2023

CYBERSECURITY REPORT

Cybersecurity is much more than a matter of IT

planetica

"Timeo Danaos et dona ferentes"

-Virgilio, Eneide Libro II, 49

1970S: ARPANET E IL CREEPER

La sicurezza informatica ebbe inizio negli anni Settanta, quando il ricercatore Bob Thomas creò un programma informatico chiamato Creeper in grado di muoversi attraverso la rete ARPANET, lasciando una scia di tracce ovunque andasse. Ray Tomlinson, l'inventore della posta elettronica, scrisse il programma Reaper, che inseguiva e cancellava Creeper. Reaper fu il primo esempio di software antivirus e il primo programma autoreplicante, il che lo rese il primo worm informatico in assoluto.

1980S: NASCITA DEGLI ANTIVIRUS COMMERCIALI

Il 1987 è stato l'anno di nascita degli antivirus commerciali, anche se ci sono state rivendicazioni contrastanti per l'innovatore del primo prodotto antivirus. Andreas Lüning e Kai Figge rilasciarono il loro primo prodotto antivirus per l'Atari ST, che vide anche il rilascio di Ultimate Virus Killer nel 1987. Nello stesso anno tre cecoslovacchi crearono la prima versione dell'antivirus NOD e negli Stati Uniti John McAfee fondò McAfee e rilasciò VirusScan.

1990S: IL MONDO VA ONLINE

Con la diffusione di Internet, un numero sempre maggiore di persone inizia a mettere online le proprie informazioni personali. Le entità del crimine organizzato videro in questo fenomeno una potenziale fonte di guadagno e iniziarono a rubare dati da persone e governi attraverso il web. A metà degli anni Novanta, le minacce alla sicurezza della rete sono aumentate in modo esponenziale e per proteggere il pubblico è stato necessario produrre in massa firewall e programmi antivirus.

2000S: LE MINACCE SI DIVERSIFICANO E SI MOLTIPLICANO

All'inizio degli anni 2000 le organizzazioni criminali hanno iniziato a finanziare pesantemente i cyberattacchi professionali e i governi hanno iniziato a dare un giro di vite alla criminalità dell'hacking, comminando pene molto più gravi ai colpevoli. La sicurezza informatica ha continuato a progredire con la crescita di Internet ma, purtroppo, anche dei virus.

OGGI

Il settore della sicurezza informatica continua a crescere alla velocità della luce.
La cybersecurity è un tema divenuto ormai di rilevanza strategica per tutti i Paesi: dalle dinamiche legate alla difesa e alla sicurezza, alla politica industriale e all'avanzamento tecnologico, fino alle implicazioni geopolitiche.

DOMANI: LA PROSSIMA GENERAZIONE

SOMMARIO

PREFAZIONE

Dopo più di un anno dall'inizio della guerra in Ucraina e della Cyber Warfare (guerra cibernetica) ad essa collegata, si rileva un aumento delle attività relative alle aggressioni ed incursioni informatiche ai danni degli alleati NATO: crescono gli attacchi verso i portali istituzionali, verso le infrastrutture e le aziende italiane.
In questo contesto, Planetica propone, anche quest'anno, la sua analisi di approfondimento relativa ai temi della sicurezza digitale avviata nel 2018 con l'obiettivo di indagare il livello di maturità della cybersecurity in Italia, "sorvegliando" i driver che ogni anno influenzano il contesto in modo diversificato.
Planetica si propone come il partner ideale per supportare aziende e professionisti offrendo un servizio di identificazione di eventuali vulnerabilità sul piano della sicurezza informatica, di valutazione della metodologia più adatta in ottica di rafforzamento del comparto IT e di supporto verso il raggiungimento di una corretta e coerente "Cyber Immunity" al fine di garantire elevati standard di protezione e sicurezza.
Prendere consapevolezza del panorama attuale e del contesto nel quale cresce l'attenzione verso la cybersecurity ci consente di unire le forze e le competenze con quelle del nostro Cliente per contrastare un potenziale futuro peggioramento della situazione.

Andrea Rivetti
Presidente & Partner

Matteo Marco Marzan
Amministratore Delegato & Partner

INTRODUZIONE

Nel 2023, il panorama della cybersecurity si evolve rapidamente e presenta una serie di sfide in continua crescita per governi, aziende e individui. La **crescente connessione** delle nostre infrastrutture digitali e la diffusione di tecnologie avanzate come l'intelligenza artificiale (AI) pongono nuove domande sulla sicurezza delle nostre reti e sistemi informativi. In questo contesto, la necessità di una maggiore consapevolezza e resilienza informatica diventa sempre più cruciale.

Il presente rapporto esplora la situazione della cybersecurity a livello globale e in Italia, mettendo in luce le **principali minacce**, i **trend emergenti** e gli **attori coinvolti** nella lotta alla sicurezza informatica. Analizziamo inoltre il ruolo delle forze di intelligence e della Difesa, esaminando le operazioni multidominio e il Cyber Warfare.

In particolare, ci concentriamo sui **rischi** associati all'intelligenza artificiale e all'evoluzione delle tecnologie AI, come la chatbot GPT di OpenAI, evidenziando le sfide e le opportunità che queste innovazioni pongono in termini di cybersecurity.

Infine, abbiamo avuto l'**opportunità** di **raccogliere** preziose **testimonianze** da **figure apicali** nel campo della **cybersecurity**. Abbiamo esplorato, attraverso interviste approfonite, tematiche rilevanti e complesse relative alla sicurezza informatica, al fine di trarre spunti utili per **migliorare le strategie** e **le soluzioni adottate**. Gli esperti intervistati hanno offerto una visione chiara e aggiornata delle sfide attuali e future, condividendo le loro competenze ed esperienze per contribuire a una maggiore consapevolezza e preparazione in un ambito in continua evoluzione.

3. VISIONE GLOBAL VS ITALIA

Come per il 2021, anche il 2022 conferma il trend crescente di attacchi informatici che oramai risulta essere una costante negli ultimi 5 anni. Infatti, confrontando i numeri del 2018 con quelli del 2022, si evidenzia come **la crescita del numero di attacchi gravi** di dominio pubblico sia stata del 60% (da 1.554 a 2.489 rispetto al 2018), con un aumento allarmante della media del numero di attacchi gravi mensili a livello globale che è passata dal 130 a 207. Va sottolineato che oltre che in quantità, gli attacchi sono cresciuti anche in gravità, arrivando a livelli di **impatto elevato o critico** nell'80% dei casi.

Trend annuale degli attacchi gravi a livello globale (2018 - 2022)

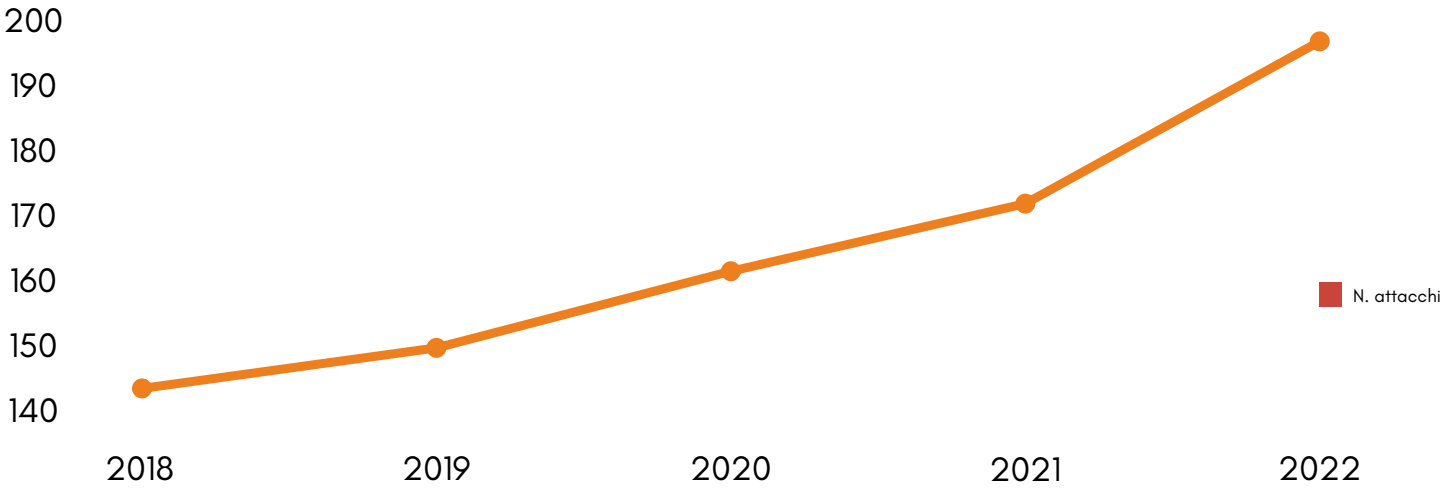


Figura 1 - Trend annuale degli attacchi gravi a livello globale (2018 - 2022) - Fonte: Rapporto Clusit 2023

Parte di questo peggioramento è facilmente riconducibile all'aumento di attività di Cyber Intelligence, di Cyber Warfare e di operazioni ibride derivanti da operazioni offensive utilizzate dai contendenti nel conflitto tra Russia e Ucraina. Come ulteriore elemento rafforzativo di questa tesi evidenziamo infatti che il picco massimo dell'anno e di sempre è stato registrato a marzo, quindi un mese dopo lo scoppio del conflitto, con un numero di 238 attacchi registrati globalmente.

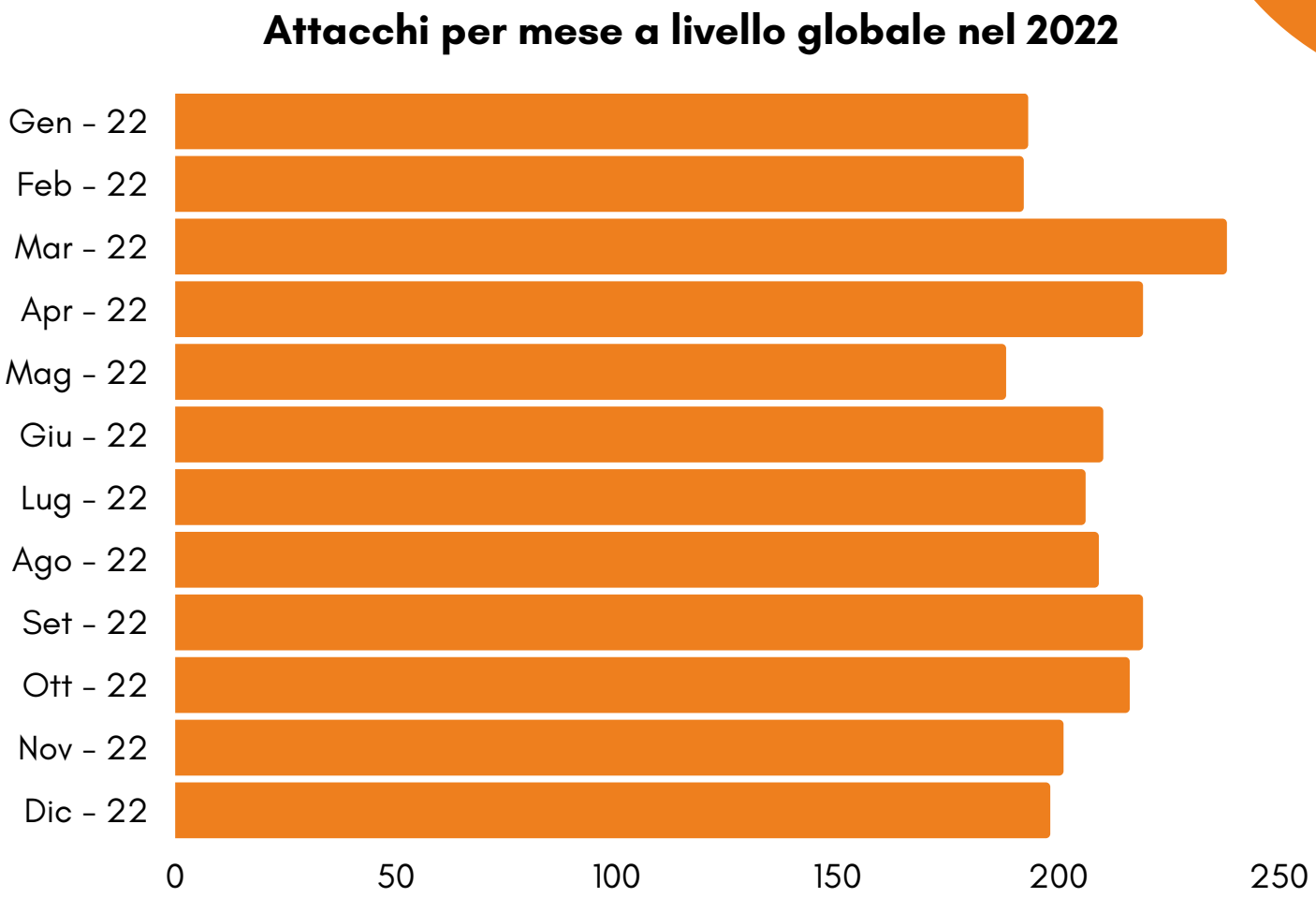


Figura 2 - Attacchi per mese a livello globale nel 2022 - Fonte: Rapporto Clusit 2023

Tuttavia, per quanto ancora prevalgano in **ambito intelligence** e **militare** attacchi effettuati tramite il cyberspazio, si evidenzia già un cambio di interesse di bersagli ed un **aumento di attacchi verso infrastrutture critiche o piattaforme digitali sensibili** e meno tutelate che risultano tuttavia essenziali per la collettività.

