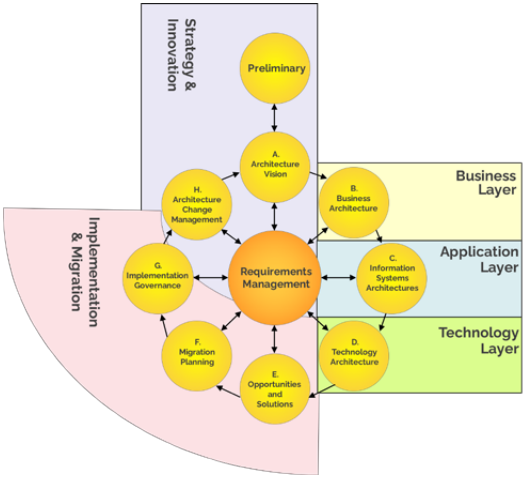


Figura 3: *Fonte Open Group – Layers e ADM relations*

All'interno di questi quattro livelli, la modellazione delle entità e le relazioni tra di esse devono essere necessariamente definite in modo specifico e personalizzato per ogni organizzazione; pur potendo fare riuso di *pattern* o *building blocks* già conosciuti ed efficaci, è fondamentale che il meta-modello rispecchi proprio la specificità di ciascuna organizzazione e che quindi sia frutto di un'approfondita auto-analisi di questa. La definizione del contenuto e della costruzione di ciascuno dei *layer* dell'EA è oggetto di una specifica fase del processo proposto dalla metodologia TOGAF.
Descritte le basi di ciò che intendiamo per Enterprise Architecture, si può provare a dare una definizione operativa anche di Security Architecture partendo dalla traduzione della voce specifica riportata dal NIST (National Institute of Standards and Technology): **la Security Architecture è l'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 sicurez-**

za 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**[4].

Risulta evidente una sovrapposizione ed una sinergia tra l'Enterprise Architecture, che fornisce la più alta rappresentazione dell'architettura di sistema, e la Security Architecture, che disegna le *policy* per la sicurezza delle informazioni. I collegamenti concettuali, tra le definizioni, sono così stretti che risulterebbe davvero difficile immaginare progettazioni separate e distinte.

Gli aspetti più rilevanti in comune tra la disciplina dell'Enterprise Architecture e quella dell'Information Security possono essere sintetizzati in:

- **cultura del "**by design**"**, cioè dell'affrontare la progettazione dei sistemi e la soluzione dei problemi strategici disegnando sin dall'inizio la situazione ideale desiderata dall'organizzazione, avvalendosi di tutti gli strumenti e le metodologie migliori e avendo la migliore consapevolezza possibile della situazione da cui si sta partendo;
- necessità di approcciare la **governance** del sistema avendone sempre una visione complessiva aggiornata, che permetta di valutarlo da tutte le angolazioni possibili in modo equilibrato, cioè non sbilanciandosi nella direzione di un'unica prospettiva;
- desiderio di individuare continuamente nuovi **driver di miglioramento** dei processi e di innovazione organizzative e tecnologica.

Il meta-modello informativo

Acquisito il significato del termine "architettura", in entrambi i contesti, e verificata l'ampia correlazione tra Enterprise Architecture e Security Architecture, è possibile cominciare a rispondere ad alcune domande:

- che cosa può fare EA per supportare l'Information Security?
- Quali sono gli scenari di correlazione che potrebbero portare alla creazione di un unico meta-modello a servizio di entrambe le esigenze?
- Come e dove l'Information Security può e/o deve essere supportata da uno strumento di Governance di livello Enterprise?
- Come è possibile "vedere" le conseguenze di un attacco prima che questo si verifichi?

4 La definizione di "security architecture" del NIST: "A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected. Note: The security architecture reflects security domains, the placement of security-relevant elements within the security domains, the interconnections and trust relationships between the security-relevant elements, and the behavior and interaction between the security-relevant elements. The security architecture, similar to the system architecture, may be expressed at different levels of abstraction and with different scopes". https://doi.org/10.6028/NIST.SP.800-37r2

Gartner propone questa definizione: "the discipline and associated process of planning and designing organizational, conceptual, logical, and physical components that interact in a coherent fashion, aligned with business requirements, in order to achieve and maintain a state of managed security-related risk." ("3 Steps to Drive Business Alignment Using Security Architecture", 2021)

Per rendere più evidenti le risposte, si propone il disegno di un meta-modello "standard", in cui sono rappresentate le entità utili e sufficienti allo scopo (non si tratterà quindi di un modello sempre valido o buono per tutte le stagioni, ma solo di una semplificazione riscontrata in contesti reali), trascurando le modalità con cui avviene il *popolamento* dei dati attingendo dai verticali informativi che li detengono. Il modello è quindi utile a fini esemplificativi e non vuole rappresentare una struttura effettivamente implementata in uno specifico contesto.

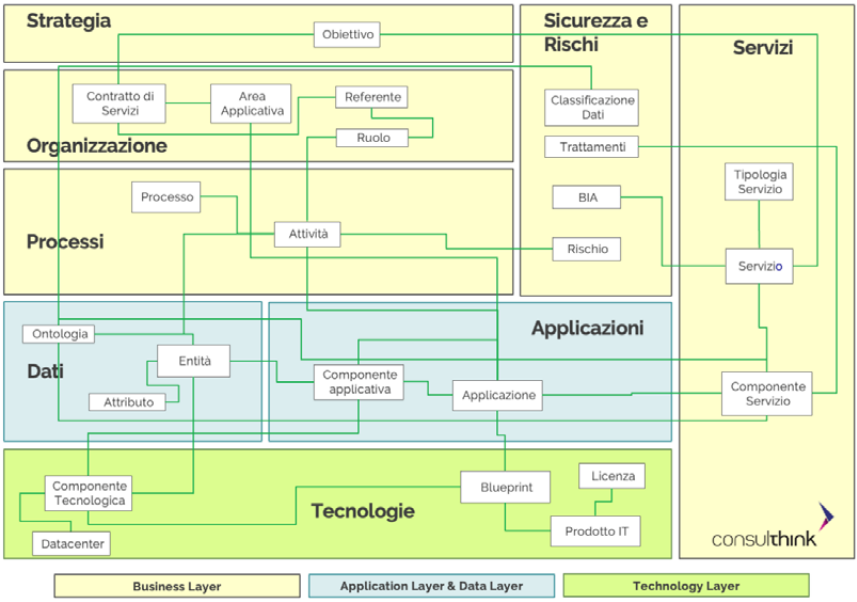


Figura 4: *Meta-modello semplificato*

Nel modello sono rappresentati i quattro layer fondamentali prescritti dalla metodologia. Per esigenze espositive, il layer di business è stato *partizionato* per evidenziare meglio alcune possibili sotto aree d'interesse alla trattazione. Si possono quindi identificare: un'area specifica per il catalogo dei servizi, una per la gestione dei processi, una per il risk management e la sicurezza ed infine una per la strategia. Le entità presenti nelle varie aree del modello sono quelle che ci sembrano più utili per costruire il set di scenari di collaborazione tra EA e Information Security, pur essendo anche astrazioni che difficilmente possono mancare in una Enterprise Architecture.
È importante notare come le varie aree corrispondano a diversi settori dell'organizzazione e che le entità in esse identificate siano in coerenza con quei settori. I dati così rappresenta-

bili appartengono a verticali informativi propri di una specifica parte dell'organizzazione (si pensi alle informazioni presenti nel Configuration Management Database – CMDB, costituite da Configuration Items o ai processi e le relative attività, mantenute in uno specifico sistema di disegno e versionamento dei processi). Questi sistemi specializzati possono sia conferire informazioni all'EA che ricavarne; in questo modo il sistema informativo dell'EA diventa un terreno comune, dove alle singole entità viene attributo un più ampio contesto semantico e dove il collegamento *end to end* tra esse va a costituire nuove catene informative.

Il valore profondo del meta-modello è quello di definire ed alimentare le relazioni tra le entità che lo costituiscono. Su questa base si propongono, di seguito, una serie di scenari in cui l'introduzione di entità, attributi o relazioni possono facilitare o implementare dei requisiti della sicurezza architetturale[5].

Basandosi sul modello dati così definito, il prodotto software specifico - utilizzato per raccogliere i dati e realizzare l'esperienza utente - potrà fornire tutte le necessarie interfacce di navigazione ed interrogazione a supporto delle richieste poste dalle varie anime dell'organizzazione, rappresentando in modo efficace le informazioni raccolte nel repository dell'EA.

[5] Non viene descritta in uno scenario specifico - ma è intrinseca al modello stesso - la necessità di garantire la sicurezza e la confidenzialità tanto della sua struttura che dei dati raccolti, nonché la necessità che i processi di accesso al sistema e consultazione siano correttamente implementati dal punto di vista della sicurezza. Nel repository dell'Enterprise Architecture potrebbero infatti essere presenti informazioni sufficienti per pianificare e d attuare un efficace attacco ai punti deboli dell'organizzazione che vi viene descritta.

Scenari di Information Security supportati dall'EA

Vengono di seguito illustrati alcuni scenari di Information Security che possono essere supportati dal meta-modello informativo dell'EA. Per ciascuno scenario sono evidenziate in highlight giallo le componenti informative del meta-modello applicabili e con linea continua rossa le relative relazioni.

Analisi dei Rischi di Sicurezza. Innanzi tutto, è possibile utilizzare le informazioni acquisite nel repository relativamente al mondo dei **processi** aziendali per eseguire la valutazione dei rischi di sicurezza ad essi associati. La presenza nell'EA di queste valutazioni permetterà di stimare correttamente i livelli di rischio relazionati sia con i **processi di business** che con le **applicazioni**, i servizi software ed i **dati** da queste trattati. Queste relazioni saranno quindi utilizzabili, ad esempio:

- nella definizione delle aree di maggiore rischio correlato al Business, dove concentrare gli investimenti;
- nella progettazione delle misure di sicurezza, fornendo un contesto di riferimento su cui definire e tarare le misure stesse;
- nella progettazione delle simulazioni di situazioni di crisi, a supporto della *problem determination* durante le emergenze;
- nella progettazione delle migrazioni sicure da una piattaforma tecnologica ad un'altra, come nei progetti di re-hosting o re-platforming;
- nei progetti di re-sizing infrastrutturale o di migrazione a soluzioni cloud-based, per non perdere di vista il posizionamento fisico degli asset mantenendo la relazione con i servizi di business.

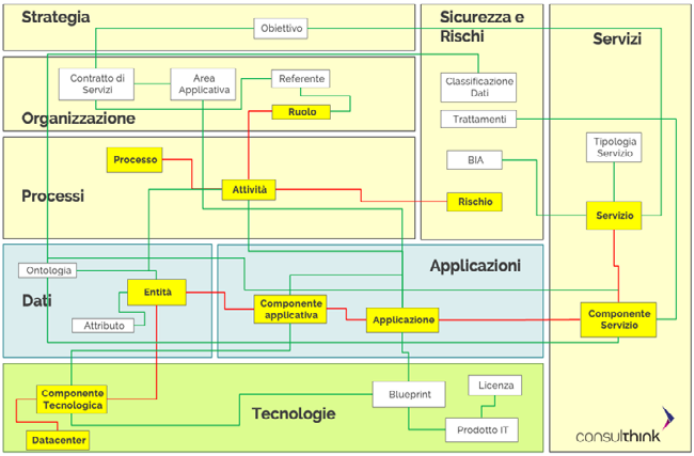


Figura 5: *Scenario Analisi Dei Rischi*

Business Impact Assessment (BIA) e Piano di Continuità Operativa e di Disaster Recovery. La catena tra servizi di business, applicazioni software e infrastrutture fornita da EA può consentire di contestualizzare correttamente le valutazioni relative all'impatto di una interruzione dei servizi, o della perdita dei dati conseguenti ad un evento disastroso, e di **classificare** quindi nel modo più opportuno i servizi di business, attribuendo ad essi i giusti valori di **RTO** (*Recovery Time Objective* - tempi di ripristino del sistema) e **RPO** (*Recovery Point Objective* - quantità di dati che possono essere persi per mancata sincronizzazione). A valle di questa attività, il sistema informativo dell'EA potrà essere fonte preziosa per la definizione del **perimetro** dei servizi critici, permettendo di disegnare gli scenari di *disaster recovery* qualificati con le corrette priorità ed implementare i relativi piani di resilienza.

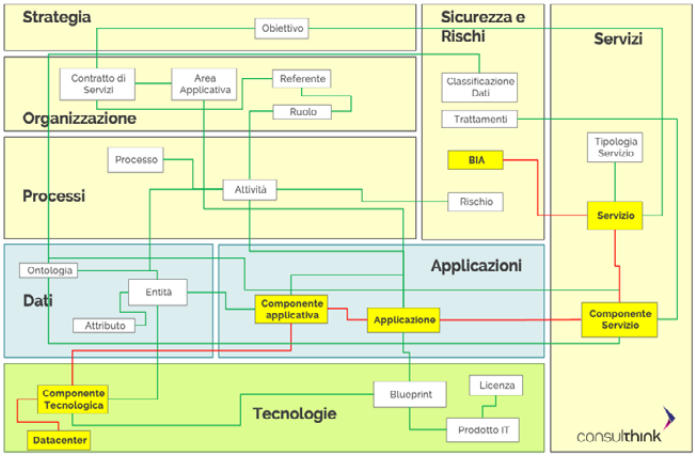


Figura 6: *Scenario BIA*

Supply Chain Security. Tramite il legame tra i contratti che l'organizzazione stipula con i fornitori di servizi informatici e le applicazioni da questi sviluppate, manutenute o supportate in produzione è possibile governare i processi di *on boarding /off boarding* dei fornitori e, in caso di incidente, gestire la sicurezza in tutta la catena di fornitura, individuando con sicurezza le **persone chiave** da coinvolgere. Tutto ciò al fine di tenere sotto controllo anche gli aspetti della sicurezza legati non solo al *software* e all'*hardware,* ma anche a quello che alcuni chiamano *wetware*, cioè la componente *umana* del sistema.

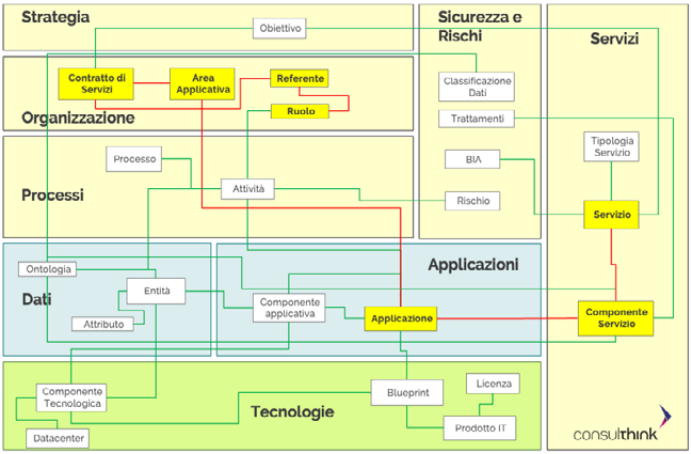


Figura 7: *Scenario Supply Chain Security*

Identity and Access Management. La definizione delle abilitazioni sul software di un'organizzazione spesso segue un percorso che ignora completamente il disegno dei processi aziendali. Di fatto, però, ogni software sviluppato o acquisito da un'organizzazione ha il compito di digitalizzare o automatizzare una o più attività descritte in un processo aziendale ed assegnate ad **uno specifico ruolo**. Per mantenere un perfetto allineamento tra business e digitalizzazione dei processi, è necessario avere uno strumento che metta in correlazione i ruoli per l'esecuzione dell'attività dei processi ed i profili utente definiti all'interno dei sistemi di profilazione. Tramite questo allineamento si potrebbe arrivare ad **automatizzare la gestione della configurazione delle autorizzazioni** sulle applicazioni, partendo direttamente dal disegno dei processi.

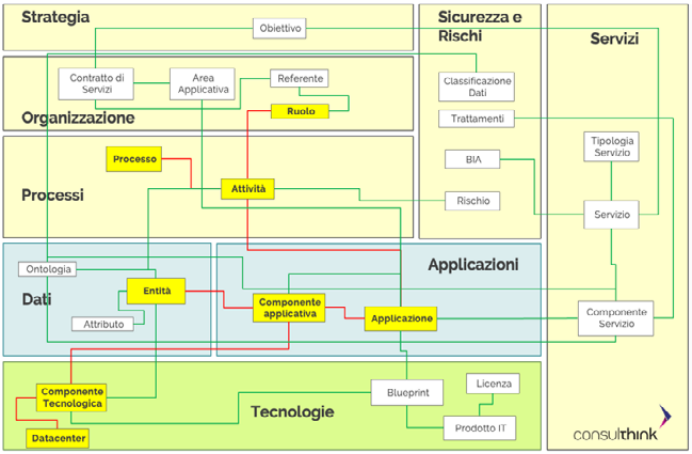


Figura 8: *Scenario Identity Access Management*

Gestione degli incidenti di Cybersecurity. Questa lista di scenari è stata aperta con l'analisi dei rischi per la sicurezza, attività che ha come principale scopo quello di contrastare gli incidenti di security, definiti come violazioni di Riservatezza, Integrità e Disponibilità di asset ed informazioni. Purtroppo, per quanto ci si impegni, è impossibile escludere del tutto che eventuali attacchi informatici possano provocare incidenti di sicurezza. Nel caso in cui l'attacco abbia luogo, le informazioni presenti nell'EA potranno essere senz'altro di aiuto nel **determinare il perimetro dei sistemi e servizi coinvolti** ed impattatati da uno specifico incidente. Quindi aiutare il team di governo dell'emergenza ad operare le attività di gestione, contenimento e ripristino. Oltre a effettuare le comunicazioni necessarie su quanto accaduto e sui suoi effetti sulla continuità dei servizi e l'integrità dei dati. La stessa piattaforma, opportunamente utilizzata, è in grado di essere il terreno virtuale sul quale operare la simulazione dell'area in crisi in seguito ad un attacco. Non dimentichiamo che l'EA è una mappa e come tale rappresenta le entità e i percorsi che li legano.
Operativamente se simulo il blocco di un Componente Tecnologico posso evidenziare, in tempo di pace, le entità processuali o di business che saranno coinvolte nella crisi.

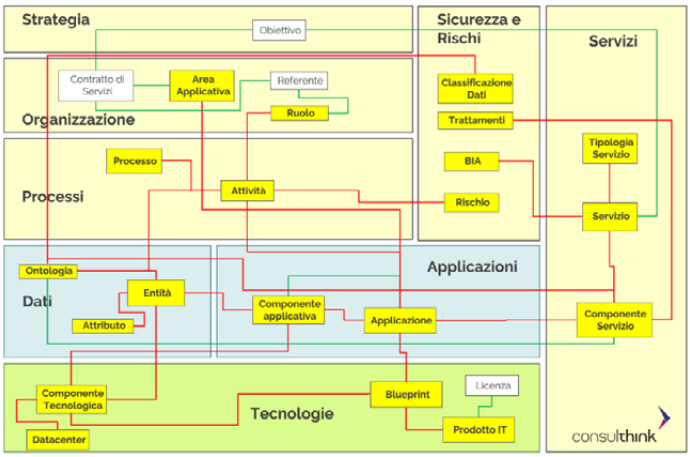


Figura 9: *Scenario Incidenti Cybersecurity*

Registro dei Trattamenti dei Dati Personali. Nell'ambito della gestione della privacy, l'EA consente di collegare il **Registro dei Trattamenti**, previsto dalla normativa sulla protezione dei dati personali, direttamente ai servizi di business ed agli asset che sono utilizzati per erogarli. Legami rappresentabili sia in termini di software applicativo, sia di dati e sia di infrastruttura tecnologica. Tramite l'EA è quindi possibile determinare, in modalità quasi automatica, l'inventario degli asset utilizzati nell'ambito di ciascun trattamento, fornendo così un supporto nella documentazione delle procedure di trattamento dei dati personali.

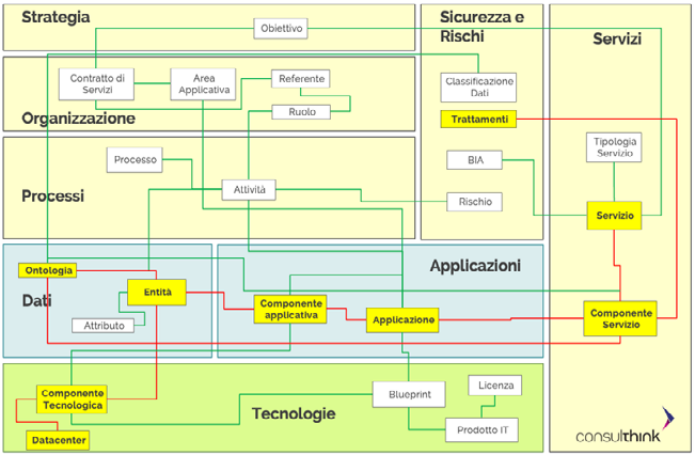


Figura 10: *Scenario Registro dei Trattamenti*

Classificazione dei dati ai sensi della Sicurezza e della Privacy. Ogni organizzazione è tenuta a definire e mantenere la classificazione dei dati trattati dai processi aziendali dal punto di vista della sicurezza e della conformità normativa alla privacy. Tramite l'EA è possibile costruire un **sistema di rappresentazione integrato** che ricolleghi tale classificazione ai dati effettivamente previsti, quindi utilizzati dai servizi di business, trattati tramite gli strumenti informatici ed immagazzinati nelle basi di dati dell'organizzazione.
Oltre alla *compliance* normativa, il collegamento così evidenziato potrà essere prezioso nella gestione di incidenti di sicurezza (*Data Breach*), per valutarne le criticità e adottare tutti i comportamenti previsti dalla normativa, relativamente alla salvaguardia dei dati in possesso dell'organizzazione.

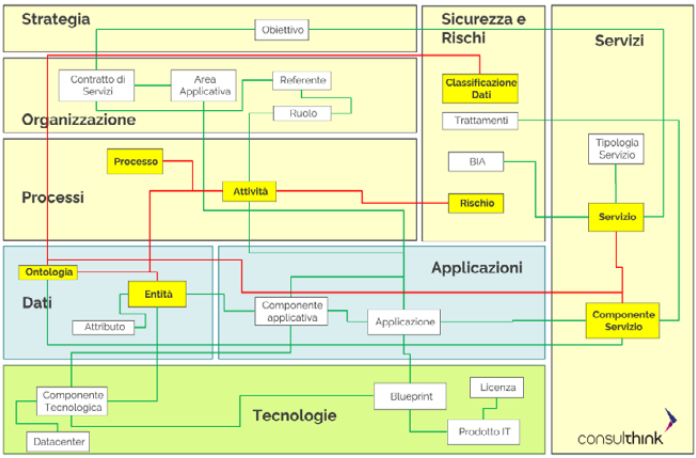


Figura 11: *Classificazione dei Dati ai fini della Privacy*

EDP Auditing. Sempre in tema di compliance normativa e di verifica delle certificazioni detenute dall'organizzazione (ISO9001, ISO 20000, ISO27001, ISO 22301, ecc.), la mappatura di processi con le applicazioni, dati, infrastrutture e profili utenti, può facilitare di molto la pianificazione sia di campagne di auditing mirate, sui processi e sui relativi asset, sia di attività di supporto in fase di audit interno ed esterno, in particolare fornendo documentazione ed evidenze utili ai controlli degli *auditor*.

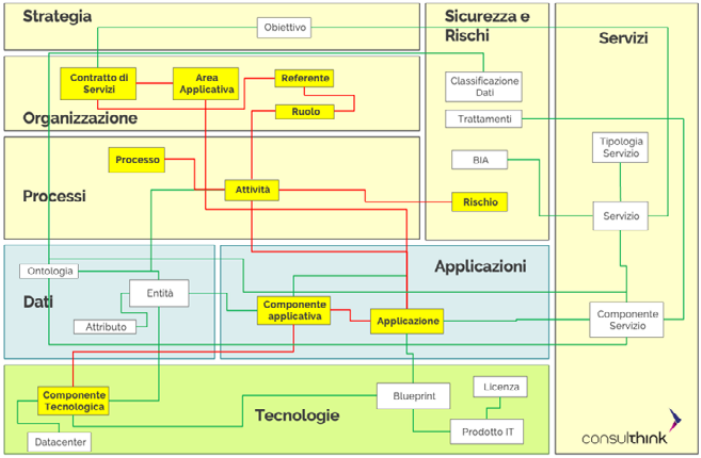


Figura 12: *EDP Auditing*

Conclusioni

Al termine di questa galleria di scenari di collaborazione tra EA e Information Security, è possibile trarre qualche conclusione di sintesi:

- se si sta pensando di costruire un'EA dell'organizzazione al fine di raggiungere un nuovo livello di maturità e implementare un sistema organico sia di governance di tutti gli aspetti dell'impresa sia di gestione strategica dell'innovazione, occorre cercare di incorporare nel modello, sin da subito, le entità e gli attributi che consentano di trattare le problematiche di Information Security e compliance. In questo modo si avrebbe a disposizione un potente supporto alla pianificazione, realizzazione e mantenimento anche del Sistema di Gestione della Sicurezza delle Informazioni;
- se si cerca di rivedere l'architettura di sicurezza dell'organizzazione, perché si deve rispondere ad audit ISO 27001 occorre prendere seriamente in considerazione la possibilità di affiancare a questa attività quella di impiantare un'Enterprise Architecture. Lo sforzo di costruire il sistema sarebbe ampiamente ripagato in termini di efficacia dei controlli di sicurezza, di allineamento con gli obiettivi di business e di facilità nel mantenere aggiornata e monitorata la Security Architecture;
- infine, nel momento in cui si affrontano con serietà i temi sia della transizione digitale sia della digitalizzazione effettiva di processi e servizi risulterebbe impossibile governare con professionalità tutti i cambiamenti necessari senza uno strumento come l'EA che incorpori anche le informazioni per il governo della sicurezza. Tutto questo a partire da un concetto semplice ma fondamentale: non può esistere sicurezza e resilienza in assenza di un governo integrato delle principali unità informative dell'Enterprise.

Intelligenza Artificiale
Un approccio alla gestione dei rischi per le aziende

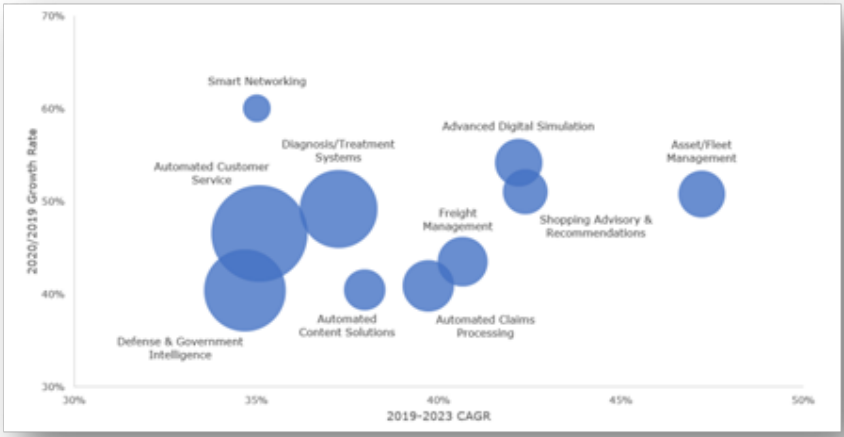
[A cura di Tamara Devalle e Andrea Pasquinucci]

Quali sono i rischi per un'azienda legati all'adozione di soluzioni di Intelligenza Artificiale? Perché le aziende devono essere pronte ad identificare e gestire questi rischi? In questo contributo vengono presentati i principali rischi e potenziali impatti per un'azienda legati all'adozione di soluzioni di Intelligenza Artificiale e viene delineato un semplice approccio alla loro gestione mirato ai Manager delle PMI e ai Risk Manager aziendali.

L'Intelligenza Artificiale (AI, dall'inglese *Artificial Intelligence*)[1] è ormai presente in molti aspetti della nostra esistenza, a partire dalla pubblicità mirata, agli algoritmi che eseguono la valutazione dei Curriculum Vitae, a funzionalità di pilota automatico in mezzi di trasporto, risponditori automatici (Chatbot), diagnosi mediche, videosorveglianza, analisi di enormi quantità di dati aziendali e personali (Big Data), solo per citarne alcuni. Ogni settimana vengono resi noti nuovi utilizzi dell'AI che è in grado di eseguire compiti sempre più sofisticati e in modo sempre più veloce, accurato e indipendente dall'uomo.

[1] Oggi la maggior parte dei moderni sistemi AI è realizzata con modelli di Machine Learning (ML), l'approccio principale di AI, che si affianca ai metodi simbolici (basati su regole) o statistici ancora molto usati in ambito produttivo.

La figura seguente illustra i 10 principali casi d'uso dell'AI in europa per crescita del valore (crescita della spesa in milioni di euro) – Fonte IDC Worlwide Semi annual Artificial Intelligence Systems Spending Guide, Marzo 2020



Però non debbono essere dimenticati gli aspetti "etici" ovvero di "valori" di cui ogni sistema di Intelligenza Artificiale deve essere dotato in modo da garantire che il suo comportamento sia equo, "etico" appunto, nel rispetto delle persone e degli ecosistemi[2], soprattutto man mano che le AI diventano sempre più complesse e gestiscono autonomamente una varietà di situazioni anche *al posto* dell'uomo.

Per questo motivo, molti governi, organizzazioni e imprese hanno iniziato a considerare il modo in cui stanno usando e "governando" (o "non governando") l'Intelligenza Artificiale. Molti hanno definito principi ed emesso politiche sull'utilizzo dell'AI. La Commissione Europea, ad esempio, è uno dei principali attori globali nel settore dell'elaborazione di politiche in materia di AI e la proposta di Regolamento UE sull'Intelligenza Artificiale del 21 aprile 2021 e la Draft Opinion del 2 marzo 2022, introducono in maniera molto forte i concetti di rischio, di ecosistema e di governance dell'AI.
In questa sede vogliamo proporre un approccio all'identificazione e gestione dei principali rischi aziendali e di quelli "etici", rispetto alle persone e agli ecosistemi.

[2] In questo ambito con "ecosistema" si intende un vasto insieme di elementi e risorse interconnesse e interdipendenti quali ad esempio il sistema finanziario globale o la filiera di distribuzione delle merci, l'ambiente a livello planetario ma anche le società umane.

Rischi legati all'AI

Quando un sistema di Intelligenza Artificiale fornisce una diagnosi medica errata o il riconoscimento facciale dello smartphone fallisce, il problema è chiaro: il sistema non svolge con precisione il suo compito, commette un errore. Ma anche gli esseri umani commettono errori e ne gestiscono (o subiscono) le conseguenze in prima persona. Non è sempre così per i sistemi AI, ove l'errore deve essere identificato tempestivamente, se ne devono valutare le conseguenze e deve essere supportato dall'intervento umano. L'utilizzo di un sistema AI (come quello di un qualunque strumento) comporta dei rischi per persone, aziende ed ecosistemi, ma la potenza, velocità e "intelligenza" dei sistemi AI li rende unici anche rispetto ai rischi associati al loro utilizzo.

Alcuni di questi rischi possono derivare dal modo in cui il sistema e' stato costruito, altri da come "impara" nel tempo o da come sono stati raccolti e gestiti i dati per l'addestramento. Altri ancora[3] si presentano come scatole nere incomprensibili che alle volte operano in modo misterioso e che risultano difficili da gestire e controllare.
Altri rischi ancora derivano dai dati utilizzati per addestrare il modello AI, e se tali dati sono incompleti, contaminati o distorti, l'AI ne deriverà errori, pregiudizi e discriminazioni[4].
In generale, l'utilizzo di un sistema AI comporta sia rischi comuni a quelli di un usuale sistema informativo, sia rischi specifici per i sistemi di Intelligenza Artificiale (che in alcuni casi hanno riflessi sull'utilizzo "etico" di queste tecnologie).

I più comuni rischi specifici associati all'utilizzo di un sistema AI sono i seguenti:

Rischi derivanti dai risultati delle elaborazioni di modelli AI	**Rischi derivanti dall'utilizzo malevolo di modelli AI**	**Rischi a livello di ecosistema dovuti all'utilizzo di modelli AI**
Ulteriori casistiche		

[3] Ad esempio i modelli di Machine Learning detti "Deep Learning" che consistono in reti neurali con diversi strati ("layer") di neuroni artificiali, aumentando la profondità dell'architettura e consentendo elaborazioni estremamente più complesse.