Infatti, su scala globale, è possibile notare come i Multiple Targets siano tornati ad essere le principali vittime (22%) con un aumento del 91% rispetto al 2021. Segue, come secondo settore più colpito, la sanità (12,2%) e il settore governativo e delle pubbliche amministrazioni (12%) che nell'arco di cinque anni ha visto un incremento complessivo del 36%.

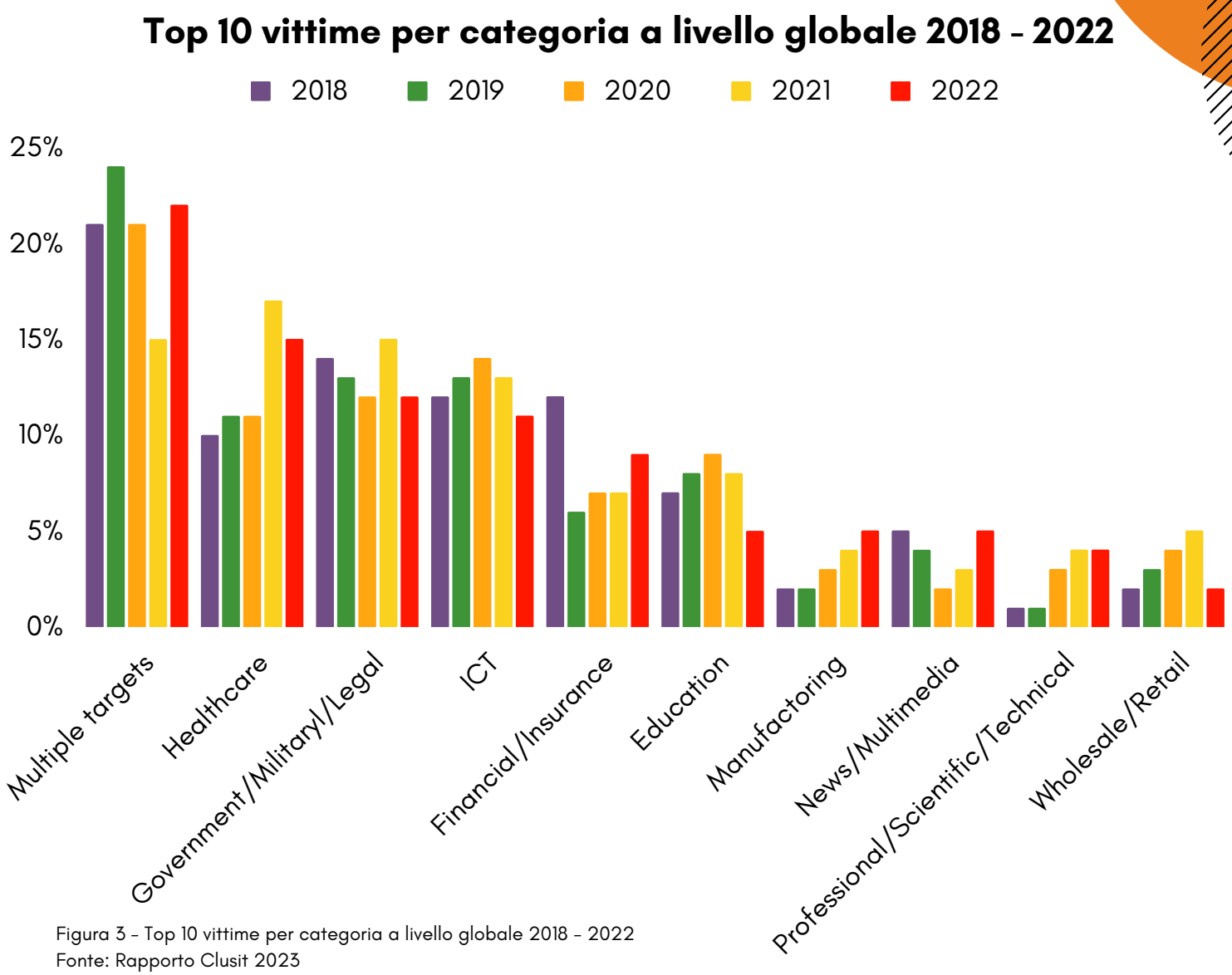


Figura 3 - Top 10 vittime per categoria a livello globale 2018 - 2022
Fonte: Rapporto Clusit 2023

In coerenza con quanto avviene a livello globale, anche in Italia si rileva che il numero di incidenti che è cresciuto significativamente, con un aumento del 527% dal 2018 al 2022.

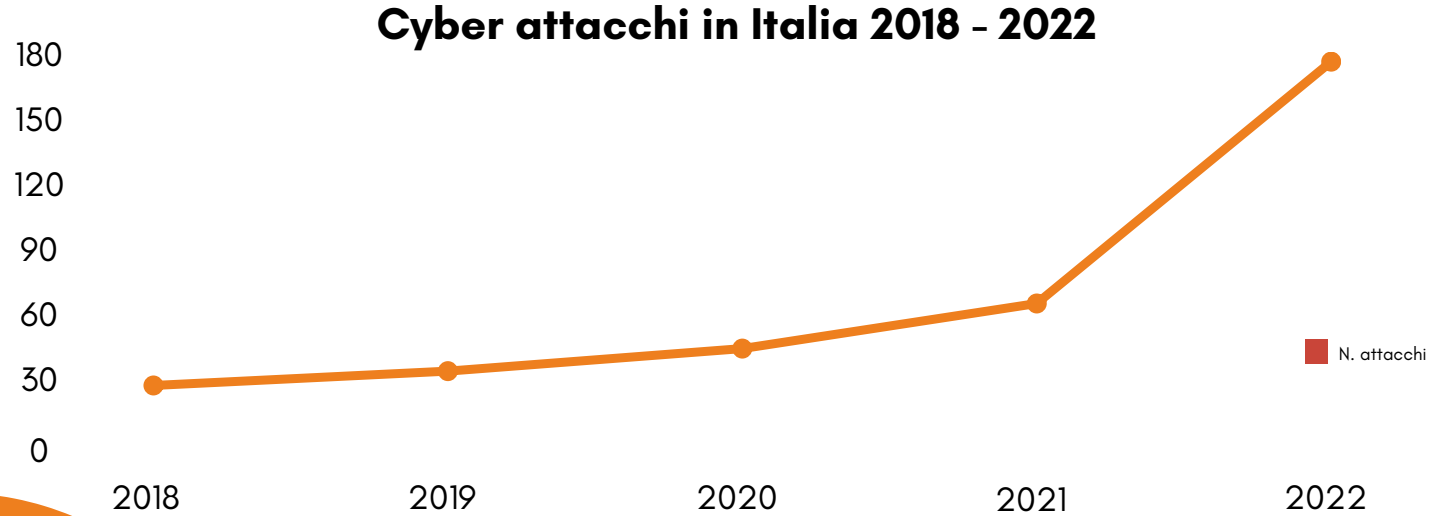


Figura 4 - Cyber attacchi in Italia 2018 - 2022 - Fonte: Rapporto Clusit 2023

Un **dato preoccupante** se confrontato in termine di percentuali di crescita rispetto al dato globale: nel 2022 il dato italiano rappresenta il 7,6% del totale del campione complessivo considerato a livello globale.

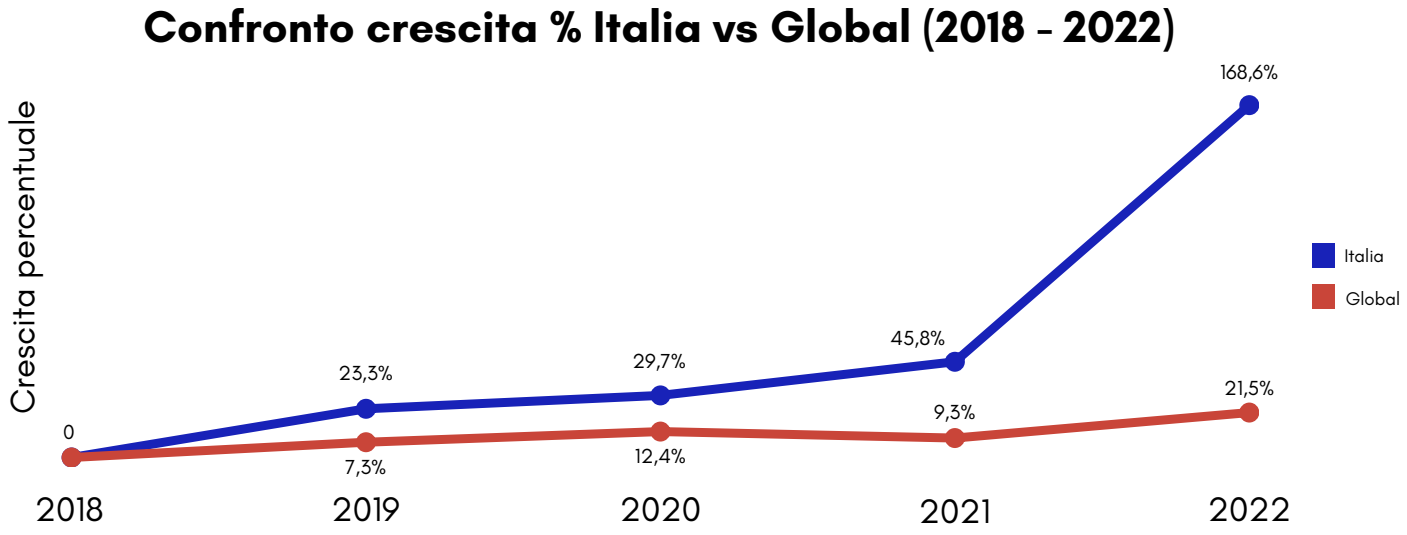


Figura 5 - Confronto crescita % Italia vs Global (2018 - 2022) - Fonte: Rapporto Clusit 2023

La distribuzione delle vittime degli attacchi nel nostro Paese si ripartiscono significativamente in maniera diversa rispetto al campione evidenziato su livello mondiale: la categoria merceologica per cui si rileva un maggior numero di attacchi risulta essere "Government" (20% del totale) e Manufacturing (19%).