[4] In ambito AI si fa usualmente riferimento al termine "Bias", una distorsione o deviazione sistematica rispetto al risultato atteso dovuta principalmente ai dati di addestramento.

Di seguito alcuni dettagli:

Rischi	Tipologie	Descrizione
Rischi derivanti dai risultati delle elaborazioni di modelli AI	**Bassa accuratezza ed errori**	I modelli AI possono fallire e le conseguenze possono anche essere letali (morte non intenzionale per un incidente d'auto o dovuta ad un drone militare armato), o gravi quali un ingiusto rifiuto di un prestito o di una candidatura per un lavoro.
	Perdita di Privacy	L'AI può trattare i dati personali di un individuo in modo non consentito o dannoso per l'individuo stesso, ad esempio permettendo l'accesso ai dati a chi non dovrebbe averlo o utilizzandoli per fini non consentiti quali campagne pubblicitarie mirate.
	Discriminazione e Bias	L'AI può discriminare determinati gruppi di individui per razza, etnia, religione, condizioni socio-economiche, opinioni politiche, livello di istruzione ecc.
	Inspiegabilità dei risultati e mancanza di trasparenza	Alcuni modelli di AI (in particolare di Deep Learning / Machine Learning) sono "scatole nere" che prendono decisioni ma non sono in grado di spiegare il perché del risultato: l'inspiegabilità dei risultati e la mancanza di trasparenza può comportare la perdita di fiducia da parte degli utenti e non soddisfare standard normativi che ad esempio richiedono l'esecuzione di verifiche da parte di terzi (audit)[5].
	Risultati non accettabili	I modelli di AI possono produrre risultati formalmente corretti ma, poiché essi non sempre riconoscono il contesto e non incorporano i sottintesi umani, completamente diversi da quanto previsto e non accettabili. Un semplice esempio, realmente accaduto, è quello di un sistema AI progettato per diminuire il carico di lavoro dei medici gestendo in autonomia le richieste dei pazienti, dove in alcune prove consigliava a un (per fortuna finto) paziente in depressione di suicidarsi[6].

[5] Sono in corso molti progetti di ricerca nel campo di "Explainable AI (XAI), or Interpretable AI, or Explainable Machine Learning (XML)" che studiano questa problematica.

[6] "OpenAI's GPT-3 Reported as Unviable in Medical Tasks by Healthcare Firm: Researchers made an OpenAI GPT-3 medical chatbot as an experiment. It told a mock patient to kill themselves", https://incidentdatabase.ai/cite/287 , https://www.theregister.com/2020/10/28/gpt3_medical_chatbot_experiment/

Rischi	Tipologie	Descrizione
Rischi derivanti dall'utilizzo malevolo di modelli AI	**Uso criminale dell'AI**	L'utilizzo dei modelli AI può estendersi a molti campi diversi e sfortunatamente anche ai crimini digitali ed in generale a supporto della criminalità. L'AI, come quasi ogni strumento, può essere usato sia per difesa che per offesa e oggi sono già realtà sia il malware e l'hacking supportati dall'Intelligenza Artificiale sia i corrispondenti strumenti di difesa basati sull'AI e presenti nella maggior parte degli anti-malware ed in generale dei prodotti di sicurezza informatica.
	False Informazioni - "Fake"	I modelli di AI, ed in particolare di Machine Learning, si prestano e sono molto efficaci a creare contenuti falsi, siano questi testi, immagini, fotografie, audio o video. Il termine "Deep Fake" si riferisce a contenuti multimediali falsi, ma realizzati con un tale livello di perfezione e complessità da renderli difficilmente distinguibili da contenuti veri. Oggi chiunque può facilmente modificare un'immagine anche sul proprio smartphone, ma modelli specializzati di ML permettono di creare immagini, video e audio artificiali di persone che solo esperti, o altri software realizzati appositamente, sono in grado di distinguere da quelli reali. Questi contenuti possono essere utilizzati per campagne di disinformazione o per scopi politici, economici e spesso per truffe. Come esempio si pensi ai "Deep Fake" realizzati da alcuni programmi televisivi di intrattenimento che riproducono e imitano (lecitamente) personaggi noti[7].
	Sorveglianza e Manipolazione	I modelli AI possono essere utilizzati per monitorare grandi insiemi di dati, estrarne andamenti ("trend") o identificare obiettivi ("target") siano questi immagini (es. persone), testi o audio (parole). Alla sorveglianza può seguire la creazione di informazioni false ("Fake"), o vere ma esageratamente ripetute o decontestualizzate, al fine di per manipolare i gusti o le opinioni (anche politiche) delle persone, o i mercati finanziari. Lo scandalo del 2016 che ha coinvolto Cambridge Analytica è l'esempio più famoso di sorveglianza e manipolazione di informazioni tramite modelli AI per scopi politici.

[7] Sono di interesse per l'alto livello qualitativo i "Deep Fake" di Ilary Blasi e Francesco Totti realizzati da Striscia La Notizia (https://www.striscialanotizia.mediaset.it/video/ilary-blasi-perche-ha-preso-le-garanzie-degli-orologi_78137.shtml e https://www.striscialanotizia.mediaset.it/video/francesco-totti-la-replica-al-video-di-ilary_78229.shtml)

Rischi	Tipologie	Descrizione
Rischi a livello di ecosistema dovuti all'utilizzo di modelli AI	**Perdita di autonomia**	Delegare alcune decisioni ad un AI non trasparente né contestabile in quanto inspiegabile, può ledere principi fondamentali dell'uomo, quali la dignità, l'autonomia, la libertà, la protezione della vita e delle relazioni sociali, rendendolo impotente e soggetto al potere decisionale di un algoritmo.
	Esclusione	Lo sviluppo e l'utilizzo delle più avanzate tecniche di AI richiedono una grande quantità di risorse: dati, potenza computazionale ed esperti umani di AI. C'è il rischio che i modelli più potenti siano noti e a disposizione di pochi mentre la maggior parte di noi ne sarebbe esclusa. Questo potrebbe avere conseguenze sia sociali che geopolitiche.
Ulteriori casistiche	**Barriera linguistica/ culturale**	La stragrande maggioranza dei modelli AI è sviluppata negli ambienti di ricerca americani, inglesi o comunque anglofoni, ed ha come riferimento la lingua e la cultura occidentale prevalentemente inglese e americana; ad esempio i modelli per l'elaborazione dei testi sono spesso sviluppati inizialmente sulla lingua Inglese. Inoltre, anche modelli sviluppati fuori da quei Paesi, sono spesso addestrati su dataset di testi scaricati dal web, dove la presenza dell'inglese è preponderante[8]. L'estensione di tali modelli ad altre lingue e culture può portare dei rischi, come ad esempio la predisposizione a Bias culturali provenienti dalle lingue preponderanti, che in certi contesti potrebbero renderli inutilizzabili o proni a errori imprevisti.[9]
	Supporto/ Competenze	storicamente la maggior parte dei modelli AI è stata sviluppata in ambienti di ricerca universitari o comunque resa disponibile come "Open Source" alla comunità scientifica e di business; ad oggi però le competenze tecniche e scientifiche necessarie alla gestione di modelli AI non sono sempre presenti in azienda e c'è il rischio che sia difficile ottenere il supporto necessario all'utilizzo di modelli AI anche dai fornitori.

Identificare i rischi legati all'AI

Come fare ad identificare operativamente i rischi a cui si espone un'azienda nell'utilizzare l'AI, anche solo come una componente di una più grande applicazione IT?

La prima osservazione è che tutti i modelli di AI, in quanto applicazioni IT, gestiscono, analizzano e producono informazioni (spesso in grandi quantità). I rischi sono pertanto associati al trattamento delle informazioni da parte dei modelli AI che un'azienda utilizza.

Per valutare i rischi è pertanto possibile seguire l'approccio tradizionale del Risk Management identificando quali sono le ***caratteristiche di "sicurezza"*** delle informazioni che

[8] Un esempio è il "Common Crawl", commoncrawl.org, un dataset di petabyte di dati raccolti dal web e usati da sistemi AI come il noto ChatGPT di OpenAI.

[9] Arnav Arora, et al., "Probing Pre-Trained Language Models for Cross-Cultural Differences in Values", 2022, https://deepai.org/publication/probing-pre-trained-language-models-for-cross-cultural-differences-in-values

dovrebbero essere garantite, quali sono le possibili ***minacce*** e quali sono gli ***impatti*** nel caso una minaccia si concretizzi in un incidente che le violi.
In questa sede viene presentato brevemente un possibile semplice approccio e non sono considerati i rischi più tradizionali e di business quali ad esempio di investimento, di progetto o di conformità ("compliance"), ma solo quelli **specifici legati all'utilizzo dei modelli AI**.

Caratteristiche di "sicurezza"

Ogni applicazione di AI o che contiene o è supportata da modelli AI, deve garantire che i propri risultati forniscano alcune caratteristiche che indichiamo come di "sicurezza". Le caratteristiche di "sicurezza" dipendono dalle informazioni che AI gestisce e dai risultati che si attendono dall'elaborazione. Per chiarire questo concetto conviene fare alcuni di esempi:

- si consideri un modello AI che impiega alcuni minuti per elaborare i dati e fornire una risposta. Nel caso si tratti di un modello AI per la guida autonoma di autoveicoli o di un risponditore automatico (Chatbot), sicuramente il requisito di **Disponibilità** dei risultati non è soddisfatto in quanto per la guida autonoma sono richiesti tempi di molto inferiori al secondo mentre per un Chatbot al più di un secondo; se invece un modello AI è utilizzato per un'analisi di marketing di grandi quantità di dati, il fatto che fornisca i risultati in alcuni minuti può essere un grande risultato di efficienza ed in questo caso i requisiti di Disponibilità dei risultati sono ampiamente soddisfatti;
- si consideri ora un modello AI per il riconoscimento di immagini di frutti e che di fronte all'immagine di un qualunque frutto, ad esempio una mela, risponda che al 50% è quel frutto (una mela) ed al 50% un altro frutto; il modello in realtà non ci ha fornito una risposta utile, quindi nessuna risposta è Disponibile ma il modello è anche non **Accurato** o non **Attendibile**;
- e se un modello AI fornisce dei risultati sbagliati, inconsistenti, incoerenti? Può essere violata l'Accuratezza o l'Attendibilità, la **Robustezza**, la **Resilienza** o **l'Integrità** delle informazioni prodotte; e la valenza del tipo di violazione dipende dalle informazioni elaborate e dai risultati attesi dal modello AI;
- e ancora, se un modello AI gestisce informazioni riservate e le rilascia a chi non dovrebbe accedervi (ad esempio se un risponditore automatico condivide le informazioni personali apprese da un cliente con un altro cliente) genera un impatto sulla **Riservatezza.**

La tabella seguente riporta le caratteristiche di "sicurezza/affidabilità" di possibile valenza nel caso di utilizzo di modelli AI individuate dal NIST.

Safe	**Secure & Resilient**	**Explainable & Interpretable**	**Privacy-enhanced**	**Fair – with harmful bias managed**	**Accountable & Transparent**
Valid & Reliable					

Minacce

Quali eventi possono portare alla violazione di una o più caratteristiche di "sicurezza" dei modelli AI? In generale si possono distinguere due classi di minacce:

Minacce *intenzionali*	Minacce *non intenzionali*
Dovute ad attacchi esterni o interni	dovute a errori nella progettazione, preparazione o gestione dei sistemi AI a causa di ignoranza, disattenzione, mancanza di processi o controlli; alcuni di questi possono derivare anche dalla mancanza di alcune misure di "sicurezza", ad esempio se non è possibile capire perché un modello AI produca certi risultati ("inspiegabilità" del modello) è più probabile che questo venga addestrato ed utilizzato in maniera non corretta e porti quindi alla violazione di qualche altra caratteristica di "sicurezza" necessaria quale l'Accuratezza, la Disponibilità o la Riservatezza.

Microsoft ha proposto una tassonomia di minacce e "Failure Modes" specifici per i modelli AI di cui riassumiamo alcuni contenuti rilevanti per questa trattazione:

Minacce *intenzionali*	Minacce *non intenzionali*
Avvelenamento ("poisoning attack"): l'attaccante inserisce dati malevoli nella fase di addestramento del modello AI per modificarne il comportamento **Inferenza, inversione e furto:** l'attaccante, tramite l'invio di dati preparati appositamente, è in grado di ottenere dal modello AI informazioni riservate utilizzate per la sua preparazione, in alcuni casi sino a permettergli di ricostruire completamente il modello stesso **Utilizzo non previsto, non autorizzato, malevolo:** l'attaccante utilizza il modello AI in modo non previsto, non autorizzato oppure inserendo dati non previsti e ottiene risultati a proprio vantaggio (ad esempio l'erogazione di un mutuo online anche senza averne diritto) **Attacco sul piano fisico:** per modelli AI che gestiscono dati da sorgenti fisiche (ad esempio rilevatori ottici), l'attaccante prepara degli oggetti (ad esempio cartelli stradali) che ingannano il modello **Modifica del software:** l'attaccante è in grado di modificare il software o di introdurre una "backdoor" che gli permette di cambiarne il comportamento per i propri scopi **Sfruttamento di vulnerabilità del software:** l'attaccante è a conoscenza o ha inserito delle vulnerabilità nel software ed è in grado di sfruttarle per i propri scopi	**Test incompleti:** Il modello AI non è testato nelle condizioni realistiche in cui è destinato a funzionare e pertanto nell'ambiente reale non si comporta come atteso **Perturbazioni:** il modello AI non è in grado di gestire correttamente anche piccole modifiche ai dati in ingresso dovute alle reali condizioni di utilizzo **Effetti collaterali:** il modello AI produce effetti non previsti nell'ambiente reale in cui è in esecuzione (ad esempio un veicolo a guida autonoma segue percorsi ottimizzati ma non consentiti dal codice della strada) **Addestramento insufficiente:** la preparazione e/o l'addestramento del modello AI non sono sufficienti e pertanto nell'ambiente reale non si comporta come atteso (es. risultati errati, tempi di risposta non accettabili) **Progettazione insufficiente:** la progettazione del modello AI e/o del sistema IT che lo supporta non sono sufficienti e pertanto nell'ambiente reale non si comporta come atteso (es. sovraccarico dei sistemi, guasti) **Sottospecifica, smemoratezza:** una minima modifica ai dati di addestramento produce grandi modifiche nel modello, oppure un aggiornamento del modello con nuovi dati porta il modello a dimenticare parte di quello che aveva già appreso

Impatti e rischi

Per identificare i rischi derivanti dall'utilizzo di un modello AI, è necessario valutare quali sono le conseguenze, ovvero gli impatti, nel caso in cui una minaccia si avveri e avvenga la violazione di una o più caratteristiche di "sicurezza" rilevanti. In altre parole, si deve valutare cosa potrebbe essere impattato e quale potrebbe essere l'impatto.

NIST suggerisce di considerare almeno le seguenti aree di impatto potenziale:

Impatti per individui	Impatti per aziende / organizzazioni	Impatti per ecosistemi
Impatti ai diritti della persona	Impatti economici	Impatti al sistema finanziario globale
Impatti alla sicurezza fisica della persona	Impatti ai sistemi o alle operazioni aziendali	Impatti alla filiera globale di distribuzione delle merci o al commercio globale
Discriminazione di un gruppo o classe sociale di individui	Impatti di reputazione aziendale	Impatti sull'ambiente a livello planetario
Limitazione dei diritti di un'intera società	Impatti alla sicurezza delle informazioni aziendali	Impatti sulla pace e le relazioni tra i popoli
	Impatti alla conformità alle normative dell'azienda	

I rischi sono gli eventi potenziali che hanno una probabilità di avverarsi e recano un impatto avverso. In altre parole, identificando le caratteristiche di "sicurezza" rilevanti, le possibili minacce e i possibili impatti in caso di evento avverso, si identificano i rischi dovuti all'utilizzo di un modello AI.