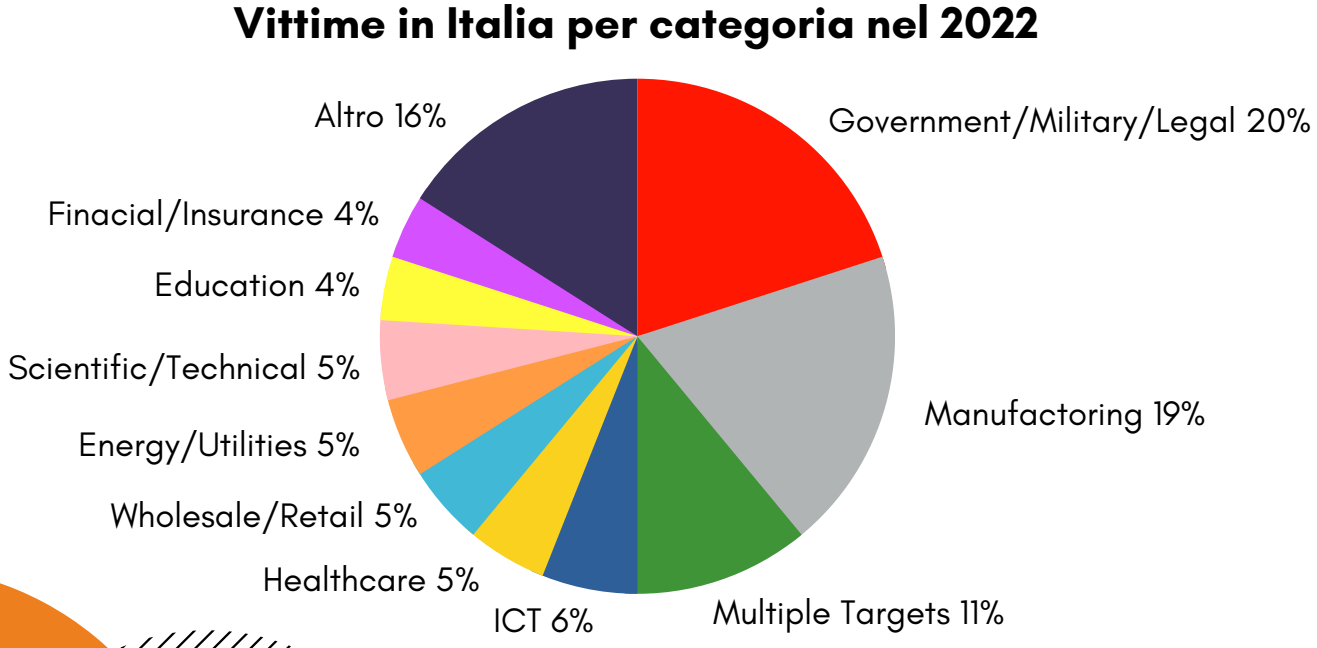


Figura 6 - Vittime in Italia per categoria nel 2022 - Fonte: Rapporto Clusit 2023

Tuttavia, è bene sottolineare come, in coerenza con quanto avviene a livello globale, **l'Italia** registra la **maggiore crescita percentuale** anno su anno per la categoria **Multiple Targets** (+900%), sottolineando come gli attacchi nel nostro Paese sembrano andare di pari passo con il grado di maturità tecnologica negli specifici ambiti: i settori dei servizi professionali, e tecnico-scientifico vedono un incremento del 233,3% di incidenti gravi, l'industria manifatturiera il +191,7%. Essendo tra le più colpite, è rilevante anche la crescita per le organizzazioni del comparto informatico, (+100%) e governativo-militare (+65,2%).

Top 10 vittime in Italia 2018 - 2022

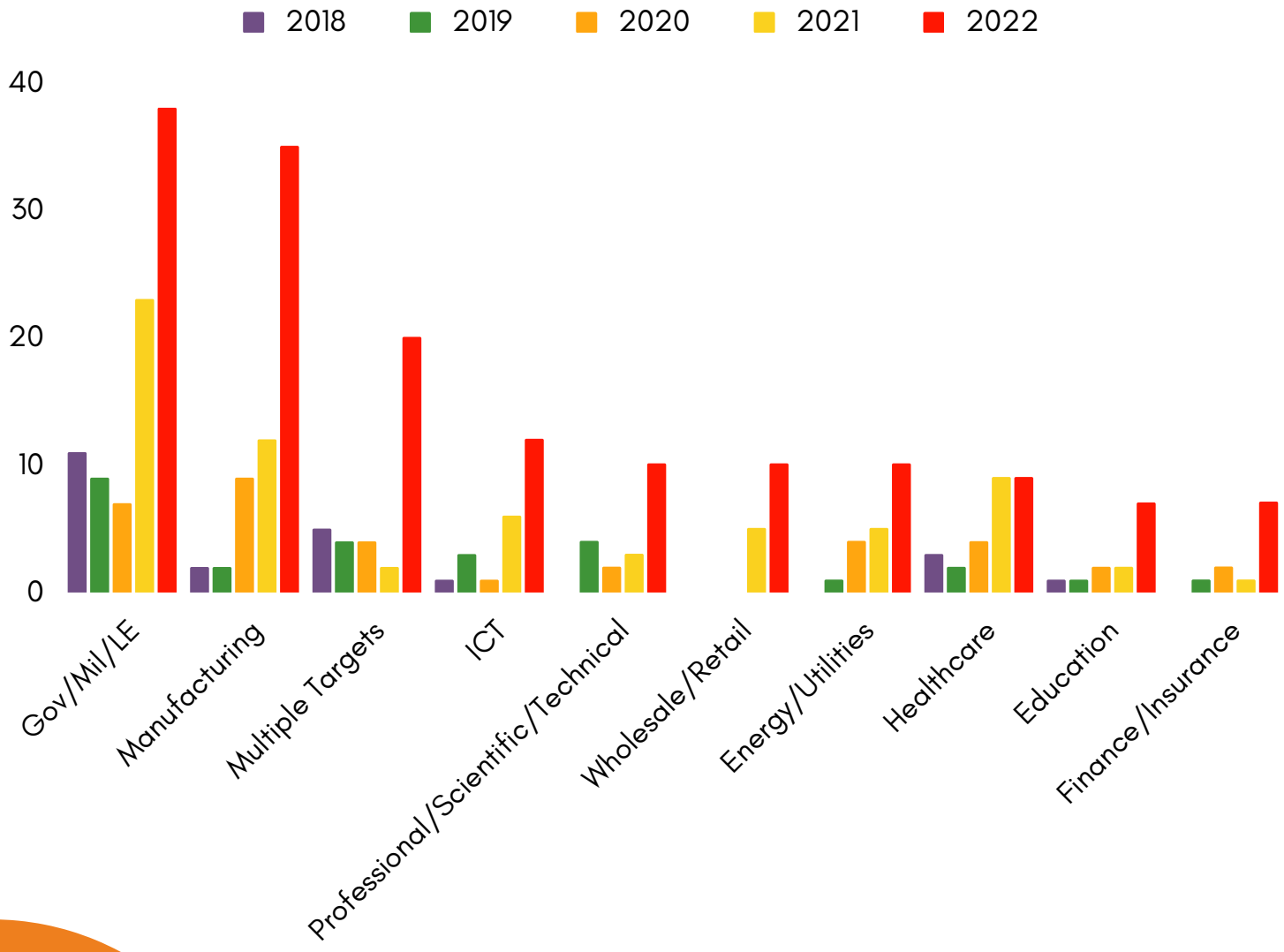


Figura 7 - Top 10 Vittime in Italia 2018 - 2022 - Fonte: Rapporto Clusit 2023

Rispetto alle quattro principali macrocategorie per finalità d'attacco, il **Cybercrime** fa registrare il **maggior numero di episodi** (93% del totale, +11% rispetto al resto del mondo dove la percentuale è pari all'82). In ordine, per numero di attacchi, troviamo a seguire Hacktivism e Spionaggio/sabotaggio, come evidenziato in figura.

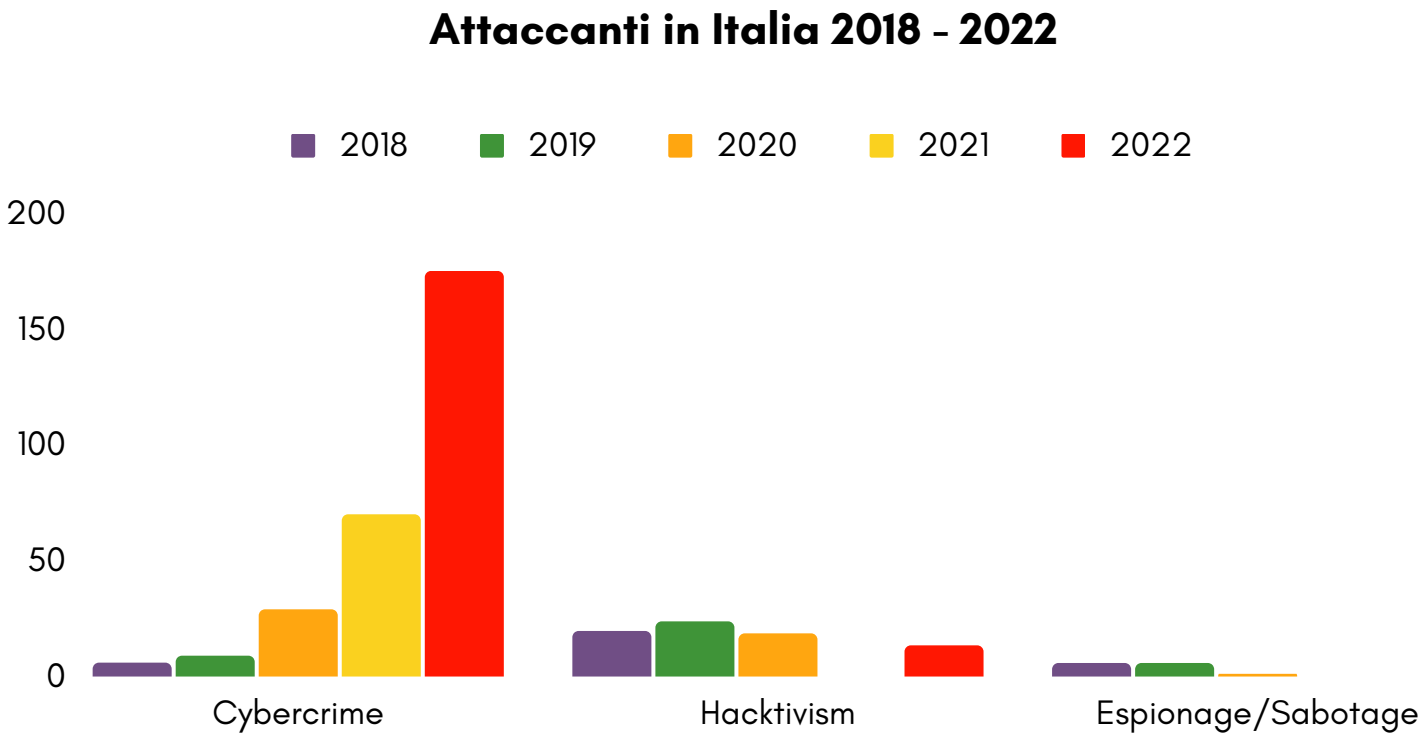


Figura 8 - Attaccanti in Italia 2018 - 2022 - Fonte: Rapporto Clusit 2023

Con riferimento alle tecniche di attacco, in Italia, come nel resto del mondo, **prevalgono** gli **attacchi** tramite **malware** (53%, +6% rispetto al dato globale), ovvero tutte quelle applicazioni finalizzate ad arrecare un danno alla vittima attraverso tecniche oramai standardizzate nel panorama del cyber-crime. Resta invece **preoccupante** la percentuale di **incidenti su vulnerabilità** note che potrebbe facilmente scomparire se le organizzazioni adottassero efficaci processi e procedure di gestione delle vulnerabilità relative alla sicurezza informatica (6% rispetto al 12% globale).