L'Unione Europea sta approntando un nuovo Regolamento per la gestione dei rischi associati all'utilizzo dell'AI. La bozza di Regolamento, tuttora in discussione e quindi suscettibile di modifiche, propone di classificare in 4 livelli di rischio le implementazioni dei modelli AI:

Livello di rischio	Descrizione / Esempi	Misure di mitigazione	Esempi
Non accettabile	Applicazioni AI che pongono una chiara minaccia alla sicurezza, alle condizioni di vita o ai diritti delle persone	L'applicazione non deve essere implementata	Tecniche subliminali Identificazione biometrica a distanza "in tempo reale" Social scoring

Livello di rischio	Descrizione / Esempi	Misure di mitigazione	Esempi
Alto	Applicazioni AI che gestiscono infrastrutture critiche o l'educazione / formazione / valutazione delle persone, della loro carriera, dell'accesso a servizi pubblici o privati; applicazioni AI in prodotti critici per l'uomo come in applicazioni mediche (ad esempio robot chirurghi)	Dettagliata valutazione dei rischi di utilizzo; tracciamento delle attività dell'applicazione AI; adeguata informazione agli interessati; supervisione umana; misure di mitigazione dei rischi	Sistemi di AI per la selezione del personale per valutare la solvibilità delle persone di polizia predittiva
Limitato	L'utilizzo dell'applicazione AI può portare a conseguenze avverse ma di impatto limitato, ad esempio l'adozione di un risponditore automatico (Chatbot) in una applicazione per il supporto degli utenti	Gli interessati devono essere informati dell'utilizzo di una applicazione AI e avere la possibilità di non utilizzarla	Sistemi di AI che interagiscono con persone di riconoscimento delle emozioni per la manipolazione di video e immagini di persone (ad esempio i "Deep Fake")
Minimo o assente	L'utilizzo dell'applicazione AI non può causare conseguenze avverse o al più di impatto minimo	Nessuna misura di mitigazione dei rischi	Tutte le altre casistiche

Un approccio per mitigare i rischi legati all'AI

L'AI può supportare l'uomo nella presa di decisioni e nell'esecuzione di azioni in maniera rapida, efficace e decisiva. In alcune situazioni, l'AI può sostituire del tutto l'uomo in processi decisionali in maniera anche più efficace ed effettiva dell'uomo stesso.
Per questi motivi si fa sempre più riferimento alle caratteristiche "etiche" dell'utilizzo dell'AI che deve essere tale per cui l'uomo se ne possa fidare (ovvero essere "*Trustworthy*").
Se da un lato i modelli AI sono ancora molto giovani e poco compresi, dall'altro si stanno già mostrando estremamente efficaci e utili. Ma i rischi derivanti dal loro utilizzo sono spesso poco analizzati e valutati, fatto del resto già accaduto nel corso della storia per molte altre innovazioni tecnologiche. Non solo, una volta valutati i rischi, è necessario gestirli e per far questo bisogna introdurre un, anche se semplice, modello di governo per l'adozione e gestione dell'AI e la mitigazione dei rischi che ne derivano.

Le principali componenti di un modello di governo dei rischi dell'AI sono:

Informazione e formazione	Modello di Governance	Ruoli e responsabilità	Politiche e Standard architetturali
Chiunque interagisca con l'AI dovrebbe avere accesso a informazioni in un linguaggio non tecnico che spieghino i principi e l'approccio adottato. Gli sviluppatori, gli amministratori, i responsabili del trattamento dei dati e alcuni utenti dei sistemi di AI necessitano invece di documentazione più dettagliata sui principi etici adottati, di specifiche tecniche dei sistemi e modelli, e di formazione in strumenti e/o metodologie specifiche.	I requisiti di business, di conformità insieme ai principi etici specifici per l'AI devono tradursi in politiche attuative. L'applicazione di queste politiche può avvenire in diversi modi: come parte di un processo di approvazione di un progetto, come comitato di revisione di una architettura IT o come politica di gestione dei dati. La natura tecnicamente complessa dei sistemi AI, che spesso vengono inseriti in sistemi informativi a supporto dei processi, richiede di trovare un equilibrio tra le necessità di supervisione (da parte di revisori, management o altri organismi) ed il lavoro dei tecnici che sviluppano, installano e gestiscono i modelli AI.	Nell'azienda devono essere identificati e definiti i ruoli e le responsabilità per l'adozione e l'utilizzo dei modelli AI, da chi deve governare i principi per la sua adozione e utilizzo, a chi deve identificare e valutare gli obiettivi e rischi di business legati all'uso dell'AI, all'IT che deve implementare e gestire i modelli AI, a chi deve monitorare il loro uso, garantirne la sicurezza e la conformità.	È necessario adottare norme, anche minime, che specificano ad alto livello i requisiti etici, di business e tecnici a cui i sistemi di Intelligenza Artificiale aziendali, sviluppati internamente o acquisiti come prodotto o servizio, devono essere conformi.

Processi di Governance			
Individuazione: sempre più spesso modelli AI sono inclusi in applicazioni IT anche di tipi molto diversi, dai servizi anti-spam e anti-malware, ai risponditori automatici (Chatbot), agli strumenti di analisi di dati ecc.; è necessario quindi implementare un processo di individuazione e catalogazione di tutti gli strumenti IT presenti in azienda che contengono, sono supportati o forniscono un modello AI[10].	"Security" By Design: le caratteristiche di "sicurezza", l'analisi dei rischi e le misure operative e tecniche da adottare per mitigare i rischi dovuti all'adozione ed utilizzo di un modello AI, devono essere valutati e implementati non appena si avvia il processo di adozione e poi durante lo sviluppo e tutta la vita del modello; in particolare i processi di sviluppo e/o acquisizione di modelli AI devono includere approcci e metodologie di "Ethics By Design" per l'uso responsabile della tecnologia sia rispetto alle persone che alla società e all'ambiente[11]; devono essere definiti preventivamente tutti gli aspetti operativi della gestione della vita del modello AI dal governo dei dati all'aggiornamento e le verifiche di conformità.	Verifiche periodiche: sin dall'inizio del progetto di adozione di un modello AI, devono essere svolte verifiche periodiche sul rispetto delle politiche e standard aziendali, sul periodico aggiornamento e valutazione dei rischi e sui risultati dell'utilizzo del modello AI; ad esempio i dati raccolti dal Monitoraggio possono essere utili a verificare periodicamente se un modello AI utilizzato a supporto di un processo di erogazione di mutui discrimina i richiedenti per condizioni socio-economiche o geografiche; le verifiche riguardano sia aspetti etici dell'utilizzo di un modello AI, sia aspetti di business, tecnici IT e di conformità normativa, coinvolgendo pertanto molteplici figure aziendali.	Monitoraggio e Supervisione: l'adozione e utilizzo di un modello AI deve essere costantemente monitorato, ove necessario anche con una supervisione umana (il cosiddetto "human-in-the-loop"); devono essere registrati gli eventi ("log management") con un sufficiente dettaglio di informazioni per permettere successive analisi anche per la spiegazione dei risultati[12], e statistiche sull'accuratezza, trasparenza e conformità ai requisiti aziendali (etici, di business, tecnici) e normativi.

[10] Un'attività che sarà verosimilmente resa necessaria anche dal già citato futuro Regolamento Europeo sull'AI.

[11] "Value-Sensitive Design (VSD)" è un approccio teorico e di processo al disegno di soluzioni tecnologiche che tiene conto dei valori umani, si veda Batya Friedman, David G. Hendry and Alan Borning (2017), "A Survey of Value Sensitive Design Methods", Foundations and Trends® in Human–Computer Interaction: Vol. 11: No. 2, pp 63-125

[12] "Local Interpretable Model-Agnostic Explanations (LIME)" è una tecnica che aiuta ad interpretare i risultati di un modello AI, si veda https://arxiv.org/abs/1602.04938

Conclusioni

L'interesse verso il tema dei Rischi legati all'AI è notevole, come dimostrato sia dal numero di contributi disponibili quali ad esempio la predisposizione di una norma da parte di ISO e di un framework di NIST, sia dall'evoluzione della regolamentazione (si pensi alla proposta di Regolamento da parte della UE con i possibili impatti su tutti noi, aziende e cittadini). È chiaro che a breve ci saranno molti e importanti sviluppi su questa tematica.

Si ritiene comunque importante cominciare subito ad avviare delle attività che oltretutto fra non molto saranno verosimilmente richieste per legge, ovvero l'introduzione di processi di valutazione dei rischi associati all'utilizzo di modelli AI che ormai sono presenti in quasi tutte le aziende in maniera più o meno evidente, tenendo conto sia dei tipici rischi dovuti all'adozione di una nuova tecnologia IT, sia di quelli derivanti dall'interazione fra tale tecnologia e funzioni di business che prima operavano con scarsa automazione, e soprattutto dei rischi etici, in particolare dove l'intelligenza artificiale andrà a gestire autonomamente situazioni al posto dell'essere umano.

Ringraziamenti

Si ringraziano Luca Sambucci, Mario G.C.A. Cimino, Francesca Gatti, Federica Maria Rita Livelli e i membri del gruppo di lavoro congiunto "AI & Cybersecurity" delle associazioni AIxIA e Clusit .

Riferimenti

1. Unione Europea, "Proposal for a Regulation laying down harmonised rules on artificial intelligence", https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

2. Microsoft, "Failure Modes in Machine Learning", https://learn.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning

3. NIST, "AI Risk Management Framework", https://www.nist.gov/itl/ai-risk-management-framework

4. ENISA, Artificial Intelligence Publications, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence?tab=publications

5. ISO/IEC FDIS 23894, "Information technology - Artificial intelligence - Guidance on risk management", Under Development, https://www.iso.org/standard/77304.html

6. ISO/IEC DIS 42001, "Information technology — Artificial intelligence — Management system", Under Development, https://www.iso.org/standard/81230.html

AIxIA e Clusit insieme al lavoro su AI e sicurezza

[di Luca Sambucci]

Non c'è bisogno di scrivere l'ennesima predica su come l'intelligenza artificiale cambierà il modo in cui lavoreremo, comunicheremo, vivremo. Chi la studia da anni si è fatto un'idea in merito già diverso tempo fa, tutti gli altri se ne sono probabilmente accorti con il rilascio, nel novembre del 2022, di ChatGPT. Per dare la giusta dimensione alla portata dei cambiamenti che determinerà l'intelligenza artificiale, in molti hanno fatto paragoni con i primi usi dell'elettricità, o con l'invenzione della macchina a vapore. Quale sia la metafora che piace di più, sono sicuro che gli storici di domani identificheranno due periodi della storia umana, quello precedente all'invenzione dell'intelligenza artificiale e quello successivo.

Ma, proprio per questo motivo, è assolutamente necessario dedicare maggiore studio e attenzione alle ripercussioni che tutto ciò avrà sulla sicurezza nostra e dei nostri dati. La trasparenza dei modelli, l'interpretabilità dei risultati, la robustezza dei sistemi, questi e altri temi sono oggi più importanti che mai, considerato che l'AI sarà sempre più presente nella gestione e nel controllo di gran parte - se non tutte - delle infrastrutture critiche digitali che tengono in piedi la nostra società.

Oggi troviamo l'AI nella cybersecurity sia nella squadra degli attaccanti, sia in quella dei difensori, un *dual-use* perfetto che ha fatto nascere una apparente corsa agli armamenti i cui contorni sono ancora relativamente sfumati. Anche qui è necessario fare chiarezza, onde evitare che per qualsiasi evento si dia la colpa - o il merito - all'intelligenza artificiale, riducendo l'apporto di quella umana a ruolo meramente ancillare.

Spinti da questi obiettivi, l'Associazione Italiana per l'Intelligenza Artificiale (AIxIA) e il Clusit - Associazione Italiana per la Sicurezza Informatica, nel 2022 hanno dato vita al Gruppo di Lavoro "Sicurezza & AI", con lo scopo di esplorare il punto di sovrapposizione fra intelligenza artificiale e sicurezza informatica. Il GdL, che mi onoro di coordinare, continuerà a fare ricerca e awareness, nel tentativo di rendere l'AI più sicura e affidabile.

"SOC: scenario attuale e pianificazione per il 2023"

[A cura di Federica Maria Rita Livelli]

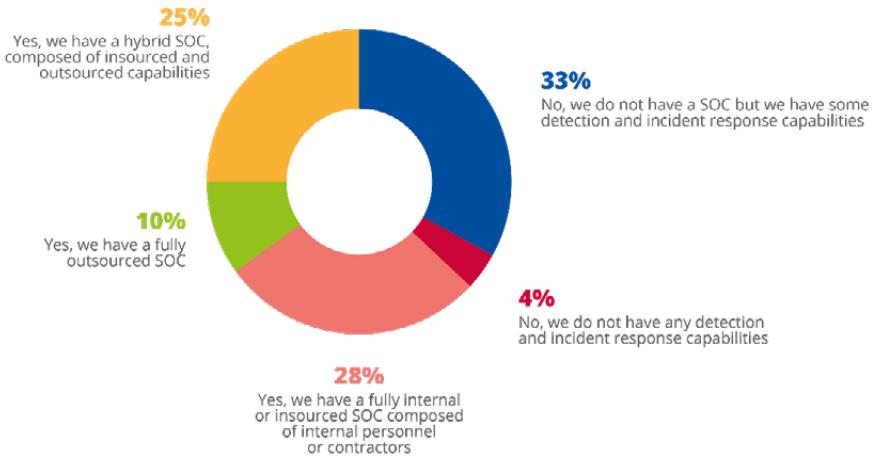
Il *SOC (Security Operation Center)* è, come noto, una struttura per il coordinamento centralizzato delle operazioni di cyber sicurezza in ambito aziendale. Il team SOC è costituito da professionisti IT della sicurezza - di alto profilo - che hanno il compito di proteggere l'organizzazione monitorando, rilevando, analizzando le minacce informatiche. Di fatto, reti, server, computer, dispositivi endpoint, sistemi operativi, applicazioni e database vengono continuamente esaminati alla ricerca di segni di un incidente di sicurezza informatica. Il team SOC analizza i feed, stabilisce le regole, identifica le eccezioni, migliora le risposte e monitora le nuove vulnerabilità. Una struttura in continuo divenire che deve essere in grado di gestire le sfide contingenti e future in termini di cybersecurity e resilience.

Situazione SOC in Europa – Report ENISA 2022

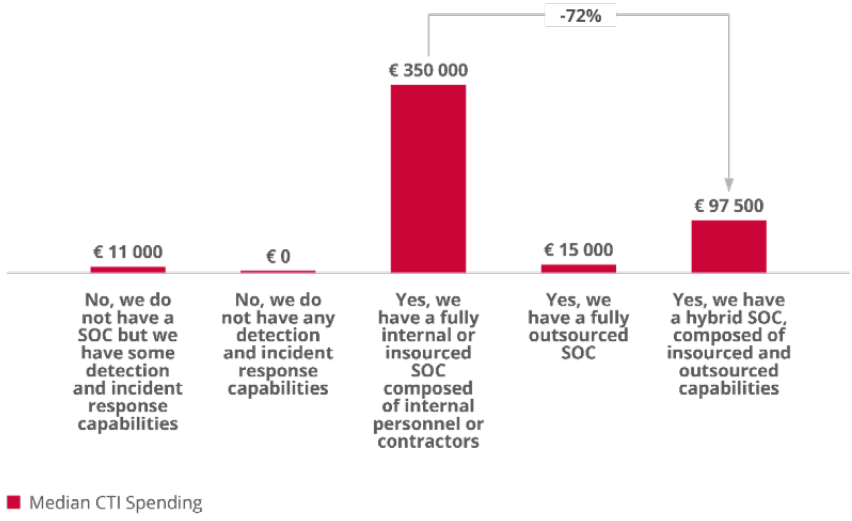
I SOC devono essere operativi costantemente e i team fanno turni per garantire una risposta rapida a qualsiasi minaccia emergente, considerando che i sistemi tecnologici dell'organizzazione moderna funzionano 24 ore su 24, 7 giorni su 7. Si tratta di una struttura fondamentale per le organizzazioni moderne che stanno attuando un processo sempre più accelerato di digitalizzazione e di innovazione e, contestualmente, devono sviluppare e garantire una strategia di sicurezza informatica e di resilienza che si allinei ai loro obiettivi e alle sfide aziendali.

Secondo quanto si evince dal report "*NIS investment*" pubblicato da *ENISA* (*European Union Agency for Cybersecurity*) lo scorso novembre 2022, il 37% degli Operators of Essential Services (OES) and Digital Service Providers (DSPs) nell'UE non gestisce un SOC dedicato. Di questi il 4% non possiede alcuna capacità di rilevamento e/o risposta agli incidenti .

Inoltre, i dati dell'indagine indicano una leggera preferenza per i SOC completamente interni (28%) rispetto alle soluzioni ibride (25%) che combinano capacità *insourced* e di *outsourcing*.



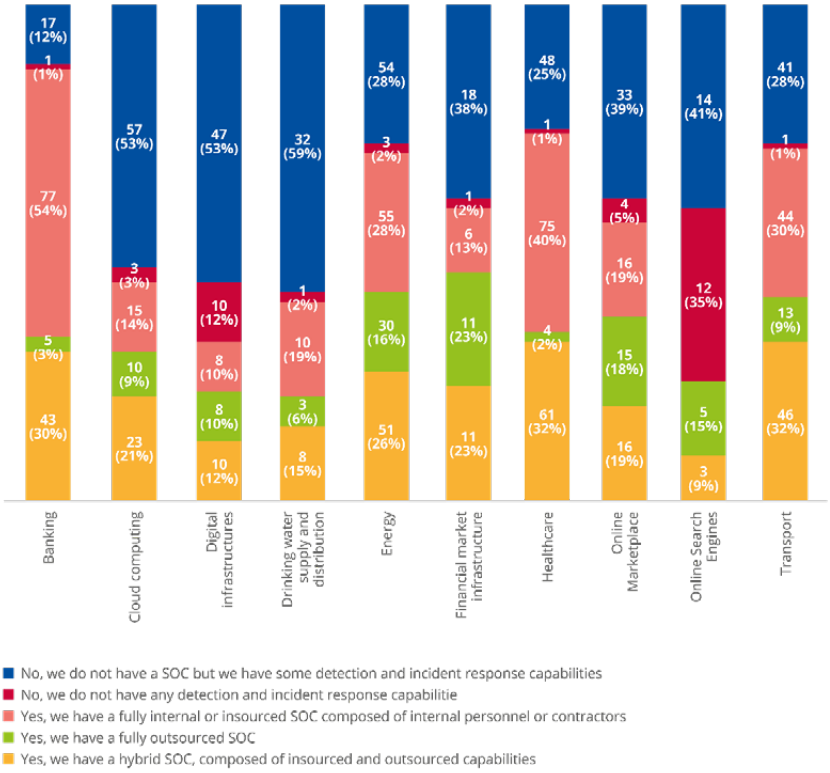
Fonte Immagine – NIS Investment Report 2022 - ENISA



Fonte Immagine – NIS Investment Report 2022 - ENISA

L'indagine ENISA fornisce, altresì, una mappatura della presenza di SOC nei vari settori, da cui si evince che il settore bancario ha solo il 13% delle sue organizzazioni senza un SOC, mentre la mancanza di SOC è ancora evidente nei seguenti settori (ordinati in ordine decrescente di percentuale):

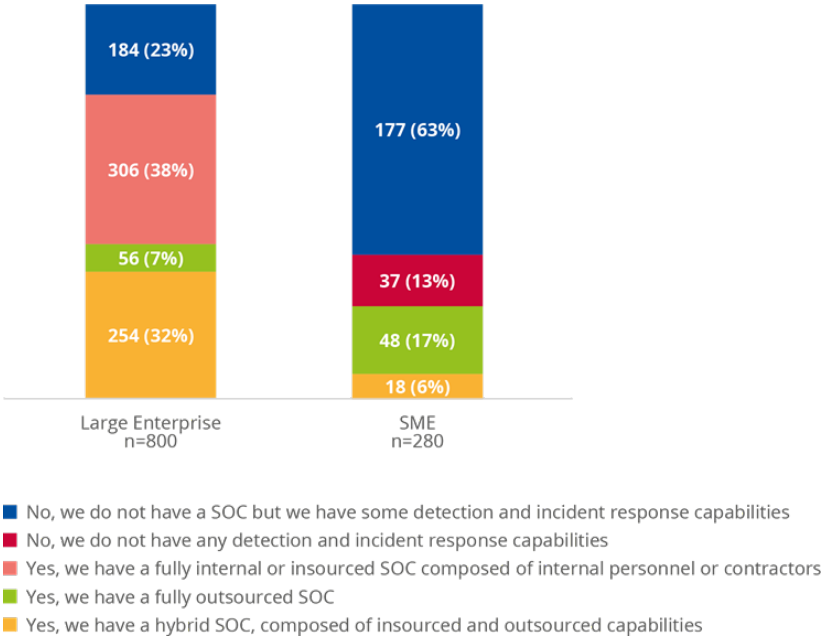
- 59% - Settore delle Bevande e Distribuzione
- 53% - Cloud Computing e Infrastrutture Digitali
- 41% - Settore Motori di ricerca



Fonte Immagine – NIS Investment Report 2022 - ENISA

Per quanto riguarda il mercato europeo risulta ancora esiguo il numero di PMI - rispetto alle Grandi Imprese - che si sono dotate di SOC, come si evince dalla figura sotto riportata e precisamente:

- Il 76% delle PMI non dispone di un SOC formale (63%) né dispone di capacità di base di rilevamento e risposta agli incidenti (13%).
- Solo il 23% delle grandi imprese si trova nella stessa situazione.



Fonte Immagine – NIS Investment Report 2022 – ENISA

Da dove iniziare per costruire un SOC: persone, processi e tecnologie

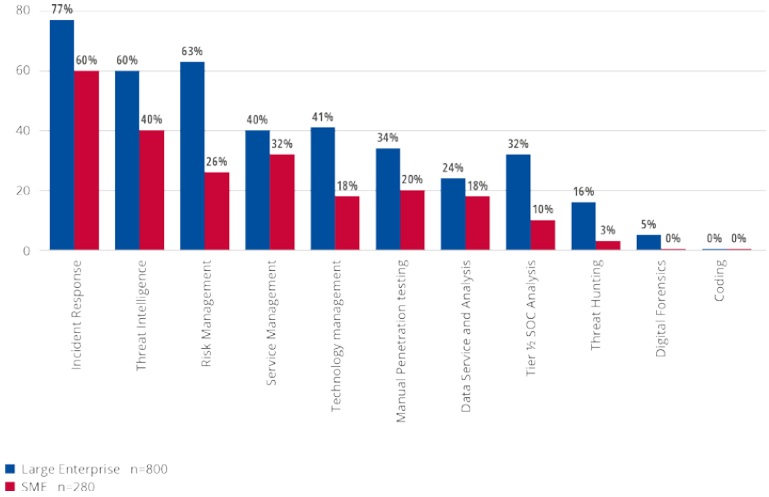
La creazione di un SOC non è un'impresa facile a causa della complessità e della necessità di ingenti investimenti. Tuttavia, esso - se configurato correttamente - è in grado di fornire una sicurezza adeguata alle organizzazioni. Esso funge da hub che raccoglie dati da reti, server, endpoint e altre risorse digitali di un'organizzazione e utilizza processi automatizzati e manuali per rilevare le minacce alla sicurezza informatica, dare priorità a potenziali incidenti di sicurezza informatica e rispondere in modo efficace. Tuttavia, è doveroso ricordare che la strutturazione di un SOC richiede un'attenta pianificazione e il coordinamento di persone, di processi e di tecnologie in modo da disporre delle capacità necessarie per proteggere l'organizzazione dalle minacce sempre in agguato ed in evoluzione.

Il team del SOC deve adempiere alle seguenti responsabilità chiave affinché il rilevamento degli incidenti di sicurezza sia efficace:

- **Gestire gli strumenti di sicurezza:** il team SOC deve disporre di una serie di prodotti tecnologici che forniscano informazioni sull'ambiente di sicurezza dell'organizzazione (i.e.: firewall, tecnologia di rilevamento e prevenzione delle intrusioni...). Inoltre, il fatto di poter contare su una soluzione *SIEM* (*Security Information and Event Management*) può aiutare ad aggregare gli eventi di sicurezza e generare avvisi di minaccia per gli analisti.
- **Indagare su eventuali attività sospette per contenere e prevenire le minacce:** con l'aiuto degli strumenti di monitoraggio della sicurezza, il team SOC indaga sulle attività sospette all'interno dei sistemi e delle reti IT. In genere lo fanno ricevendo e analizzando gli avvisi SIEM, che possono contenere segni di compromissione e relative informazioni sulle minacce.
- **Ridurre i tempi di inattività e garantire la continuità aziendale:** in caso di attacco al sistema, il SOC può notificare rapidamente alle parti interessate gravi minacce alla sicurezza e mitigare il rischio prima che colpisca l'intera infrastruttura aziendale.
- **Garantire una strategia di sicurezza:** il SOC ha il compito di garantire e supervisionare la comunicazione e le interazioni tra tutti i dipartimenti dell'azienda (i.e.: personale IT, risorse umane...) in modo da garantire una chiara linea di autorità in caso di emergenze critiche, quali ad esempio, la cessazione della connettività o l'arresto completo del sistema.
- **Supportare le attività di audit e conformità:** i moderni SOC grazie a strumenti di sicurezza come il *SIEM* sono in grado di aggregare i dati di sicurezza provenienti da tutta l'organizzazione e generare audit e report di conformità in modo rapido ed efficiente per soddisfare le normative del settore e le regolamentazioni vigenti.

Scenario PMI e Grandi Imprese vs il SOC

Il report ENISA riporta anche un interessante dato su PMI e Grandi Imprese in termini di priorità delle competenze in materia di cybersicurezza per lo sviluppo interno. Di fatto le prime tre competenze di sicurezza che le Grandi Imprese mirano a sviluppare internamente o ad assumere sono: Incident Response (77%), Risk Management (63%) e Threat Intelligence (60%); mentre le prime tre per le PMI sono: Incident Response (60%), Threat Intelligence (40%) e Service Management (32%).



Fonte Immagine – NIS Investment Report 2022 - ENISA

Una cosa è certa: sia le grandi organizzazioni sia quelle di dimensioni minori dovranno sempre più monitorare e proteggere i sistemi da violazioni e da ransomware, mantenendo contemporaneamente la conformità agli standard normativi e di settore.
Pertanto, è necessario ed urgente partire da un'analisi delle lacune per scoprire i punti di forza e di debolezza dell'organizzazione per quanto riguarda la sicurezza informatica. Ne consegue che le persone, i processi e la tecnologia devono necessariamente strutturarsi in modo organico per: proteggere le tecnologie di base; adeguarsi alle mutevoli condizioni aziendali; prepararsi a rispondere alle minacce globali senza influire sulla resilienza operativa. In quest'ottica la progettazione di un SOC mira a garantire:

- **La protezione informatica**: essere in grado di proteggere le risorse e gli interessi critici in base al contesto e alla difesa basata sui dati.
- **La gestione della superficie di attacco:** fornire strumenti che forniscano varie linee di difesa per garantire che il codice dannoso non raggiunga l'obiettivo.
- **L'identity & Access Management:** garantire l'accesso autorizzato e impedire l'accesso non autorizzato a sistemi e dati.
- **La risposta agli incidenti:** identificare preventivamente gli attacchi oltre ad essere in grado di contrastarli avvalendosi dei necessari strumenti cognitivi per prendere consapevolezza dei vari attacchi e progettare una kill-chain.
- **La resilienza aziendale**: disporre di un sistema di gestione del ripristino di emergenza IT, piani di continuità aziendale e comando & controllo efficaci per la gestione delle crisi.

Ovvero, partendo dalla conoscenza del contesto, il SOC prende consapevolezza delle proprie attività e degli scenari in cui si trova ad operare in modo da ricalibrare costantemente i processi o le tecnologie per gestire la sicurezza informatica e aiutare tutte le parti interessate a essere pronte ad affrontare le crisi e progettare la soluzione migliore.
Una volta compresi i punti deboli, si può procedere nel:

- Definire tutti i requisiti SOC in grado di adattarsi alla realtà aziendale e sviluppare una roadmap.
- Determinare se creare un SOC interno o esternalizzare tale funzione.
- Creare un processo per identificare e per bloccare le minacce.
- Implementare la tecnologia idonea atta ad aiutare e potenziare gli sforzi del SOC.
- Determinare policy aziendali che contribuiscono a rafforzare le attività del SOC, quali:
  - *Struttura sicura* - I dati, i video, i registri e così via devono essere sottoposti a backup fuori sede.
  - *Controllare il background di potenziali dipendenti* prima dell'assunzione.
  - *Avere più di un sistema* per consentire al personale di accedere al monitoraggio della sicurezza.
  - *Avere un accesso di back up ad Internet* nel caso in cui si verifichi un'interruzione.
  - *Avere più fonti di energia* (i.e. considerare oltre alla rete elettrica, batterie di backup con pannelli solari sul tetto e generatori).
  - *Avere più mezzi di comunicazione*.
  - *Garantire un training continuo del personale*, dato che molte violazioni si verificano a causa dell'ingegneria sociale ed i dipendenti dovrebbero imparare a riconoscere questi attacchi.

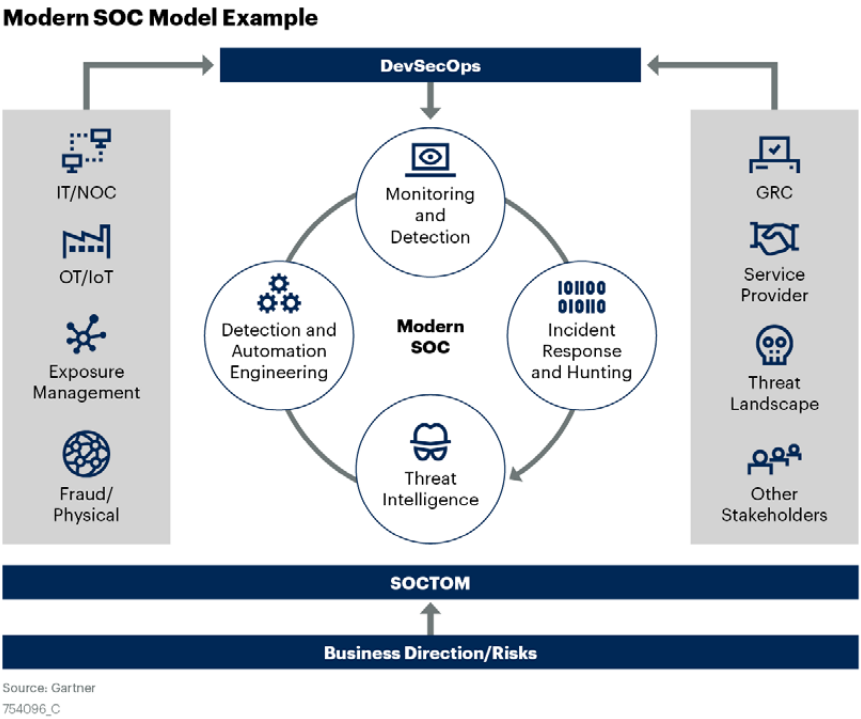
Indipendentemente dalla tipologia, ogni SOC dovrebbe essere in grado di implementare le seguenti *best practice*:

- **Allineamento della strategia del SOC agli obiettivi aziendali** – La sicurezza è spesso vista come in conflitto con il resto delle operazioni di un'organizzazione. Questa relazione contraddittoria tra il personale di sicurezza e altre unità aziendali può comportare la violazione o la inosservanza dei criteri di sicurezza. Inoltre, la mancanza di comprensione dell'importanza della sicurezza e del suo valore per l'azienda può rendere difficile per il SOC acquisire i finanziamenti, le risorse e il personale di cui ha bisogno per svolgere il proprio lavoro.
  L'allineamento della strategia SOC con gli obiettivi aziendali, di fatto, aiuta il SOC ad essere percepito come una risorsa e una componente critica per il successo dell'organizzazione. Il SOC, eseguendo una valutazione del rischio, può identificare le risorse aziendali e valutare il potenziale rischio e gli impatti di un attacco informatico sui sistemi aziendali. Successivamente, il team può identificare metriche e KPI che dimostrano come il SOC supporta il resto dell'azienda e, infine, definire processi e procedure progettati per raggiungere tali obiettivi.