Tecniche di attacco in Italia nel 2022

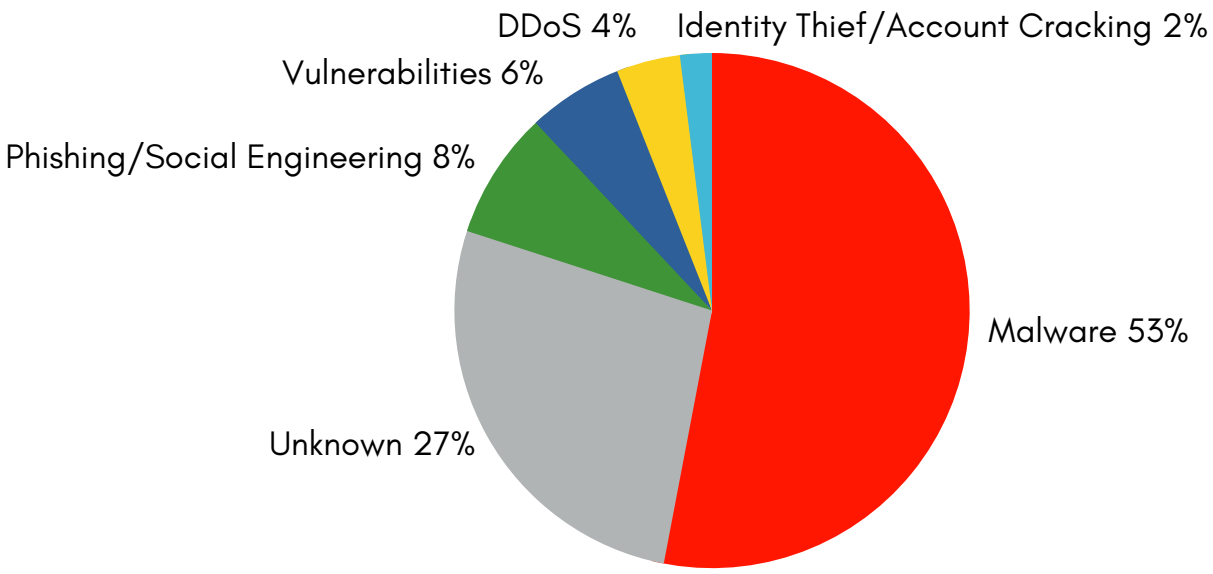
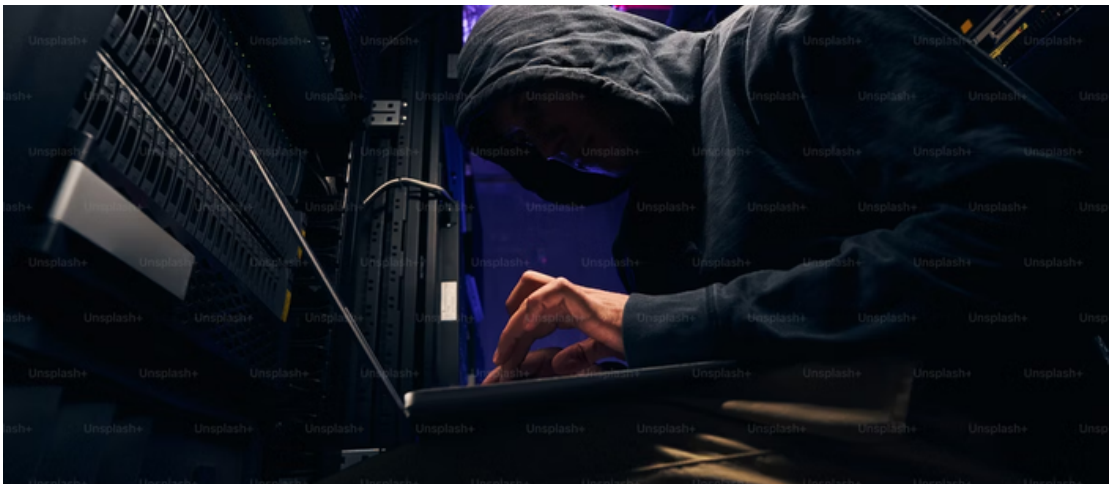


Figura 9 - Tecniche di attacco in Italia nel 2022 - Fonte: Rapporto Clusit 2023

4. VISIONE ITALIA

4.1 Minaccia cibernetica: stato attuale, trend emergenti e attori coinvolti nella lotta alla cybersecurity

Il **contesto geopolitico** e la **pandemia da Covid-19** hanno portato ad un aumento delle minacce cibernetiche a livello globale e nazionale, con **attacchi Ransomware** ai settori dell'**energia**, dei **trasporti**, della **finanza** e dei **servizi governativi**. Lo spionaggio cibernetico è stato soprattutto appannaggio degli attori statuali dotati di ingenti risorse umane e strumentali. Gli **attacchi degli hacktivisti** si sono indirizzati verso la **questione ucraina** e solo inizialmente verso il **settore sanitario nazionale** come forma di protesta contro le disposizioni per il contenimento della pandemia da Covid-19. Nella lotta alla minaccia cibernetica, i Servizi Segreti Italiani si sono concentrati sulla rilevazione e il monitoraggio degli attacchi, principalmente da parte dei gruppi APT (Advanced Persistent Threat).



Questi gruppi sono spesso affiliati a entità governative e sono caratterizzati da una grande abilità nell'intrusione e nella realizzazione di campagne digitali a lungo termine. Tendono a concentrarsi sullo spionaggio cibernetico, ma anche su **attacchi "disruptive" e "destructive"**.

Gli attacchi di tipo **"disruptive"** sono in grado di causare violazioni alla confidenzialità, integrità e disponibilità di sistemi e informazioni, così come malfunzionamenti su dispositivi e reti digitali o interruzioni di rete limitate nel tempo.

Gli attacchi **"destructive"**, invece, sono in grado di rendere completamente inutilizzabili i sistemi colpiti, ostacolandone la ricostruzione.

I Servizi hanno osservato che le attività digitali hanno in prevalenza interessato le infrastrutture informatiche riferibili a soggetti privati, con particolare attenzione verso i settori delle infrastrutture digitali/servizi IT, dei trasporti e del bancario. Le azioni in danno di obiettivi pubblici hanno riguardato principalmente le Amministrazioni Centrali dello Stato e infrastrutture IT riferibili a enti locali e strutture sanitarie. Per quanto riguarda la tipologia di attori ostili, con alcuni gruppi attivi in territorio nazionale che hanno esfiltrato dati sensibili o installato "backdoor" su risorse digitali riconducibili ad alcune Aziende Sanitarie Locali e associazioni sindacali.

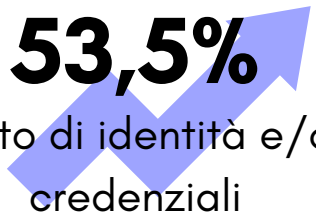
Il numero di **gruppi coinvolti** nello spionaggio cibernetico è **aumentato** del 3%, rappresentando il 26% del totale. Si osserva inoltre un incremento dei tentativi di accesso alle risorse delle organizzazioni attraverso le vulnerabilità dei sistemi di telelavoro. Gli attori delle minacce stanno utilizzando strumenti reperibili sul deep e dark web per camuffare le loro attività. Le **azioni** di matrice non identificabile sono **diminuite** dal 22% all'18% grazie alle capacità di rilevamento sviluppate dai servizi di intelligence italiani. Le registrazioni di domini malevoli costituiscono il 41% degli attacchi, mentre l'uso di malware, in particolare ransomware, è aumentato. Infine, il furto di identità e/o credenziali è cresciuto del 53,5%.

18%

Azioni di matrice non identificabile

41%

Registrazione di domini malevoli



53,5%

Furto di identità e/o credenziali

4.2 Le Attività dell'intelligence per la sicurezza nazionale e il rafforzamento delle difese legali

L'attività di intelligence nel 2022 ha permesso di monitorare la crescente minaccia cibernetica, proveniente da attori statali, organizzazioni criminali e hacktivisti, che mirano a diversi obiettivi, tra cui spionaggio, ritorno economico e discredito.
Si sono **utilizzate diverse tecniche d'attacco**, tra cui software malevoli e ransomware, e si è registrato un aumento delle azioni contro obiettivi privati, oltre a nuovi trend di attacco durante l'invasione russa dell'Ucraina. L'attività di intelligence nel 2022 ha permesso di monitorare la crescente minaccia cibernetica, proveniente da attori statali, organizzazioni criminali e hacktivisti, che mirano a diversi obiettivi, tra cui spionaggio, ritorno economico e discredito. Si sono utilizzate diverse tecniche d'attacco, tra cui software malevoli e ransomware, e si è registrato un aumento delle azioni contro obiettivi privati, oltre a nuovi trend di attacco durante l'invasione russa dell'Ucraina. Le statistiche del Comparto dimostrano un **aumento** degli **attacchi** per ottenere **vantaggi economici** (53% rispetto al 9% dell'anno precedente) e delle incursioni digitali per minare **la reputazione** dei sostenitori delle parti coinvolte nel conflitto russo-ucraino (31% rispetto all'1% dell'anno precedente). Le campagne di spionaggio (3%) sono state dirette ai sistemi dei Dicasteri CISR, ovvero Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanza e infine Sviluppo Economico, e fornitori nazionali di servizi di comunicazione elettronica, utilizzando tecniche sofisticate.

Gli **attacchi senza** una chiara **finalità** sono **diminuiti** dall'anno precedente (13% rispetto al 80%).
Il **Decreto "Aiuti bis"** conferisce al Presidente del Consiglio il potere di **autorizzare** particolari **misure di intelligence** di contrasto in situazioni di crisi o emergenza, potenziando la capacità di contrasto e risposta del Comparto intelligence contro la minaccia cibernetica che è in costante evoluzione. L'implementazione efficace dell'innovazione tecnologica nel settore dell'intelligence richiede una **partnership tra Pubblico e Privati** che sostenga l'innovazione e la ricerca, un primo passo in questa direzione è rappresentato dalla ratifica del Secondo Protocollo addizionale al Trattato sulla criminalità informatica (la Convenzione di Budapest del 2001), che è stata sottoscritta da 22 paesi del Consiglio d'Europa, tra cui l'Italia, con l'autorizzazione dell'UE mediante la Decisione 2022/722 del Consiglio del 5 aprile 2022, con lo scopo di contrastare le attività cyber-criminali finalizzate all'accumulo di risorse finanziarie.

4.3 Il ruolo della Difesa: Operazioni Multidominio e Cyber Warfare

Il mondo digitale ha raggiunto un'importanza geopolitica e geostrategica fondamentale, poiché rappresenta un possibile supporto alle operazioni militari e un elemento di diffusione e intensificazione di altre minacce. **La sfera informatica** dei conflitti si è ormai **fusa** con quella tradizionale, aumentando il pericolo e allargando l'ambito cognitivo. L'uso delle nuove tecnologie nel campo dell'informazione e dei social media ha evidenziato il potenziale per destabilizzare e influenzare l'opinione pubblica. In questo contesto, il cyberspazio rappresenta un fattore abilitante che amplifica il potenziale delle minacce ibride e costituisce un campo ideale per l'estremismo violento.

Anche i Carabinieri stanno sviluppando capacità:

Internet investigation

Digital forensics 

al fine di potenziare i sistemi di analisi delle investigazioni scientifiche e condurre **attività investigative** relative al **cybercrime**, al **deep web** e agli **scambi** finanziari in **criptovalute**. Il contesto attuale è caratterizzato da molteplici dinamiche che portano a situazioni di instabilità e minacce persistenti, alimentando uno stato di competizione permanente tra gli attori internazionali. Le moderne minacce sono multidimensionali e trasversali, rendendo obsoleto il concetto lineare di escalation militare.