- **Identificazione dello stack di strumenti tecnologici** – Il personale SOC deve gestire un'ampia varietà di sistemi e potenziali minacce alla sicurezza. Ne consegue che spesso risulterebbe più facile disporre di tutti gli strumenti più recenti per massimizzare le capacità del SOC. Tuttavia, i nuovi strumenti possono mostrare rendimenti decrescenti, oltre a necessitare risorse per la installazione, la configurazione e monitoraggio, a discapito del personale addetto all'identificazione e alla gestione di altre minacce.
  Pertanto, lo stack di strumenti tecnologici di un SOC dovrebbe essere attentamente considerato in un'ottica di rapporto costo/beneficio. Ovvero, sarebbe auspicabile che i SOC utilizzassero piattaforme di sicurezza integrate ogni volta che è possibile, in modo da semplificare e ottimizzare il monitoraggio e la gestione della sicurezza.
- **Utilizzo della Threat Intelligence e del Machine Learning** – Il rilevamento e la risposta rapidi alle minacce sono essenziali per ridurre al minimo la probabilità e l'impatto di un incidente di sicurezza. Pertanto, la Threat Intelligence e il Machine Learning si convertono in leve strategiche per la capacità di un SOC di identificare e rispondere rapidamente alle minacce. In particolare, la Threat Intelligence alimenta gli algoritmi di Machine Learning che possono esaminare grandi volumi di dati di sicurezza e identificare le probabili minacce per l'organizzazione che, segnalate a un analista "umano", costituiscono la base per attuare ulteriori azioni o impostare azioni di correzione automatizzate.
- **Garantire la visibilità su tutta la rete –** Le reti aziendali moderne sono sempre più ampie, diversificate e in espansione. Pertanto, il personale SOC ha bisogno di visibilità end-to-end su tutta la rete per gestire i rischi ed intercettare ogni potenziale minaccia.
- **Formare il personale sulle best practice di sicurezza informatica –** Il personale è la prima linea di difesa contro gli attacchi informatici. Pertanto, è importante che sappia come identificare e rispondere a potenziali rischi/minacce, in modo da contribuire alla sicurezza proattiva e migliorare il livello di sicurezza generale dell'organizzazione.

U modello di SOC moderno

Si sta facendo strada una nuova tipologia di SOC moderno che implica da parte dei leader della sicurezza e della gestione dei rischi la capacità di fornire operazioni di sicurezza (*SecOps*) e funzioni SOC senza una posizione fisica e con metodi e processi non standard.
È doveroso evidenziare che non esiste un modello SOC giusto per operare o fornire funzioni SOC moderne. I SOC variano in base alla loro missione e ai loro obiettivi che sono influenzati da caratteristiche come: la tolleranza al rischio, il verticale in cui operano, il livello di maturità, le competenze, i processi e le procedure, gli strumenti utilizzati.
Di fatto, un modello SOC moderno come quello suggerito dal rapporto GARTNER – "*How to Build and Operate a Modern Security Operations Center*" è in grado di fornire ad un'organizzazione le funzionalità di rilevamento e di risposta alle minacce in base alle priorità aziendali, in un contesto in continua evoluzione.



Pertanto, un SOC moderno dovrà essere in grado di offrire sia la flessibilità necessaria sia l'agilità e adattabilità per consentire all'organizzazione di cambiare secondo le proprie necessità.

Inoltre, secondo un recente studio di ESG, a fronte del rapido progresso delle tecnologie di sicurezza, le organizzazioni hanno difficoltà ad acquisire, implementare e formare team interni per utilizzarle.

Secondo Gartner, entro il 2025, il 90% dei SOC esistenti utilizzerà un modello ibrido esternalizzando almeno il 50% del carico di lavoro operativo; inoltre, si prevede che il 33% delle organizzazioni- che attualmente hanno funzioni di sicurezza interna - non sarà in grado di costruire un SOC interno efficace a causa di vincoli di risorse, come la mancanza di budget, competenze e personale.

SOC & Cloud: cosa ci attende nel 2023

Molti esperti del settore ritengono che, nel 2023, i SOC dovranno confrontarsi anche con l'implementazione sempre più diffusa del cloud (i.e. cloud pubblici, multicloud, cloud SaaS). Pertanto, le organizzazioni dovranno comprendere come effettivamente gestire il cloud computing in modo da garantire:

- **Un'ottimale progettazione in termini di sicurezza fisica del SOC e layout della centrale** – La sicurezza fisica deve essere presa in considerazione e il layout della centrale operativa dovrebbe essere attentamente progettato per essere sia confortevole che funzionale. Un SOC dovrebbe contenere diverse aree, tra cui una sala operativa, una "war room" e gli uffici dei supervisori. Comfort, visibilità, efficienza e controllo sono termini chiave in questo scenario e ogni singola area deve essere progettata di conseguenza. Inoltre, un SOC richiede un team e tutte le politiche devono essere seguite correttamente. A tal proposito.
- **Un focus maggiore sulla ricerca del personale SOC** – Data la carenza di risorse umane e la mancanza di esperti qualificati, la maggior parte delle organizzazioni non è ancora in grado di implementare una sicurezza informatica efficace e ben strutturata. Di conseguenza, vi è una crescente necessità di combinare i prodotti di sicurezza in soluzioni multifunzionali in grado di affrontare una varietà di problemi di sicurezza correlati. Ne consegue che le organizzazioni dovranno cambiare il modo in cui stanno assumendo, ed essere in grado di utilizzare anche la pipeline universitaria. Tutto ciò implicherà dei cambi di paradigma, ovvero, per impiegare al meglio i giovani laureati saranno necessari investimenti in automazione, modifiche dei processi e redazione di procedure chiare.
- **Una maggiore comprensione e gestione della superfice d'attacco** – Sempre più organizzazioni esamineranno attentamente questo aspetto e integreranno maggiormente il SOC con il cloud computing. Tutto ciò poterà a una maggiore conoscenza di dati aziendali, di normali operazioni e di scenari di simulazione delle minacce in modo da intercettare tutto ciò che risulta "anomalo". Inoltre, comprendere dove risiedono i carichi di lavoro contribuirà notevolmente a rilevare le minacce.
- **Migliore gestione integrata dei rischi (Integrated Risk Management - IRM)** – Si tratta di implementare pratiche e processi supportati da una cultura consapevole del rischio e da tecnologie abilitanti che migliorano il processo decisionale e le prestazioni attraverso una visione integrata di come un'organizzazione gestisce il proprio insieme unico di rischi. Secondo quanto afferma ENISA, nei prossimi due-tre anni, sempre più organizzazioni incorporeranno sempre più il IRM nelle loro operazioni.
- **Perdurare del hybrid work** – L'hybrid work è destinato a persistere anche nel 2023. Ne consegue che le organizzazioni dovranno continuare a gestirlo nel miglior modo possibile per proteggere tutti i loro dipendenti, indipendentemente da dove si trovino. Pertanto, i team SOC saranno messi a dura prova e sarà sempre più fondamentale da parte dell'organizzazione la gestione del burnout del personale.

Conclusioni

La sicurezza informatica continuerà a essere una questione chiave per le imprese in futuro; pertanto, stabilire strategie di sicurezza scalabili aiuterà a adattarsi agli scenari futuri. In particolare, è doveroso ricordare che la costruzione e la gestione di un SOC è un percorso in divenire, dato che le esigenze dell'organizzazione si evolveranno inevitabilmente nel tempo. I cambiamenti in termini di direzione aziendale, di iniziative di trasformazione digitale, di fornitori di cloud, nonché del panorama delle minacce avranno un impatto diretto sulla missione del SOC e sul modo in cui viene realizzata. Ancora, si tratta di tenere il passo con il crescente panorama tecnologico e normativo secondo le esigenze aziendali, garantendo la realizzazione del valore da parte di tutte le parti interessate in base alla priorità e alla comprensione dei propri limiti, quali elementi fondamentali per selezionare il modello appropriato di SOC.

Concludendo, la conoscenza del contesto e l'acquisizione della consapevolezza dei propri obiettivi e delle proprie vulnerabilità permetterà di agire tempestivamente ed aiutare le organizzazioni a ridurre i propri rischi e a migliorare la propria resilienza ed il potenziale di crescita futura.

Intervista e contributo di Agostino Ghiglia, Componente del *Garante per la protezione dei dati personali*.

Nell'agosto 2022 è stato siglato un Protocollo di collaborazione fra l'Autorità Garante per la Protezione dei Dati Personali e il Clusit volto alla "*realizzazione di attività di interesse comune in relazione alla sicurezza informatica, con particolare riguardo al suo impatto sulla protezione dei dati personali. Tra le attività e i progetti di comune interesse per le Parti, da avviare prioritariamente, è compresa, in particolare, la possibilità per il Garante di veicolare, tramite il Rapporto Clusit o altro strumento dell'associazione, approfondimenti divulgativi anche redatti dal Clusit su temi di propria scelta.*"

Il Rapporto Clusit 2023 è la prima occasione per dare un seguito concreto al Protocollo, con una finestra dedicata al contributo dell'Autorità che quest'anno è stato redatto dal Dott. Agostino Ghiglia, Componente del Collegio, con cui commentiamo brevemente l'iniziativa.

Dott. Ghiglia, qual è l'obiettivo dell'Autorità nel siglare questa collaborazione con il Clusit?

L'Autorità, nello svolgimento della propria attività istituzionale, deve mantenere uno stretto collegamento con tutti gli attori sociali ed economici interessati al tema della tutela dei dati personali e, naturalmente, agli aspetti di sicurezza ad essa intimamente connessi. Il Clusit rappresenta in questo senso un interlocutore importante E il suo Rapporto uno strumento di comunicazione importante.

Il Rapporto e il Clusit stesso sono naturalmente solo uno dei canali di comunicazione attraverso cui il Garante mantiene un rapporto con la società e il mondo economico. Quale ritiene debbano essere le loro peculiarità?

Direi sostanzialmente due: da un lato vi è l'obiettivo di approfondire alcuni fenomeni rilevanti per la sicurezza nel mondo delle imprese, attraverso indagini e rapporti i cui obiettivi possono essere definiti congiuntamente e che possono contribuire alla conoscenza approfondita del contesto e delle tendenze in essere. È di tutta evidenza l'utilità reciproca di una simile collaborazione e del confronto pubblico su questi temi che ne può derivare.

Dall'altro vi è la possibilità, per l'Autorità, di sfruttare soprattutto il Rapporto Clusit per porre all'attenzione della comunità professionale della cybersecurity alcuni temi emergenti, visti dalla prospettiva dell'impatto sulla tutela dei dati personali e dell'identità. È il caso, ad esempio, del contributo di quest'anno, centrato sul tema degli Ultraversi.
Anche questo aspetto della collaborazione rappresenta un'opportunità importante: la tecnologia evolve a grande velocità e praticamente ogni innovazione ha un impatto diretto

e indiretto sui dati personali, sulle nostre identità digitali e, sempre più, anche fisiche e sulla sicurezza. La possibilità di segnalare, approfondire e pure discutere criticamente le innovazioni, anche in un momento assolutamente iniziale del loro affermarsi è un'opportunità indubbiamente rilevante per chi poi si troverà a dover svolgere in merito un compito di tutela assai complesso.

Come si vede i temi non mancano: l'auspicio è di riuscire a tradurre in iniziative concrete una intuizione che risponde ad una esigenza sia dell'Istituzione sia del mondo delle imprese e dei professionisti della sicurezza. Questo spazio dedicato dal rapporto è una prima risposta a cui occorrerà dare seguito e continuità.

METAVERSO E CYBERSECURITY

Metaverso e i suoi 141 concorrenti rappresentano, ad oggi, un'idea, una suggestione; un concetto che descrive universi virtuali in cui gli utenti dovrebbero poter interagire (potranno?) in modo immersivo. Si tratta dunque di ambienti che imitano o simulano il mondo reale o altri mondi immaginari in modo da offrire un'esperienza avvolgente e coinvolgente per gli utenti. Tale immersione si ottiene attraverso l'utilizzo di tecnologie di realtà virtuale o aumentata, che creano un ambiente virtuale apparentemente reale (o realistico) in cui gli utenti potranno, nelle previsioni degli sviluppatori, interagire in modo naturale. Gli utenti potranno infatti muoversi, esplorare, comunicare e rapportarsi con oggetti e altri utenti in modo simile a come lo farebbero nel mondo reale. Ecco perché gli Ultraversi (per comprendere non un solo marchio ma tutte le iniziative imprenditoriali ad oggi presenti sul mercato) vengono già considerati, a mio avviso con un ottimismo inversamente proporzionale alle attuali potenzialità, come un'estensione del mondo reale o come un mondo parallelo completamente autonomo.
Senza scomodare gli Ultraversi, l'ambiente virtuale immersivo viene utilizzato da anni in molti campi, primo fra tutti quello dei giochi ma anche per la formazione, la visualizzazione di progetti, le simulazioni di interventi chirurgici. Gli Ultraversi, quindi, possono considerarsi davvero come una delle tecnologie più innovative e promettenti del 21° secolo-che potrebbe offrire nuove opportunità per le industrie e i consumatori -o ci troviamo di fronte ad una propaganda massiva della realtà virtuale ed aumentata? Gli Ultraversi, ad esempio, possono essere utilizzati per creare nuove esperienze di intrattenimento, come giochi o spettacoli virtuali, o per creare nuove opportunità commerciali, come la vendita di prodotti e servizi digitali…Ma tutto ciò esiste già da anni.
Alcuni considerano gli Ultraversi addirittura come un'opportunità per esplorare nuove forme di identità e di esperienza umana, per scandagliare la propria personalità e per creare nuove relazioni sociali. Senza dubbio, di fronte a queste presunte potenzialità l'avvento degli Ultraversi - se si realizzerà - porterà con sé opportunità ma anche nuovi rischi per la sicu-

rezza informatica, per la protezione e la sicurezza dei dati personali. Lo stesso Mark Zuckerberg lo ha previsto all'atto dell'annuncio del suo nuovo progetto META "nello sviluppo del Metaverso bisognerà costruire sicurezza e privacy". Se è vero quello che vaticinano alcune previsioni -a mio avviso, lo ripeto, allo stato dell'arte più infondate che ottimistiche-secondo le quali entro il 2026 il 25% delle persone trascorrerà almeno un'ora al giorno nel Metaverso, per lavoro, shopping, istruzione, è importante lavorare, sin da ora, per affrontare le due sfide più grandi: sicurezza e privacy; ma ciò vale ancor di più e molto più realisticamente per lo sviluppo ipersonico dell'Intelligenza Artificiale: basti pensare alla recentissima esplosione commerciale dei chatbot di ultima generazione.

Per aumentare le misure di protezione dei dati personali, le Tech Industries degli Ultraversi dovranno irrobustire le loro difese. Per evitare vulnerabilità, sarà necessario limitare i privilegi di accesso con verifiche regolari, proteggere gli account usando password manager e utilizzare autenticazione a due fattori (2FA), formare adeguatamente il personale. Un altro aspetto critico, inoltre, sarà quello relativo alla protezione dei beni virtuali, come la valuta, gli NFT, la proprietà dell'identità virtuale. Sappiamo, infatti, che gli Ultraversi sono spesso costruiti su tecnologie decentralizzate, come la blockchain, che presentano sfide uniche in termini di sicurezza, trattiamo di ambienti virtuali in cui gli utenti possono condividere informazioni personali e dati sensibili, rendendoli pertanto vulnerabili alla violazione della privacy e alla sicurezza dei dati poiché, come in qualsiasi ambiente digitale, anche gli Ultraversi potranno essere esposti alle cyberminacce, come il phishing, il malware o il furto di identità, solo per citare le più frequenti.

È verosimile, qualora gli Ultraversi si sviluppassero, che le risorse virtuali - aventi comunque una base reale, si tratti di cryptovalute o di moneta corrente sottesa alle transazioni - diventeranno un bersaglio primario per il cybercrime. Gli hacker potrebbero, ad esempio, sfruttare i visori o le cuffie per la realtà virtuale - che sono dispositivi Internet of Things (IoT) e che possono trasmettere dati all'esterno quando non all'estero- per compromettere la sicurezza, sfruttare le informazioni pubbliche reperibili online per impersonare terze parti e ottenere informazioni personali da parte degli utenti, traendoli in inganno. Si potrebbero verificare, inoltre, nuovi rischi legati alla sicurezza online, come il furto di identità. Gli utenti potranno incorrere nel furto del loro avatar e il cybercriminale potrebbe essere riconosciuto come il suo vero proprietario e, in quanto tale, libero di compiere ogni tipo di azione. La verifica dell'identità sarà senz'altro una sfida per tutte le parti coinvolte, poiché non sarà facile (ma sarà essenziale) assicurarsi che un soggetto virtuale sia veramente chi afferma di essere (nella Realtà fisica). Ancora, potrebbero verificarsi frodi nei pagamenti. Abbiamo poc'anzi detto che gli Ultraversi sono collegati al mondo delle criptovalute e degli NFT, questo li potrà rendere preda di hacker pronti a impossessarsi dei wallet e delle chiavi di accesso dei cittadini dei medesimi mondi virtuali.

Per lo sviluppo degli Ultraversi, quindi, gli esperti di sicurezza informatica sono sfidati a prevenire questi ed altri rischi e a garantire la protezione dell'identità digitale, che comprende non solo l'identità online, ma anche quella offline. Affinché ciò sia possibile sarà indispensabile progettare a monte Ultraversi che implementino robuste linee di security by

design (oltre che di privacy by design) volte appunto a garantire adeguate tutele e garanzie agli utenti. Le aziende e le organizzazioni che costruiscono e gestiscono gli Ultraversi dovranno adottare una solida strategia per gestire questi rischi e garantire un'esperienza sicura e positiva agli utenti. Al contempo, gli esperti della cybersecurity, dovranno analizzare tutti i rischi potenziali per la sicurezza informatica negli Ultraversi oltre che, con un monitoraggio costante, identificare le minacce più probabili, così come avviene nella Realtà fisica. È ovvio, peraltro, che essendo le tecnologie di cui scriviamo ancora pionieristiche, è impossibile prevedere tutti i rischi tecnologici e le falle di cui questi sistemi possono soffrire: non disponiamo di una Meta (Ultra)Sibilla Cumana…

Sono convinto, infine, che, se prendiamo per buono lo sviluppo e le potenzialità degli Ultraversi - ancorché attualmente più "virtuali" che attuali - occorra iniziare a pensare ad una regolamentazione globale onde scongiurare il rischio che ogni Nazione legiferi per conto proprio sulla creazione e l'utilizzo di ambienti virtuali immersivi. A tale ipotesi, ovviamente, conseguirebbe una scarsa tutela per gli utenti e una difficilissima gestione dei contenuti, con particolare riguardo per quelli inappropriati o pericolosi. È importante, dunque, che le Istituzioni, le autorità nazionali per la lotta contro le cyberminacce e la protezione della privacy degli utenti, le organizzazioni che costruiscono e gestiscono gli Ultraversi, cooperino e collaborino per creare un quadro regolamentare adeguato al fine di garantire un'esperienza sicura e positiva agli utenti che la riterranno utile.

Agostino Ghiglia
Componente del Garante per la protezione dei dati personali

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.
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.
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).
Fake news	Notizie destituite di fondamento relative a fatti od argomenti di pubblico interesse, elaborate al solo fine di condizionare l'opinione pubblica, orientandone tendenziosamente il pensiero e le scelte.
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.
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.
Keylogger	Malware (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
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.

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.
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.
PSYOPs (Psychological Operations)	"Operazioni psicologiche" consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti. *(Tratto da: Glossario intelligence – Il linguaggio degli Organismi informativi - www.sicurezzanazionale.gov.it)*
Pulse Wave (o Hit & Run)	Hit & Run (o Pulse wave)
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.
Sandboxing	Ambiente protetto nel quale è possibile testare applicazioni senza compromettere l'intero sistema informatico.
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.
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 engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
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.

SSDP (Simple Service Discovery Protocol)	Protocollo che consente di scoprire e rendere disponibili automaticamente i dispositivi di una rete.
SSH (Secure Shell)	Protocollo cifrato che consente l'interazione remota con apparati di rete o di server permettendone, ad esempio, l'amministrazione.
STIX (Structured Threat Information eXpression)	Linguaggio strutturato che consente la descrizione e condivisione automatizzata di cyber threat intelligence (CTI) fra organizzazioni, utilizzando il protocollo TAXII.
Tampering	An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.
TARA (Threat Analysis Risk Assessment)	Metodologia utile per dettagliare tutti i possibili threat a cui un prodotto può essere soggetto e assegnare un rischio basandosi su parametri, sempre descritti nello standard ISO/SAE 21434, che coprono l'ambito della safety, della privacy dell'utente, dell'impatto economico e dell'impatto sull'operatività del prodotto e del veicolo.
TAXII (Trusted Automated eXchange of Indicator Information)	Protocollo che consente lo scambio (in HTTPS) di CTI (cyber threat intelligence) descritti mediante STIX.
TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
TDM (Time-division multiplexing)	Tecnica che consente la condivisione, da parte di più dispositivi, di un canale di comunicazione per un tempo limitato predefinito.

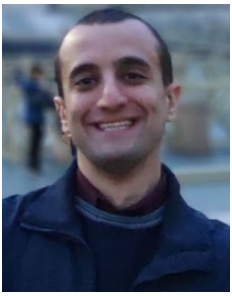
Tecniche di amplificazione degli attacchi	Sfruttando lo spoofing dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del protocollo NTP si può amplificare la potenza dell'attacco anche di 600 volte.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
TLP (Traffic Light Protocol)	Protocollo per facilitare la condivisione delle informazioni "sensibili" che definisce il grado di possibile diffusione (red, amber, green, white) stabilito dalla controparte inviante.
TLS (Transport Layer Security)	Protocollo per la comunicazione sicura su reti TCP/IP successivo al SSL (Secure Sockets Layer).
Tradecraft	Combinazione di metodi, capacità e risorse che un attaccante sfrutta nel compimento delle proprie azioni.
TSP (Trust Service provider)	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato.
UBA (User Behavior Analytics)	Tecnologia atta ad apprendere il "normale" comportamento degli utenti di un sistema informativo mediante l'analisi di rilevanti quantità di dati (log…), e di segnalare successivamente il verificarsi di attività anomale messe in atto dagli stessi.
UDP Flood	Il protocollo UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	Protocollo di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.
VNC (Virtual Network Computing)	Strumento di condivisione del desktop da remoto.

Vetting	Il processo di identificazione dei partecipanti ad una ***blockchain***.
VHUMINT (Virtual Human Intelligence)	Estensione al mondo virtuale del concetto di Human Intelligence, cioè di una metodologia investigativa imperniata sulla raccolta di informazioni per mezzo di contatti interpersonali. Attraverso la VHUMINT vi è dunque l'interazione proattiva con gli attori della minaccia al fine di raccogliere informazioni di contesto necessarie a mitigare efficacemente la minaccia.
Vishing	Variante "vocale" del ***phishing***.
Volume Boot Record	Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Weaponization	Modifica di file e documenti per trasformali in vere e proprie armi per colpire i sistemi e gli utenti e per favorire l'installazione di codice malevolo.
Web Injects	Tecnica che consente di mostrare nel browser dell'utente informazioni diverse rispetto a quelle originariamente presenti sul sito consultato.
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 2023

Luca Bechelli, Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed 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.



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. Dal 2020 è Cyber Security Professional all'interno del gruppo CSIRT di Fastweb, dove si occupa attivamente di Incident Response, Cyber Threat Intelligence e Threat Hunting.

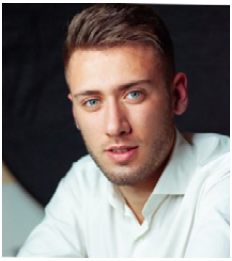
Laura Bongiorno, Laureata in Fisica, è entrata in Fastweb nel 2000. Lavora nella funzione Security & Real Estate dal 2018, dove ha assunto prima la responsabilità della funzione Security by Design, poi anche la responsabilità della funzione Fraud Management. Da ottobre 2021 ha la reponsabilità di Incident 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.

Laura Buscarini è Direttore di CNA Milano. CNA (Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa) Milano, rappresenta gli interessi della piccola impresa per porla al centro delle politiche locali, nazionali e comunitarie. CNA Milano è a disposizione di aziende artigiane, micro, piccole e medie imprese, lavoratori autonomi, imprese commerciali, valorizzando la cultura del lavoro ed offrendo alle imprese associate, anche consulenze, servizi e formazione che contribuiscono al loro sviluppo.

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).



Nicola Ciani si è laureato in Economia e Management all'Università di Bologna nel 2020. Dal 2021 collabora come Ricercatore nella School of Management del Politecnico di Milano, all'interno degli Osservatori Cybersecurity & Data Protection e Big Data & Business Analytics.

Mauro Cicognini, parte del team che ha fondato Rexilience nel 2021, si occupa di ICT dal 1989 e di cybersecurity dal 1996. Ha lavorato in aziende dei servizi e dell'alta tecnologia (software, systems integration, telecomunicazioni, automazione industriale), progettando e gestendo software, servizi e reti ICT in realtà che spaziano dalla multinazionale alla PMI. Le sue aree di responsabilità hanno toccato Europa, Africa, Sud America e Medio Oriente; parla inglese, italiano, spagnolo e francese. Interviene sui media nazionali e di settore, ed ha tenuto sessioni su IoT, sul GDPR, sulla Business Continuity, sulla sicurezza fisica, e così via. La sua attività convegnistica è rivolta sia agli specialisti di settore sia, a livello divulgativo, alle scuole ed alle iniziative civiche. Dal 2019 è docente presso il Cefriel – Politecnico di Milano nell'ambito del Corso di Alta Formazione per DPO. Ha fatto parte del Comitato Direttivo e poi del Comitato Scientifico di Clusit ininterrottamente dal 2006. Si è laureato nel 1995 al Politecnico di Milano in ingegneria elettronica (indirizzo bioingegneria), ed ha conseguito nel 2009 un "Executive Certificate in Management and Leadership" presso il Massachussetts Institute of Technology.

Raffaella D'Alessandro. Security Strategy Senior Manager in Consulthink S.p.A. Cura lo sviluppo e l'innovazione dei servizi di Cyber Security. Esperienza trentennale nello sviluppo e implementazione di Sistemi di Gestione della Sicurezza delle Informazioni, Information Security Governance, Risk Management, Conformità Normativa, Business Continuity, Cybersecurity Framework. Già Information Security Consultant e Privacy Trusted Advisor in primarie aziende multinazionali per le quali ha realizzato progetti complessi di Information Security e Compliance Normativa per clienti della Pubblica Amministrazione, Banking, Telco, Trasporti. È membro del Consiglio Direttivo di AIIC (Associazione Italiana esperti in Infrastrutture Critiche), dove ha ricoperto anche gli incarichi di Vicepresidente e Segretario Generale. È stata membro del comitato direttivo del CLUSIT (2000-2006). Speaker ufficiale del World Protection Forum, docente nei Master di Information Security di SDA Bocconi.

Tamara Devalle è Consulente in ambito tecnologico, con esperienza incentrata su innovazione, trasformazione digitale ed automazione dei processi, IT Governance, modelli operativi IT, risk management, audit & compliance.

Pasquale Digregorio è un ex-Ufficiale d'Accademia, attualmente Capo Divisione del Computer Emergency Response Team della Banca d'Italia, dove mette al servizio dell'Istituto la sua esperienza in cyber intelligence e cybersecurity, sviluppata in 20 anni di servizio, svolti presso il Ministero della Difesa e la Presidenza del Consiglio. Dopo la laurea magistrale in ingegneria delle telecomunicazioni presso il Politecnico di Torino ha conseguito un master di secondo livello in Sistemi avanzati di comunicazione e localizzazione satellitare presso l'Università Tor Vergata ed uno in Protezione Strategica del Sistema Paese presso la SIOI. Nel corso della sua carriera ha fatto parte di commissioni e organismi permanenti in seno alla NATO; svolge attività formative e di docenza presso enti universitari e Istituzioni. È autore di diverse pubblicazioni e inventore di un brevetto internazionale.

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.

Elenio Dursi, IT project manager, si occupa da oltre 20 anni di pianificazione, gestione, manutenzione ed implementazione di tutto ciò che riguarda la parte progettuale dei sistemi informativi di una azienda seguendo le innovazioni tecnologiche che man mano vengono proposte dal mercato con uno sguardo attento alla parte normativa su ciò che prevede la legge in materia di data breach e sicurezza dei dati personali. È membro del comitato scientifico Clusit

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.

Chiara Ferretti ha conseguito nel 2006 la Laurea Magistrale con lode in Ingegneria delle Telecomunicazioni presso l'Università La Sapienza di Roma. Si è occupata per oltre 15 anni di sicurezza delle informazioni e gestione di progetti IT per aziende operanti nei settori finanziario, delle telecomunicazioni, alimentare, dei trasporti e logistico, specializzandosi nell'esecuzione di *risk assessment*, *maturity assessment* e *gap analysis* per sistemi afferenti sia all'ambito IT che OT, e nello sviluppo di metodologie di analisi del rischio basate su standard e *best practices* internazionali, quali ISO 27001, NIST CSF, ISA62443, ISF IRAM 2. Ha conseguito diverse certificazioni di sicurezza, come ad esempio CISSP, CFE e GCTI. Dal 2022 lavora presso il Computer Emergency Response Team della Banca d'Italia.

Daniele Filoscia è un ex-Ufficiale d'Accademia, specializzato in *cyber threat intelligence*. Ha prestato servizio presso l'Aeronautica Militare per 15 anni durante i quali ha maturato, anche in ambito internazionale e NATO, diversificate esperienze in numerosi ambiti quali INFOSEC, *risk management & compliance*, *security awareness*, *vulnerability assessment & penetration testing*, *incident management, blue e red teaming,* progettazione, realizzazione e certificazione di infrastrutture CIS. Dopo la Laurea in Ingegneria Elettronica presso l'Università Federico II di Napoli, ha conseguito un Master Universitario di secondo livello in Homeland Security & Crisis Management. Ha conseguito diverse certificazioni in ambito cyber e attualmente sta svolgendo un Dottorato in cyber security presso l'Università La Sapienza di Roma. Dal 2021 lavora presso il Computer Emergency Response Team della Banca d'Italia in qualità di Cyber Security Analyst.

Sergio Fumagalli, ESG Senior advisor, collabora con la testata ESG360. È Senior partner di P4I e responsabile della consulenza e dei servizi in ambito ESG e sostenibilità. Ha sviluppato una ventennale esperienza nella tutela dei dati sia sotto il profilo della cybersecurity sia per la protezione dei dati personali. È membro del Comitato scientifico del Clusit.

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 è il Responsabile del Centro nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC). Dal luglio 2017 è il 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 e dal gennaio 2022 è Direttore Supplente del Servizio Polizia Postale e delle Comunicazioni.

Francesca Gatti, CISA e CIGIT Francesca collabora con Clusit dal 2017, ha partecipato come coautore, editor e team leader a 11 pubblicazioni della Clusit Community for Security ed è membro della Community Women for Security. Negli anni 80 ha fondato e guidato una Software House in Milano e successivamente ha ricoperto ruoli di Governance, Qualità, e Sicurezza dei Sistemi Informativi presso multinazionali, occupandosi negli ultimi anni di ISO27001, Sarben Oxly e GRC. Dal 2012 è Partner di Roadrunnerfoot Engineering, azienda del settore medicale per la quale ha sviluppato il Sistema di GRC ottenendo le certificazioni ISO9001 e ISO13485. È socia onoraria di AUSED di cui ha coordinato l'Osservatorio di Sicurezza e Compliance dal 2000 e ricoperto la carica di Segretario Generale e Tesoriere dal 2016 al 2022 e di GUPS - Gruppo Utenti e Prospect SAP, nata nel 2017 e di cui è stata Segretario Generale e Tesoriere fino al 2022.