L'esigenza è quella di pensare alla sicurezza e alla difesa nazionale in un'ottica di sistema-paese in cui tutti gli interessi sono collegati e interdipendenti. L'approccio nazionale deve consentire di sviluppare policy, normative e procedure innovative e ad ampio spettro che permettano alla Difesa di sviluppare capacità per operare efficacemente nelle nuove forme del confronto e contribuire a giocare un ruolo attivo nel continuum of competition. La nuova strategia di Difesa nazionale integrata richiede un ripensamento delle modalità di affrontare il confronto nella dimensione militare.
Nasce quindi il concetto di **Operazioni Multidominio (MDO)** e della loro importanza nell'intero spettro della competizione militare. Le MDO si basano sulla **presa di consapevolezza** che **non** è **possibile** mantenere una **supremazia** costante in **tutti i domini**, ma che è possibile sfruttare delle finestre di opportunità limitate entro cui far convergere gli effetti tramite una combinazione integrata di capacità militari e non militari nei diversi domini. Affinché tali azioni siano efficaci, occorre **applicare** costantemente l'**approccio Multidominio** e **migliorare la** situational **awareness**, sfruttando le Emerging & Disruptive Technologies (EDT). Il successo nelle operazioni Multidominio dipende dall'integrazione di tutti i fattori coinvolti e dall'attitudine ad intercettare gli indicatori della minaccia alla Sicurezza nazionale. Particolare attenzione verrà data al dominio cibernetico, con lo sviluppo e il rafforzamento di competenze specifiche e di strumenti e capacità di Cyber Warfare impiegabili nell'intero spettro delle operazioni.

5. INTERVISTE

Il presente report sulla cybersecurity è **impreziosito da** un ciclo di **interviste** condotto con **figure apicali** di diversi settori. L'obiettivo del ciclo di interviste è stato quello di **approfondire** il **contesto** e lo stato dell'arte attuale in **ambito sicurezza informatica**. Gli intervistati sono stati selezionati in base alla loro esperienza e conoscenza del settore, con l'obiettivo di fornire una visione completa e dettagliata delle sfide e delle opportunità che caratterizzano il mondo della cybersecurity. Grazie alla loro partecipazione, abbiamo acquisito una panoramica dettagliata sulle tendenze attuali e sulle strategie adottate dalle organizzazioni per proteggere le proprie attività e i propri dati da minacce sempre più sofisticate.
Le interviste sono state eseguite tramite videocall tra Aprile e Maggio 2023.

planetica

> “Quali sono le **principali** / **nuove minacce** informatiche che si prevede potrebbero verificarsi nei prossimi mesi?”

CIO Automotive

L'**interconnessione dei veicoli** emerge come una **minaccia** crescente. Sebbene l'automazione e la connettività portino con sé benefici significativi, è fondamentale riconoscere e affrontare le sfide correlate. Il **punto** più **critico** risiede nei **fornitori** che, rispetto a noi, possono risultare meno strutturati e pronti ad affrontare tali minacce. Questo configura un pericolo notevole nella catena di valore e nella supply chain. Riteniamo sia cruciale che tutti stiano attribuendo a questa questione la giusta importanza. Personalmente, spero che i fornitori che **non** mostrano un **adeguato livello di sicurezza** possano essere inseriti in una "**Blacklist**" per garantire la sicurezza globale del settore.

CIO Energy & Utility

In termini qualitativi, attacchi informatici come **ransomware, phishing e whaling** rimangono una **costante minaccia** come negli anni passati. Tuttavia, in termini quantitativi, stiamo assistendo a un **aumento preoccupante delle minacce**, con una proiezione di triplicazione di tali attacchi anno su anno. Questa è una realtà che richiede un aumento dell'attenzione e della preparazione da parte delle organizzazioni. Inoltre, vediamo un incremento nella frequenza degli "attacchi sociali", che mirano a **manipolare** e sfruttare la **fiducia** degli individui, costituendo un'importante sfida per la sicurezza.

CISO Truck & Industrial Equipment

Si distinguono **tre grandi pericoli**. Prima di tutto, i **ransomware**, che compromettono la reputazione di chi è attaccato. Poi, gli **attacchi** legati alle **tensioni geopolitiche**, perpetrati da gruppi paramilitari di cybercriminali. Infine, c'è l'**AI**, che a causa degli errori degli utenti e delle potenziali applicazioni maliziose e fraudolente della tecnologia, rappresenta un rischio significativo.

CIO Automotive Supply

Le minacce **principali** sono rappresentate dalla disponibilità di strumenti d'attacco avanzati e dalla sofisticazione crescente dei gruppi criminali. In termini di aree di attacco, la supply chain rimane particolarmente esposta.

planetica

“Quali sono i principali fattori che possono influenzare la sicurezza informatica (tecnologia, fattore umano, altro) di un'organizzazione e come possono essere gestiti?”

CIO Automotive

L'**obsolescenza** è un rischio, magari a fronte di investimenti importanti sull'IT in altre aree (ad esempio in manufacturing) le tecnologie sono una potenziale fonte di pericolo; penso anche che il **fattore umano** sia l'anello più debole della catena.

CIO Energy & Utility

Tecnologia e **fattore umano**, entrambe, così come la sicurezza in un’auto dipendono dalle specifiche tecniche della suddetta e dalla guida del pilota. Come si può rendere più sicura la guida? dotando la vettura di optional di sicurezza (ABS, Luci, Adas) ma se la si guida in modo pericoloso è del tutto inutile.
Che fare? Riguardo alle tecnologie, bisogna **dotarsi** di tutte (o quasi, in funzione di un rapporto rischio/costo della **tecnologia**) quelle che servono, ma evidentemente **non bastano** i **firewall**, i **SOC** e quant’altro per evitare di “cadere nella rete”: fondamentale la consapevolezza dei dipendenti, il “prima di cliccare, pensaci”. Noi in azienda **ci siamo dotati** delle **tecnologie** più all'**avanguardia** (Antivirus, Antiphishing, un SOC che gestisce tutte le threat di gruppo e un servizio che fa il Triage di tutte le minacce che riceviamo) in quanto membri della comunità informatica che fornisce servizi essenziali allo stato italiano siamo monitorati dallo CSIRT.

CISO Truck & Industrial Equipment

Il **fattore umano** è molto forte, noi **facciamo** delle campagne di sensibilizzazione; facciamo **fake phishing** e a livello apparente la gente è attenta ma appena inseriamo allegati o magari sfruttiamo il black Friday o eventi di questo tipo l'errore umano aumenta rapidamente.

CIO Automotive Supply

Non c'è solo un fattore, sia la **parte IT** che il **fattore umano** al **50%** concorrono al **rischio**; noi stiamo investendo in tutte e due gli ambiti, nuovi software e protocolli così come continue sensibilizzazione sul phishing con test e eventuale formazione aggiuntiva per chi ne ha bisogno.

planetica

“Quali sono **le principali azioni** che le aziende dovrebbero mettere in atto **per proteggersi** da queste minacce (organizzazione interna Cyber, awareness dipendenti, investimenti in tecnologie, ecc.)?”

CIO Automotive

Attualmente, le attività più fruttuose sono rappresentate dagli attacchi di phishing simulati e casuali, che forniscono importanti indicatori per individuare chi necessita di formazione supplementare. Ci avvaliamo anche di **società terze per condurre test** di penetrazione che rilevano occasionalmente errori compiuti anche dai nostri tecnici più esperti, come l'utilizzo di password già usate o la codificazione. Un'idea potrebbe essere l'introduzione di **meccanismi di audit** per anticipare la problematica.

CIO Energy & Utility

Come precedentemente accennato, tutte queste misure insieme formano un sistema di difesa in cui il 'punto più debole' è determinante: basta un piccolo varco nella muraglia del castello per creare una vulnerabilità facilmente **sfruttabile dagli hacker**. Inoltre, è fondamentale garantire l'aggiornamento costante dei software.

CISO Truck & Industrial Equipment

La struttura interna dedicata alla sicurezza informatica deve gestire efficacemente tutto, a partire dalla **conformità normativa**, passando per la formazione, fino alla rilevazione delle minacce. Abbiamo effettuato notevoli investimenti tecnologici, ma a mio avviso l'aspetto cruciale è insistere con il consiglio di amministrazione e i dirigenti affinché comprendano **l'importanza della cybersecurity**.

CIO Automotive Supply

Riguardo l'organizzazione interna per la sicurezza informatica, quest'anno abbiamo stabilito un incontro trimestrale con il consiglio di amministrazione, durante il quale possiamo richiedere supporto organizzativo. In questo modo, si realizza un efficace **approccio 'top-down'** e si organizza la **simulazione di attacchi**.

planetica

“**Come** si può **migliorare** la **consapevolezza** dei dipendenti sull'importanza della sicurezza informatica e su come gestire correttamente i dati sensibili?”

CIO Automotive

La **formazione** rappresenta il fulcro della nostra strategia: **offriamo contenuti** didattici **online**, corsi annuali sulla protezione dei dati e sulla privacy. Questi sono **considerati obbligatori**, poiché insistiamo affinché vengano completati da tutti i membri del personale.

CIO Energy & Utility

Abbiamo **adottato** una serie di **misure**. Innanzitutto, conduciamo **esercizi di phishing** fittizi per misurare il grado di vulnerabilità dei nostri dipendenti. **Abbiamo sviluppato procedure** operative **per classificare i dati** come **pubblici**, **confidenziali**, **strettamente confidenziali** e segreti per prevenire divulgazioni inappropriate. Le nostre applicazioni più sensibili tracciano automaticamente download e accessi. Infine, seguendo la **politica** del '**bisogno minimo di informazioni**', concediamo agli utenti solo i privilegi minimi necessari per svolgere il proprio lavoro.

planetica

“Data la crescente **importanza** della **sicurezza** informatica nella **supply chain**, quali sono i principali rischi e come si possono gestire in modo efficace?”

CIO Automotive

Rispetto al rischio nella supply chain, il più **grande problema** è l'Internet delle Cose (**IoT**) e le sue applicazioni nei plant produttivi. Le linee di produzione possono essere bloccate molto facilmente e ci sono diversi casi noti di problemi di questo tipo, ad esempio, Toyota.

CIO Energy & Utility

La nostra politica prevede di **interrompere** tutte le **connessioni VPN** con un **fornitore** che subisce un **attacco**. Tuttavia, la velocità con cui gli attaccanti possono muoversi rappresenta un problema, poiché la minaccia potrebbe essere già penetrata quando riusciamo a disconnetterci. In tali circostanze, **forniamo ai fornitori PC aziendali** per escludere i loro sistemi dal network.

CISO Truck & Industrial Equipment

Stiamo lavorando per **identificare i rischi** associati agli **attacchi ai fornitori**, che possono portare a interruzioni della catena di fornitura o a frodi. A tal fine, stiamo **definendo** dei **processi** per ottenere **autovalutazioni** dai **fornitori** sulle misure di sicurezza che hanno implementato.

CIO Automotive Supply

Fornitori e clienti, a causa della nostra stretta integrazione, possono **diventare canali** per gli attacchi. Per questa ragione, lavoriamo con società specializzate nel **monitoraggio** continuo dei fornitori e abbiamo sviluppato linee guida specifiche. Inoltre, cerchiamo di **fornire formazione** congiunta per aumentare la consapevolezza in materia di sicurezza.

planetica

“Quali sono le **tecnologie emergenti** che potrebbero avere un impatto critico sulla sicurezza informatica in futuro e come dovrebbero essere gestite per garantire la massima sicurezza?”

CIO Energy & Utility

Mentre l'**IoT**, soggetto a vulnerabilità, presenta dei rischi, considero l'**Intelligenza Artificiale** come l'emergente tecnologia più critica per la sicurezza informatica.

CISO Truck & Industrial Equipment

Utilizziamo il **machine learning** per identificare attacchi tramite **AI**, e impieghiamo autenticazione multifattore o biometrica.

CIO Automotive Supply

Il **Quantum Computing** è al centro dell'attenzione, soprattutto per le sue applicazioni nel campo della **crittografia**. L'industria tecnologica è al lavoro per sviluppare chiavi o metodi alternativi in grado di contrastare potenziali usi malevoli del Quantum Computing. Per quanto riguarda la **Blockchain,** pur essendo progettata per essere sicura, alcuni rischi persistono e necessitano di monitoraggio. Infine, l'**Intelligenza Artificiale** è un'altra tecnologia da tenere sotto osservazione.

planetica

"Quali sono le possibili **future minacce** di **cyberattacchi** nel contesto geopolitico attuale e futuro in cui ci troviamo (guerre, flussi migratori, blocco orientale con Russia, Cina, Nord Corea, altro)?"

CIO Automotive

La nostra azienda ha avuto presenza in Russia e Ucraina, per cui abbiamo adottato misure preventive per assicurare la sicurezza delle nostre operazioni, mettendo in **campo strategie e firewall** per difenderci anche da possibili dipendenti insubordinati. L'anno scorso, la situazione è stata monitorata con particolare attenzione, data la nostra preoccupazione per possibili attacchi mirati, che fortunatamente non si sono verificati. Si può dire con certezza che l'**area orientale comporta** un grado di **rischio** superiore rispetto all'occidente.

CIO Energy & Utility

La minaccia è considerevole, motivo per cui abbiamo proceduto con la **disattivazione degli accessi** alla nostra rete da qualsiasi account originario di determinati Paesi, come Russia, Bielorussia e Corea del Nord.

CISO Truck & Industrial Equipment

Diamo la **massima priorità** a questo aspetto, cercando di delimitare e rimanere **vigili** nei confronti dell'industrializzazione di questi gruppi di hacker.

CIO Automotive Supply

Essendo un'azienda con operazioni internazionali, ci troviamo esposti a tutte queste guerre e flussi migratori. Abbiamo impianti in zone di conflitto e stiamo lavorando attivamente per garantire la nostra capacità operativa, indipendentemente dalle circostanze. Abbiamo dovuto **affrontare anche problemi** relativi alla catena di **approvvigionamento**.

planetica

"Quali sono i **potenziali rischi** per la sicurezza associati all'utilizzo dei **social media** da parte dei dipendenti durante l'orario di lavoro e quali misure possono adottare le organizzazioni per mitigare questi rischi senza limitare completamente l'accesso?"

CIO Automotive

Non imponiamo restrizioni, poiché ogni individuo è libero di usare il proprio cellulare come desidera. Abbiamo politiche che **proibiscono** di pubblicare immagini dei prodotti o informazioni interne all'azienda. Eventuali violazioni sono solitamente commesse da terze parti.

CIO Energy & Utility

Siamo **vulnerabili** agli **attacchi via social media**, in quanto la nostra unica difesa dipende dal comportamento di 5500 dipendenti, il che rende quasi impossibile coprire tutti. Attraverso i social media, si può creare una rete di informazioni tramite i parenti o i "follower" per raggiungere il personale 'sensibile'. Abbiamo **una procedura** che proibisce la **divulgazione** di informazioni aziendali e fino ad ora non abbiamo avuto violazioni in tal senso.

CISO Truck & Industrial Equipment

Ci sono **due rischi potenziali**. Molte associazioni riescono a **identificare i dirigenti** tramite i social media, mettendoli **potenzialmente in pericolo**. Succede anche che i **dipendenti**, o persone che pretendono di essere tali, **pubblichino** sui social media contenuti razzisti, omofobi, etc., causando una serie di problemi.

CIO Automotive Supply

Il **rischio principale** è che le persone possano condividere inconsciamente su **social media** informazioni sensibili o riservate, la maggior parte delle volte per semplice ingenuità. Inoltre, c'è la **questione dell'ingegneria sociale**, con attacchi che nascono dalla raccolta di informazioni sui social media. A mio parere, le soluzioni si trovano all'incrocio tra il mondo cyber e l'HR, con politiche mirate e formazione. È meglio implementare una certa forma di blacklist e qualche tecnologia DLP.

planetica

“Quali sono i **rischi** in ambito **compliance e protezione** della proprietà intellettuale che si presentano quando si utilizzano tecnologie come A.I. e web 3 (es. Blockchain)?”

CIO Automotive

In questo momento non stiamo **implementando misure specifiche**, ma vista la rapida crescita degli ultimi anni, questo sarà senza dubbio un campo in evoluzione.

CIO Energy & Utility

Si tratta di un **argomento piuttosto complicato,** con questioni legali che, sinceramente, trovo difficili da affrontare.

CISO Truck & Industrial Equipment

Ci potrebbero essere dei **rischi**. Prendiamo, ad esempio, l'ipotesi in cui **un'intelligenza artificiale comparasse due documenti** per determinare il migliore: otterresti una **risposta rapida**, **ma** avresti **condiviso con l'IA le tue informazioni** o proprietà intellettuali o quelle dei tuoi fornitori, senza conoscere bene le possibili implicazioni. Ciò che stiamo facendo per proteggerci è **redigere regolamenti** e creare linee guida per affrontare anche la possibile violazione del copyright da parte del software installato dall'utente.

CIO Automotive Supply

I **rischi** sono gli stessi di cui abbiamo discusso precedentemente. **Non** crediamo che la soluzione sia **chiudere tutto** e proibirne l'uso, piuttosto riteniamo che sia **più efficace monitorare** attentamente e avere le risorse necessarie per gestirli in modo controllato.

planetica

“Come possono **garantire** le aziende che il loro utilizzo **aderisca** alle leggi sul **copyright** e sulla **proprietà intellettuale**?”

CIO Energy & Utility

Adottiamo **misure precauzionali** a livello contrattuale, **stabilendo** per iscritto a chi **appartiene la proprietà intellettuale**, sia che essa risieda nell'azienda o nell'ente esterno che ci fornisce il prodotto.

CIO Automotive Supply

L'approccio che adottiamo prevede l'**implementazione di un front end** di nostra gestione, possibilmente attraverso strumenti di analisi comportamentale e modelli di governance. Utilizziamo anche Policy, **formazione e soluzioni** di prevenzione della perdita di dati per prevenire eventi imprevisti.

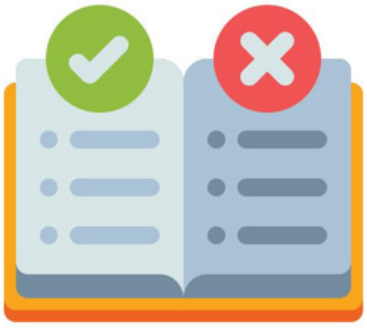
6. RESILIENZA INFORMATICA

A conclusione dell'anno appena trascorso, il Parlamento Europeo ha approvato due importanti regolamenti: la **Direttiva DORA e NIS2.** Entrambi gli atti legislativi si pongono l'obiettivo di stabilire il nuovo quadro per la resilienza digitale e la sicurezza informatica che impatterà i player appartenenti alla sfera dei servizi finanziari su tutto il territorio europeo.

Il "Digital Operational Resilience Act", noto come "**DORA**", è stato approvato a dicembre 2022, al fine di uniformare a livello europeo le norme e gli standard fino ad oggi emanati per **mitigare il rischio ICT nel settore dei servizi finanziari**. In sintesi, DORA garantisce che aziende e fornitori operanti nei financial services predispongano le necessarie misure atte a mitigare gli attacchi informatici ed altri rischi che potrebbero minare la resilienza operativa digitale, stabilendo obblighi concreti di sicurezza informatica, regolando i termini contrattuali, descrivendo il ruolo prudenziale dei regolatori finanziari sulla sicurezza informatica e creando requisiti attorno alla gestione del rischio della catena di approvvigionamento.

DORA si applicherà a una **vasta gamma di entità finanziarie**, tra cui istituti di credito e di moneta elettronica, società di investimento, imprese di assicurazione e riassicurazione. Inoltre, impatterà anche le organizzazioni definite dal Regolamento come "Fornitori critici di servizi ICT", che erogano ad esempio risorse cloud edata analytics.

In termini pratici, **DORA prevede che le aziende seguano i principi di governance relativi al rischio ICT**, ponendo particolare attenzione alla responsabilità del corpo direttivo. Si dovranno intraprendere azioni di **assessment** sulla tolleranza al **rischio ICT**, basandosi su appositi framework. Gli enti, inoltre, devono **prevedere** un quadro di **gestione del rischio** che includa l'identificazione delle funzioni critiche e importanti, dei rischi associati e una mappatura dei beni ICT che le supportano, nonché specifici piani e capacità di protezione, prevenzione, rilevamento, risposta e ripristino, processi di **miglioramento continuo** e metriche, ed una strategia di comunicazione di crisi con ruoli e responsabilità definiti chiaramente.



In secondo luogo, il **Regolamento** introduce una metodologia standard di **classificazione degli incident** definita attraverso un insieme di criteri specifici (numero di utenti interessati, durata, diffusione geografica, perdita di dati, gravità dell'impatto sui sistemi ICT, criticità dei servizi interessati, impatto economico) e relative soglie che verranno pubblicate nel corso del 2024 all'interno delle RTS, ovvero Regulatory Technical Standards.

Gli incident **classificati** come **gravi** dovranno essere segnalati al regolatore nell'arco della medesima giornata, facendo riferimento alle linee guida contenute nel Regolamento. Si richiede inoltre di compilare report di follow-up, a distanza di una settimana e di un mese dall'episodio, che verranno pubblicati e condivisi con gli altri enti.

Grande **attenzione** viene posta anche sulle strategie di resilience testing, nel perimetro delle quali le **entità coinvolte** devono mettere in atto un completo programma di test, che **comprenda** una serie di **valutazioni**, **test tecnici**, **metodologie**, pratiche e strumenti, avvalendosi di figure specializzate, certificate ed indipendenti.
La Direttiva ribadisce, infine, la necessità per le organizzazioni finanziarie di dotarsi di una strategia per la gestione dei rischi delle terze parti ICT che preveda la mappatura di tutti i provider di servizi tecnologici, le attività erogate e le funzioni supportate. I fornitori dovranno essere valutati sulla base di **criteri definiti** (ad esempio livello di sicurezza, rischio di concentrazione, rischi di sub-outsourcing) e si dovrà predisporre una strategia di uscita in caso di fallimento di un fornitore.

I **fornitori critici** saranno **oggetto di valutazione** annuali effettuate direttamente dal regolatore, relativamente a **requisiti** di resilienza come **disponibilità**, **continuità**, **integrità** dei dati, **sicurezza** fisica, processi di gestione del rischio, governance e strategie di test.
Le preoccupazioni relative alla sicurezza cibernetica non sono limitate al settore dei servizi finanziari. Di fronte alla **crescente minaccia informatica** e ai sempre più sofisticati attacchi, il Parlamento Europeo dispone l'aggiornamento della direttiva sulla sicurezza delle reti e delle informazioni (NIS) (UE) 2016/1148, per stabilire obblighi più rigorosi in materia di gestione dei rischi informatici, segnalazione degli incident e condivisione delle informazioni applicabile ad un'ampia gamma di settori.

In termini pratici, **la NIS2** prevede **requisiti** più **rigorosi** rispetto alla Direttiva del 2016 includendo le modalità di risposta agli incidenti informatici, la sicurezza della supply chain, la crittografia, la gestione delle vulnerabilità e l'implementazione di adeguate misure tecniche, operative e organizzative.
Viene ampliato anche il perimetro d'applicazione: NIS2 si estende ad un numero maggiore di entità, coinvolgendo gli enti definiti come "essenziali" (tra cui trasporti, sanità e Pubblica Amministrazione) ed entità "importanti" in altri settori critici (tra cui servizi postali e produttori di alimenti).