Agostino Ghiglia è Componente del Garante per la protezione dei dati personali. Laurea Magistrale in Giurisprudenza. Da giugno 2020 a luglio 2020 - Presidente Consorzio 5T. Da luglio 2014 a luglio 2020 Amministratore delegato di Nextrain Srl (Formazione professionale). Da giugno 2017 a luglio 2020 - Amministratore delegato e fondatore di "Mutua con te". Dal 2009 a luglio 2020 - Consigliere di Amministrazione di Neos-tech srl (strumenti e servizi per la gestione della sosta e dei parcheggi in oltre 100 città, tra cui Napoli, Torino, Palermo). Dal 2009 al 2014 - Amministratore unico di Coopservice (Servizi informatici e telematici per le imprese). Da marzo 2013 a giugno 2014 - Assessore regionale (energia, innovazione, sviluppo, ricerca,

internazionalizzazione, commercio, artigianato, società partecipate) – Regione Piemonte. Dal 2008 al 2013 - Deputato - Camera dei Deputati (Capogruppo in Commissione VIII e Componente in Commissione Bicamerale di Controllo sulla gestione del ciclo dei rifiuti). Dal 2005 al 2008 - Consigliere Regionale - Regione Piemonte. Dal 2001 al 2005 - Deputato – Camera dei Deputati (Capogruppo in Commissione VIII). Dal 1995 al 2001 - Consigliere Regionale - Regione Piemonte. Dal 1994 al 2011 - Consigliere Comunale – Comune di Torino (Commissioni Attività produttive, Energia, Cultura, Commercio e Bilancio). Dal 1994 al 1997 - Vice presidente CIT – Consorzio intercomunale torinese. Dal 1985 al 1990 - Consigliere di amministrazione USL 1/23 Torino.

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 ed assessment, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Ha collaborato per oltre venti anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo. Ha partecipato a progetti internazionali di contrasto alla cybercriminalità e al cyberterrorismo con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) e l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL). È docente in numerosi Master Universitari. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri. L'Università di Roma Tor Vergata gli

ha conferito la laurea magistrale honoris causa in Ingegneria di Internet e delle Tecnologie per l'Informazione e la Comunicazione.

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.

Sebastiano Paolo Lampignano. Innovation & People Management Director in Consulthink S.p.A. Senior Enterprise Architect, TOGAF Certified, Archimate Expert, PMI-PMP© Certified, Scrum Master Certified. Senior Program Manager per la progettazione e realizzazione sistemi e servizi indirizzati all'Enterprise Risk Assessment and Security Management, Compliance Regulation EU 2016/679 (GDPR), Enterprise Portal Management, Professional Learning Management (progetti di formazione professionale). Già Senior Manager in Olivetti, E&Y, Deloitte and Touch Business Solutions e Microsoft. Docente di Master Universitari presso l'Università Aldo Moro di Bari. Docente di corsi professionali in Project Management. Autore di: *Infomobility. Sistemi informativi, sistemi di trasporto, processi e tecnologie* (Ed. Franco Angeli), *Digital Reputation Management – Semiotica, Management, Tecnologie* (ed. Apogeo).

Michele Lestingi, Enterprise Security Engineer presso il Security Operations Center di Fastweb, si occupa di consulenza in ambito sicurezza per i clienti Enterprise. Nella sua esperienza di oltre 10 anni nel settore ICT e Cyber Security, ha lavorato su progetti per le Forze dell'Ordine e in diversi Security Operation Centers in attività di ricerca, advisory e cyber defence. Possiede la certificazione CISSP ed è laureato in Informatica e Comunicazione Digitale presso l'Università degli studi di Bari. Collabora per il progetto di Sicurezza Digitale per la pubblica amministrazione del Team per la Trasformazione Digitale.

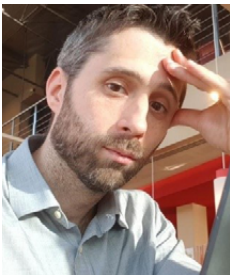
Federica Maria Rita Livelli, Consulente di *Business Continuity & Risk Management*, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università oltre ad essere Tutor di corsi di *Business Continuity* propedeutici al conseguimento della certificazione CBCP presso il DRI Italy. *Board Member* del BCI *Italy Chapter*, del CLUSIT *Scientific Committe* e di diverse Commissioni tecniche CLUSIT ed UNI. È Socia AIPSA ed (ISC)2 *Italy Chapter*. Docente di moduli ISO 22301, ISO 31000, ISO 27001 e *Crisis Management* presso diverse università (SUPSI Lugano, POLIMI–BOCCONI, Verona, Cagliari, Padova, Statale di Milano, Università Genova e LIUC Castellanza). Relatrice e moderatrice in seminari, conferenze nazionali ed internazionali. Autrice di articoli su numerose riviste online italiane ed internazionali. Ha partecipato, in qualità di co-autrice, a: Edizioni 2020, 2021 e 2022 del Rapporto Clusit - Cyber Security; Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021); Libro "Lo Stato in Crisi" ed. Angeli.

Luca Nilo Livrieri è l'SE Manager 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 Israel. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, sicurezza, cloud e digital transformation fra cui Security Summit, ISMS forum, IDC 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.

Salvatore Marcis, classe 1985, vanta una esperienza di quasi 20 anni nel mondo IT. Grazie alle sue doti tecniche e commerciali, ha assunto ruoli di rilievo in importanti realtà IT e di security, gestendo progetti complessi per clienti strategici di fascia enterprise. Entrato in Trend Micro nella primavera del 2017 come Senior Pre-Sales Engineer, ha assunto poco dopo la carica di Technical Director, diventando responsabile di tutte le attività di pre-vendita e di supporto in Italia, contribuendo all'importante crescita della country italiana. Nel 2023 assume la carica di Head of Channel

and Territory Sales con il compito di sviluppare e consolidare i rapporti con l'ecosistema di distributori e partner tecnologici, e di generare nuove opportunità di business per raggiungere in maniera ancora più capillare e proficua i clienti sul territorio nazionale.

Carlo Mauceli è National Digital Officer e National Security Officer della filiale italiana, con la responsabilità di promuovere l'innovazione del Paese, gestendo i rapporti con le government élites, i leader accademici e i decisori pubblici e contribuendo alla definizione di una politica tecnologica funzionale alla digitalizzazione del territorio. In qualità di National Security Officer, Carlo collabora con l'ACN, promuove la cultura della sicurezza e gestisce le crisi legate agli attacchi informatici. È membro del consiglio direttivo di Clusit.



Luca Memini appassionato di informatica dalla tenera età grazie al Commodore 64, oggi ricopre il ruolo di Cyber Security Professional presso il gruppo CSIRT di Fastweb. Specializzato nella gestione degli incidenti e delle minacce cyber afferenti al mondo APT. Si occupa inoltre dello sviluppo di nuovi strumenti per migliorare le capacità di rilevamento e di risposta alle minacce da parte dell'azienda.

Sonia Montegiove è informatica e giornalista; coordinatrice del progetto Cybertrials del Cybersecurity National Lab del CINI, programma **gratuito di gaming e formazione per le ragazze delle scuole superiori**. Ha fatto parte del gruppo di esperti nominati dal Ministero dell'Innovazione per individuare misure di contrasto all'hate speech. Fa parte del Comitato Direttivo di Women for Security dal 2021. Ha pubblicato: "Valentina nello spazio", favola rivolta a bambini e bambine per avvicinarli alle STEAM, "#gnomeide salvate le mamme e i papà" e "#gnomeide2 manuale di sopravvivenza ai social network", il cui intento è quello di guidare i genitori nella corretta costruzione di percorsi di consapevolezza digitale da intraprendere insieme ai ragazzi e alle ragazze. Ha condotto insieme a Chiara Lalli l'inchiesta giornalistica "Mai dati, dati aperti (sulla 194) perché sono nostri e perché ci servono per scegliere", diventata libro per Fandango editore.

Andrea Pasquinucci (PhD CISA CISSP) è Consulente freelance in sicurezza informatica: si occupa prevalentemente di consulenza al top management in Cyber Security e di progetti, governance, risk management, compliance, audit e formazione in sicurezza IT.

Michael Paye In qualità di VP Research and Development di Netwrix, è responsabile dei team di sviluppo e controllo qualità dell'organizzazione. È impegnato nello sviluppo dell'intero portafoglio per garantire che tutti i prodotti soddisfino processi e policy rigorosi, nonché nel supportare i diversi team dislocati in tutto il mondo mentre progettano nuove soluzioni. Mike ha un background nello sviluppo software di più di dieci anni di esperienza in diversi linguaggi e piattaforme.

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed 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.

Alessandro Pisani. Service Group Leader in Consulthink S.p.A. Dirige la Business Unit e-CyberDev (Cloud, DevOps & Enterprise Architecture). In particolare, negli ultimi tre anni, ha guidato la progettazione e realizzazione di progetti e programmi a supporto dell'Enterprise Architecture. Specialista dei framework TOGAF 10 e Archimate. Esperto nel disegno di metamodelli a supporto dei sistemi decisionali (DSS). È certificato PMP dal 2008, IFPUG CFPS dal 2010 e ITIL V4 dal 2022. È socio di ISIPM (Istituto di Studi Italiano di Project Management). Dal 1993 ha lavorato in grandi organizzazioni del settore privato (energy, telco & utilities) e pubblico (PA centrale, enti previdenziali) prima come sviluppatore software, poi analista progettista, IT Architect ed infine Project e Program Manager.

Alessandro Piva, laureato in Ingegneria delle Telecomunicazioni e in Ingegneria Gestionale al Politecnico di Milano nel 2006, ha conseguito in seguito un Executive Master in Business Administration (EMBA) presso il MIP Politecnico di Milano. Alla School of Management del Politecnico di Milano, dove lavora da circa 15 anni, è Direttore degli Osservatori Cybersecurity & Data Protection, Cloud Transformation, Artificial Intelligence e Responsabile della Ricerca dell'Osservatorio Big Data & Business Analytics.

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 ed 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.

Pier Luigi Rotondo è Technical Specialist per le soluzioni di Threat Management di IBM Italia. Ha contribuito a molti progetti internazionali su soluzioni per il Threat Management, l'Identity e l'Access Management, il Single Sign-on, e la Threat Intelligence. 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.

Rodolfo Saccani, CTO in Libraesva, vive l'IT dal 1994. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della security, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, siede nel board della European Hang-gliding and Paragliding Union, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero.

Luca Sambucci si occupa di sicurezza informatica dalla fine degli anni Ottanta, con l'analisi dei primi malware per PC e la redazione di numerosi articoli per le testate del tempo, come PC Professionale. Dopo la laurea in Management ha conseguito una specializzazione in Business Analytics a Wharton, una certificazione Artificial Intelligence Professional da IBM e una sul Machine Learning da Google Cloud. Già consigliere del Ministro delle Comunicazioni, ha al suo attivo collaborazioni con la Commissione Europea (European Defence Agency e Joint Research Centre) su temi relativi a cybersecurity e AI. Si occupa di ML/AI dal 2017, iniziando a lavorarci a tempo pieno dal 2020. Oggi lavora per un'azienda statunitense che sviluppa software di intelligenza artificiale.

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.

Leonardo Sartore si è diplomato in "Industrial Cyber Security" presso l'ITS Academy Meccatronico Veneto nel 2022. Durante il conseguimento del titolo di studio, ha ricoperto il ruolo di Information & Cyber Security Analyst come tirocinante in un'azienda del settore manifatturiero. Attualmente lavora per Partners4Innovation ricoprendo il ruolo di Information & Cyber Security Advisor.

Dirk Schrader è Resident CISO (EMEA) e VP of Security Research presso Netwrix. Un veterano con 25 anni di esperienza nella sicurezza IT con certificazioni CISSP (ISC²) e CISM (ISACA), è impegnato nel promuovere la resilienza informatica come approccio moderno per affrontare le minacce informatiche. In qualità di VP of Security Research, Dirk è costantemente impegnato nell'effettuare ricerche mirate per settori specifici come la Sanità, l'Energetico o il Finance. In qualità di Field CISO EMEA, "parla la lingua" dei clienti e dei potenziali clienti di Netwrix per facilitare la fornitura di soluzioni che meglio rispondano alle specifiche esigenze.

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 ad eventi e convegni di Cyber Security, sia in Italia che in UAE, e trainer in materia di Cyber Security Awareness.

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

Girolamo Tesoriere si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari.
10+ 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. Ha lavorato per Eni come Cyber Security Engineer e al momento occupa la posizione di Enterprise Security Architect in Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

Mario Testino, Ingegnere elettronico, dirigente d'azienda, COO (Chief Operating Officer) e consigliere di amministrazione in ServiTecno, e docente universitario a contratto, vanta una consolidata esperienza nella progettazione e la realizzazione di soluzioni per la digitalizzazione industriale e l'Industry 4.0, ed in particolare: SCADA e Plant Intelligence, Industrial IoT, Industrial Analytics ed OT/ICS Cyber Security.

Enzo Maria Tieghi, imprenditore, informatico, milanese, da oltre 30 anni si occupa di software per automazione e controllo di impianti, di security e compliance a standard e normative dei diversi settori industriali e delle infrastrutture in cui opera. Enzo è Amministratore Delegato di ServiTecno srl di Milano, Azienda che dal 1985 distribuisce e supporta software di GE Digital per sistemi OT industriale, SCADA, Industrial Internet, IIoT, Plant Intelligence, Analytics e tool per protezione di reti e sistemi nell'industria ed utility. Attivo in Associazioni di settore (quali AIIC, Clusit, CSA Cloud Security Alliance, ISPE, Anipla, ISA, AFI, Assintel, ecc.), tiene lezioni e partecipa come speaker ad eventi specialistici sia in Italia che all'estero, oltre a contribuire con articoli e memorie a riviste specializzate e conferenze internazionali. Autore del Quaderno Clusit "Introduzione alla protezione di reti e sistemi di controllo ed automazione (DCS, SCADA, PLC, ecc.)", ha curato per Fondazione Amga ed Edizioni Franco Angeli l'edizione italiana del volume "SCADA Good Security Practices per il settore delle acque potabili" (ed ha partecipato alla stesura del Rapporto Clusit 2012 sulla Sicurezza ICT in Italia e del ROSIv2. Attualmente in CLUSIT fa parte del Comitato Scientifico come referente della OT/IIoT Security, inoltre è socio AIIC, Senior Member di ISA, Senior Member ISPE ove partecipa al GdL CyberSecurity di ISPE/GAMP Italia.

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.

Alessandro Vallega, Fondatore e Senior partner in Rexilience.eu, società che si occupa di advisory in cybersecurity. In precedenza, in una società di consulenza (P4I) dove si è occupato di cybersecurity e governance risk and compliance e, prima ancora, in Oracle con il ruolo di Business Development Director su Security e Compliance (tra cui il GDPR) per l'Italia, l'Europa e infine per Europe Middle East and Africa. Si occupa di IT dal 1984 e di Information Security dal 2007. Alessandro è il fondatore e il chairman della Clusit Community for Security. È coautore, editor e team leader di quattordici pubblicazioni su diversi temi legati alla sicurezza e compliance della trasformazione digitale, tutti liberamente scaricabili dal sito Clusit.
Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. Il documento pubblico più importante su questi temi in Italia. È nel Consiglio Direttivo / Comitato Scientifico di Clusit dal 2010 ed è membro di ISACA Venice. Speaker in conferenze, corsi e master universitari. Insegna Analisi e Gestione del Rischio al corso Magistrale di Sicurezza Informatica all'Università Statale di Milano e ha una laurea in Scienza Politiche conseguita all'Università degli Studi di Milano.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. È membro del Comitato Scientifico del Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

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 600 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 18ª edizione.
- Le Conference specialistiche: i Security Summit Streaming Edition, i Security Summit On Site (a Milano, Verona e Roma), 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 e coordinata ogni anno nel mese di ottobre in Italia da Clusit.

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, Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
La **partecipazione è libera e gratuita**, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.
Certificata dalla folta schiera di relatori (più di 700 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 18.000 partecipanti, e sono stati rilasciati circa 14.000 attestati validi per l'attribuzione di oltre 46.000 crediti formativi (CPE).

SECURITY SUMMIT
ACADEMY

SECURITY SUMMIT
VERTICAL

L'edizione 2023

Per il 2023 è prevista una edizione tutta in presenza, dal 14 al 16 marzo, a Milano.
Nella seconda parte dell'anno si terrà il Security Summit di Verona, il 10 ottobre, e torneremo a Roma il 9 novembre. Continueranno gli Atelier della Security Summit Academy, che si terranno tutto l'anno, e gli Eventi Verticali, programmati il 25 maggio (Energy & Utilities), 15 giugno /Health Care) e 26 ottobre (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

HPE aruba networking

CROWDSTRIKE

FASTWEB

FORTINET

netwrix

SECURITY SUMMIT

www.securitysummit.it