La Direttiva **NIS2**, in sintesi, si pone l'obiettivo di favorire una maggiore **collaborazione** e **standardizzazione** in materia di sicurezza informatica nell'UE, tra cui la cooperazione tra le autorità, l'uso di norme e specifiche tecniche, i regimi di certificazione e i registri per alcuni fornitori di servizi (tra cui fornitori di cloud computing, data center e provider di reti di distribuzione di contenuti).
Le entità finanziarie incluse nel perimetro di DORA non dovranno adempiere ai requisiti cybersecurity predisposti dalla NIS2, ad eccezione dei fornitori critici di terze parti di ICT che potrebbero sottostare alle prescrizioni di entrambe le Direttive.
Sia **DORA che NIS2** mirano ad aumentare la resilienza e la sicurezza informatica dell'intera catena di fornitura e includono requisiti specifici in materia di supply chain e subappalto. Di conseguenza, anche le imprese che non sono direttamente interessate da DORA o NIS2 potrebbero sentirne l'impatto in modo indiretto, poiché i clienti coinvolti richiederanno termini contrattuali pertinenti o requisiti di conformità in materia di sicurezza.

7. TOP IT PRIORITIES & OUTLOOK

È importante **evidenziare** che il complicato **assetto economico-politico** del 2022 ha giocato un **ruolo rilevante** nelle **scelte** degli **investimenti** tecnologici e delle iniziative aziendali, influenzando la maggior parte delle strategie a livello IT dei primi mesi del 2023.

Previsione dell'aumento degli investimenti nel 2023 nei settori:

+34%
Analisi dei dati

+28%
Modernizzazione delle applicazioni / sistemi legacy

+26%
Machine Learning / Intelligenza artificiale

Nel corso del prossimo anno, i CIO di tutti i settori intervistati si aspettano di **migliorare l'efficienza operativa** delle protezioni informatiche (58%) e di **migliorare la redditività aziendale** tramite la trasformazione dei processi aziendali (54%).

Aree soggette a maggiore interesse nel 2023

70%
Sicurezza

55%
Analisi dei dati

55%
Privacy/ Conformità dei dati

Aree soggette a minor interesse nel 2023

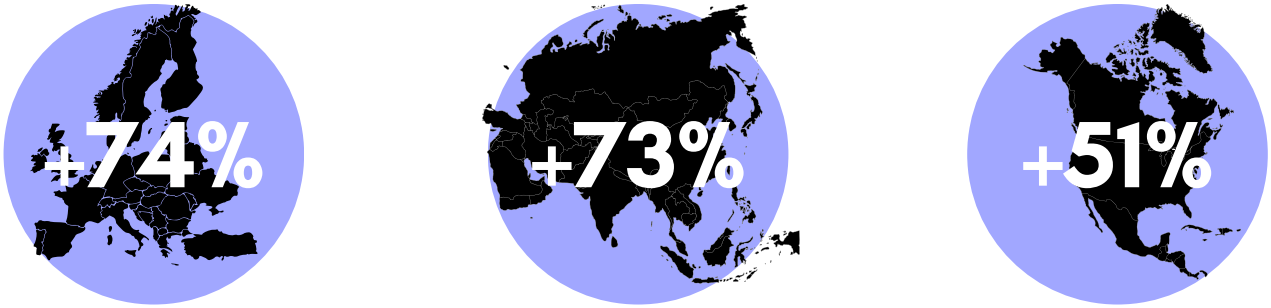
14%
Sicurezza fisica

14%
Migrazione al Cloud

13%
Supply Chain

Pur essendo un tema caldo e di grande interesse a livello globale, **le tematiche** ambientali, sociali e di governance (**ESG**) stanno avendo, e avranno, un impatto marginale sul ruolo dei CIO o sui piani di acquisto IT. Il 64% dei responsabili IT chiede ai CIO di aderire agli standard ESG e di svolgere un ruolo nella selezione di tecnologie informatiche green, ma la percentuale aumenta a livello di azienda (70%).

Richiesta di aderire ai criteri ESG nel mondo:



Mentre l'**incertezza economica** ha colpito il mercato azionario e la salute finanziaria delle aziende, i budget IT ne sono usciti relativamente indenni. Il **44% degli intervistati** e il **56% dei leader IT** prevedono **un aumento dei budget** IT quest'anno, mentre il 35% e il 48%, rispettivamente, prevedono che la situazione rimarrà invariata. Le aziende dei settori dei servizi finanziari (69%), manifatturiero (64%) e governativo (65%) sono più propense a prevedere aumenti in ambito di efficientamento e ammodernamento dei sistemi IT.

Aree soggette ad un aumento del budget

40%
Miglioramento della sicurezza

38%
Aggiornamento dell'infrastruttura IT

38%
Ammodernamento delle applicazioni

Principali cause del taglio del budget per IT

58%
Incertezza economica

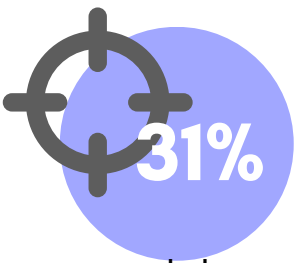
49%
Nuovi piani strategici

38%
Riduzione dell'organico

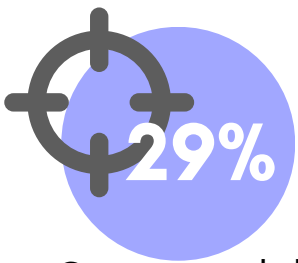
Sebbene le organizzazioni siano ancora focalizzate sulla ricerca di talenti con esperienza nelle aree di competenza critiche, si riscontra un calo di interesse nelle strategie di talent scout. **Gli investimenti IT per le attività di recruiting sono stati citati solo dal 17%** degli intervistati, con una percentuale leggermente più alta tra le aziende del settore dell'istruzione, dei servizi finanziari e della sanità.

Nel tentativo di colmare le carenze di competenze critiche, i reparti IT si rivolgono alle aree legate alla **modernizzazione** e alla **trasformazione,** con l'**integrazione/implementazione** della tecnologia (42%), l'**architettura del cloud IT** (40%) e la **gestione** del **rischio/sicurezza** (36%) che sono le più richieste. L'industria manifatturiera (50%) e i servizi finanziari (51%) hanno più bisogno di skill nell'integrazione e nell'implementazione, mentre la gestione dei rischi e della sicurezza rimane una priorità maggiore per i settori dell'istruzione (54%) e della sanità (50%).

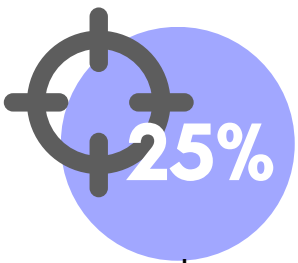
Principali soft skills richieste nel settore IT



Gestione del progetto

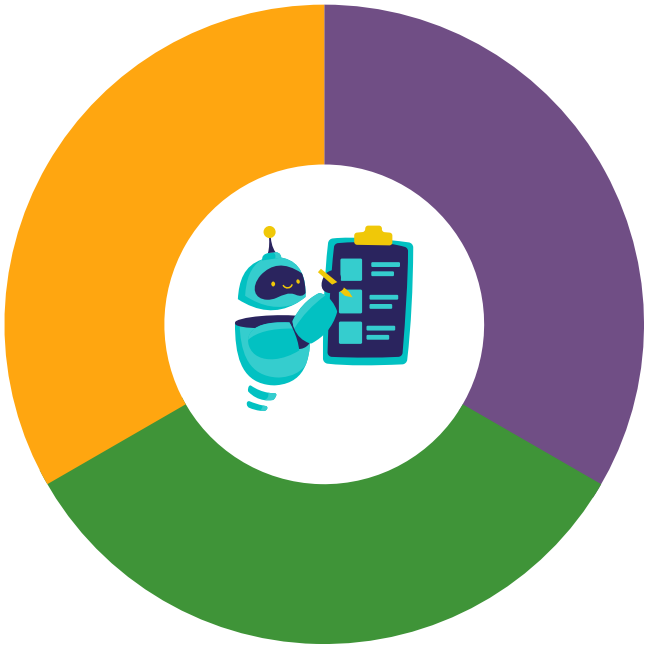


Gestione del cambiamento



Gestione di un piano strategico digitale

Nei **prossimi sei-dodici mesi,** i responsabili IT prevedono di assumere in alcune aree chiave:



Le competenze di **AI/Machine learning sono richieste dal 26%** degli intervistati, così come i candidati con **esperienza DevOps/DevSecOps e Agile (24%)**.

La priorità di queste aree rispetto alle competenze di architettura cloud e servizi cloud/integrazione è una buona indicazione del fatto che i leader IT stanno pianificando il futuro, prevedendo di tornare alle iniziative di trasformazione digitale una volta che le operazioni e la modernizzazione dell'infrastruttura saranno ben avviate.

8. FOCUS

8.1 AI & CYBERSECURITY

Basato sull'architettura GPT-4, **ChatGPT** è stato progettato con l'obiettivo di comprendere e rispondere accuratamente alle richieste degli utenti, migliorando notevolmente l'esperienza di interazione con i sistemi AI.

ChatGPT
sviluppato da OpenAI, è un'evoluzione nel campo dell'AI che mira a fornire conversazioni fluide e coerenti tra utenti e macchine.

Si tratta di un modello di linguaggio basato sull'utilizzo del **Machine Learning** e del **Deep Learning** per produrre testi simili a quelli umani o elaborare risposte a domande più o meno complesse. La tecnologia alla base dell'apprendimento automatico è il **Natural Language Processing** (NPL) che consente al programma di comprendere i modelli e le sfumature del linguaggio umano, tramite l'analisi di grosse quantità di dati, e di sviluppare così risposte pertinenti e coerenti. Ecco che quindi ChatGPT rappresenta uno degli strumenti più sofisticati nel campo dell'AI per la generazione di testo e l'interazione umana, un sistema in grado di adattarsi sempre ai diversi stili di interazione e capace di offrire risposte sempre più personalizzate.

La popolarità della chatbot OpenAI: rischi per la cybersecurity

L'enorme successo della chatbot OpenAI ha attirato l'attenzione dei criminali informatici.

Da inizio febbraio sono stati creati centinaia di siti e applicazioni che imitano l'originale, spingendo le potenziali vittime a fornire le proprie credenziali di accesso per rubarle.

Inoltre, si registra un incremento considerevole nell'utilizzo di Chat GPT da parte di criminali informatici per generare testi ingannevoli e sofisticati destinati alle e-mail di **attacchi di phishing**. Questi cybercriminali sfruttano la notevole precisione e l'abilità del sistema di generare contenuti altamente personalizzati che imitano un linguaggio autentico e spontaneo, rendendo così più difficile per le vittime identificare il tentativo di truffa. Inoltre, la versatilità di Chat GPT potrebbe essere sfruttata per creare **malware polimorfi**, ovvero codici dannosi in grado di modificarsi automaticamente per eludere i sistemi di sicurezza informatica e rendere più complessa la loro individuazione e rimozione.

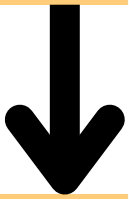
Tuttavia, gli esperti del settore della sicurezza informatica sono concordi nel sostenere che, nonostante le sue potenzialità, Chat GPT non può trasformarsi in una sorta di intelligenza artificiale autonoma per l'hacking. Infatti, le capacità del sistema sono limitate alle funzioni per le quali è stato progettato e addestrato, e la sua efficacia nel perpetrare attacchi informatici dipende in gran parte dall'intervento umano per coordinare e indirizzare le sue azioni. Per questo motivo, è fondamentale adottare misure di sicurezza adeguate e promuovere la consapevolezza degli utenti al fine di **contrastare** efficacemente l'**abuso di tecnologie avanzate** come Chat GPT nel mondo del crimine informatico.

Artificial Intelligence

L'elaborazione artificiale dell'intelligenza rappresenta un'avanguardia tecnologica nel campo informatico che rivoluziona radicalmente il modo in cui gli esseri umani interagiscono con i dispositivi elettronici e come questi ultimi interagiscono tra loro. Essenzialmente, l'AI può essere definita come il processo che consente a macchinari e sistemi informatici di emulare il funzionamento dell'**intelligenza umana**. Tra le numerose applicazioni dell'AI, alcune delle più specifiche riguardano l'analisi del linguaggio naturale, il riconoscimento vocale e la percezione visiva artificiale.

L'**obiettivo** principale dell'**AI** è **dotare i dispositivi elettronici** della capacità di eseguire azioni e ragionamenti complessi, apprendere dalle proprie inesattezze e svolgere funzioni precedentemente riservate all'intelligenza umana. Attualmente, sia in Italia che a livello globale, l'AI viene impiegata in ambito aziendale e oltre, per eseguire mansioni che per l'uomo richiederebbero molto tempo.
L'aspetto della programmazione dell'AI si concentra sull'acquisizione di dati e sulla definizione di regole per convertire i dati in informazioni fruibili.

La classificazione AI debole e AI forte sta alla base della distinzione tra Machine Learning e Deep Learning, due ambiti di studio che rientrano nella più ampia disciplina dell'intelligenza artificiale che meritano un po' di chiarezza, dato che ne sentiremo parlare sempre più spesso nei prossimi anni. Il machine learning (apprendimento automatico) è una branca dell'intelligenza artificiale che utilizza algoritmi e modelli matematici per analizzare dati e fare previsioni o prendere decisioni senza essere esplicitamente programmato per ogni possibile scenario. In pratica, si tratta di un sistema che apprende automaticamente dai dati, invece di essere programmato esplicitamente per eseguire un compito specifico.



Il deep learning è una sottocategoria del machine learning che utilizza reti neurali artificiali con un'architettura complessa per analizzare grandi quantità di dati non strutturati. A differenza di altre tecniche di machine learning, il deep learning è in grado di apprendere da dati non strutturati, come immagini, testo o suoni, senza dover essere esplicitamente programmato per riconoscere determinati pattern o caratteristiche.

Dopo aver chiarito questi concetti, possiamo definire l'intelligenza artificiale come la capacità delle macchine di svolgere compiti e azioni tipici dell'intelligenza umana.

Sfide ed opportunità in ambito sicurezza dell'Intelligenza Artificiale

Nell'era della digitalizzazione e dell'interconnessione, la **sicurezza informatica** è diventata un tema cruciale per la protezione dei dati e delle infrastrutture critiche. La crescente complessità delle minacce informatiche ha reso sempre più evidente la necessità di implementare soluzioni avanzate per contrastare gli attacchi. In questo contesto, l'intelligenza artificiale emerge come uno strumento essenziale per rivoluzionare il panorama della cybersecurity.

L'intelligenza artificiale può essere sia **un'opportunità** che una **minaccia** per la sicurezza informatica. È essenziale comprendere come può essere utilizzata sia per supportare la difesa che nelle fasi di attacco. Gli aggressori possono sfruttare l'IA per analizzare le vittime e studiare strategie di attacco, creando contenuti e liste di distribuzione mirate.

L'IA offre numerosi vantaggi, ma è fondamentale concentrare gli investimenti su ciò che è realmente utile, senza dimenticare che gli aggressori possono utilizzare sistemi di IA e che questi sistemi devono essere protetti. Tra i benefici dell'IA, possiamo evidenziare:

Protezione dei dati aziendali, spesso bersaglio di spionaggio industriale.

Utilizzo di algoritmi e combinazione di diverse tecnologie, come intelligenza artificiale, machine learning e deep learning.

Individuazione di minacce e attività sospette all'interno della rete e protezione dei dati sensibili da intrusioni non autorizzate.

Tuttavia, scegliere la tecnologia più adatta può essere difficile per chi non ha l'esperienza necessaria; affidarsi agli esperti è quindi consigliabile per una scelta informata.
L'AI sta acquisendo sempre più rilevanza nel contesto delle misure di sicurezza informatica, soprattutto nell'identificazione delle minacce. I sistemi di sicurezza che incorporano l'AI contribuiscono a individuare più efficacemente la presenza di hacker o dei loro attacchi, migliorando notevolmente il tasso di rilevamento degli attacchi sulla rete e sui dispositivi endpoint IT, come smartphone, notebook, server e **Internet of Things.**

Le forme più avanzate di **apprendimento automatico**, come l'apprendimento supervisionato e non supervisionato, sono in grado di **differenziare file dannosi** da quelli sicuri e di **identificare** dati sospetti ed esaminarli. Il deep learning, una specializzazione dell'apprendimento automatico, utilizza reti neurali più complesse per elaborare i dati e può affrontare situazioni precedentemente sconosciute.

Le minacce emergenti per le reti informatiche protette dall'IA includono:
·**Malware** guidato dall'intelligenza artificiale, che imita il comportamento dell'utente.
·**Attacchi phishing** ad autoapprendimento, che utilizzano l'IA per adattare siti web, link o e-mail all'obiettivo di un attacco.
L'IA può essere impiegata come barriera protettiva, identificando i comportamenti degli attaccanti e dei loro software e adottando misure specifiche per contrastarli. Alcune applicazioni dell'IA nella sicurezza informatica includono:

- Rilevamento dei modelli per risparmio di tempo.
- Identificazione delle e-mail di spam.
- Autenticazione degli utenti autorizzati.
- Rilevamento del malware.
- Monitoraggio degli attaccanti tramite algoritmi.
- Decodificare l'identità degli attaccanti.

Tabella riepilogativa dei vantaggi e degli svantaggi dell'IA

Vantaggi	Svantaggi
Può elaborare un grande volume di dati	La raccolta di più dati comporta problemi di privacy e protezione
Automatizza la creazione di algoritmi per il rilevamento della sicurezza informatica	Gli hacker possono utilizzare l'IA per lanciare attacchi complessi e su larga scala
Le soluzioni di sicurezza informatica abilitate possono rilevare eventuali cambiamenti e eliminare i rischi	Può aiutare gli hacker a trovare e sfruttare efficacemente le vulnerabilità
Monitoraggio dell'infrastruttura tecnologica per rilevare entità malevole e tentativi di violazione della rete	Questi metodi potrebbero essere utilizzati da paesi e governi repressivi per rintracciare i loro avversari
Consente ai ricercatori di sicurezza informatica di lavorare allo sviluppo di algoritmi o all'esplorazione di minacce emergenti	Può essere utilizzato impropriamente per il monitoraggio della privacy personale, il tracciamento e altre violazioni

Evoluzione dell'Artificial Intelligence

Il volume di traffico di dati e la complessità delle minacce informatiche continuano a crescere esponenzialmente, rendendo sempre più difficile per gli esperti di sicurezza individuare e contrastare gli attacchi. Grazie all'implementazione dell'intelligenza artificiale e delle tecniche di apprendimento automatico, è possibile analizzare enormi quantità di dati e rilevare rapidamente le violazioni nei sistemi informatici, anche quando si manifestano in modi nuovi e imprevisti.

L'apprendimento automatico dell'IA **consente di migliorare costantemente la precisione degli algoritmi** utilizzati per individuare le minacce, affinando i modelli di apprendimento sulla base delle informazioni raccolte durante il monitoraggio delle attività sospette. Questo processo di adattamento e ottimizzazione continua rende gli strumenti basati sull'intelligenza artificiale sempre più efficienti nel riconoscere e prevenire gli attacchi informatici.

Tuttavia, è importante sottolineare che l'**intelligenza artificiale non sostituisce il ruolo degli esperti di sicurezza**, ma agisce come un complemento alle loro competenze, fornendo strumenti avanzati per rafforzare le difese informatiche e gestire meglio le minacce in un ambiente digitale sempre più complesso e mutevole.

"**Senza l'intelligenza umana l'AI non esiste**. L'intelligenza artificiale è computazionale, ed è finita. L'uomo ha un altro tipo di intelligenza, paragonabile all'infinito, e in questo senso l'uomo deve imparare a convivere con altri tipi di intelligenza. Solo attraverso questa collaborazione e all'unione tra discipline differenti si può generare vero valore per il futuro" Fabio Ferrari, Fondatore Ammagamma.

8.2 Piccole e Medie Imprese

8.2.1 Rapporto Swascan

Un recente rapporto mette in evidenza un dato allarmante: l'**84% delle aziende italiane**, che contano **meno di 1000 dipendenti**, è diventata un **bersaglio privilegiato** per gli attacchi di tipo ransomware, segnando una netta divergenza rispetto al trend dell'anno precedente. Era infatti usuale che le organizzazioni di dimensioni più ampie, dotate di maggiori risorse finanziarie e capaci di implementare robuste strategie di difesa informatica, venissero prese di mira. Questa svolta sottolinea l'urgente necessità di soluzioni di cybersecurity più efficaci, soprattutto per le piccole e medie imprese (PMI), che oggi sembrano più predisposte a cedere alle richieste di riscatto, proporzionali al loro fatturato.

La **predilezione** delle **gang di cybercriminali per le PMI** italiane può essere attribuita alla facilità con cui possono penetrare in questo settore. Le risorse limitate, le competenze tecniche insufficienti e la scarsa consapevolezza del personale rappresentano un'opportunità irresistibile per gli hacker malintenzionati.

Spesso, proprio queste aziende si trovano costrette a cedere al ricatto, poiché i loro sistemi di backup - l'ultimo baluardo per il recupero dei dati - sono configurati in modo non sicuro e quindi diventano essi stessi preda della crittografia.
Queste aziende, diventate completamente indifese, si vedono spesso obbligate a pagare il riscatto per poter ripristinare le operazioni aziendali, essendo un obiettivo molto facile e altamente remunerativo per i gruppi hacker.

Le **PMI non sono solo un'opportunità** economica a breve termine per queste gang. Le PMI italiane costituiscono una quota significativa del prodotto interno lordo del paese e rappresentano il nostro vantaggio competitivo. Il loro **know-how,** i loro **brevetti,** i loro **progetti** diventano spesso **il bottino** di ogni attacco informatico da ransomware, sono infatti esfiltrati dati e informazioni che potrebbero essere di interesse anche per un paese come la Russia, attualmente soggetto a un blocco completo delle importazioni.
Questo costituisce un ulteriore motivo di preoccupazione a livello nazionale. La perdita di questi dati comporta un danno competitivo a livello geopolitico nel medio e lungo termine.

E' quindi indispensabile fornire un sostegno concreto alle PMI. Il Piano Nazionale di Ripresa e Resilienza (PNRR) potrebbe rappresentare una soluzione, ma è altrettanto necessario agire a livello legislativo sulla questione del pagamento dei riscatti.

Un intervento in questa direzione potrebbe costituire un vero e proprio scudo di protezione per le nostre aziende, disincentivando gli attacchi legati al cybercrime e riducendo drasticamente la possibilità di ottenere un guadagno da attacchi informatici.

8.2.2 AGENDA DIGITALE

Nei primi giorni di febbraio, il Computer Security Incident Response Team (CSIRT) francese **segnala il propagarsi di una serie di operazioni malevole** che tentano di sfruttare **le vulnerabilità dei server VMware ESXi** riscontrate e segnalate anche in Italia nel febbraio 2021, quindi ormai due anni fa.

Ventiquattro ore più tardi l'Agenzia per la Cybersecurity Nazionale, attraverso lo CSIRT Italia, rilancia il medesimo alert alle aziende italiane che, nella quasi totalità dei casi, sono già al riparo da questo tipo di attività criminali, avendo applicato per tempo l'aggiornamento di sicurezza e tamponato la falla in questione.

Ma quali sono state le conseguenze nel concreto? L'operazione di hacking ha determinato la **contaminazione di 22 server** "scoperti" in Italia, sui quali si poggiano **circa 400 aziende**. In nessun caso noto, tuttavia, i software malevoli si sono attivati, bloccando i file e chiedendo il riscatto di **42mila euro per la loro "liberazione"**. Se si considera che ogni giorno in Italia assistiamo a circa 3 milioni di tentativi di infrazione, quella di questi giorni può essere derubricata come ordinaria amministrazione se la si legge dal punto di vista di chi si occupa quotidianamente di proteggere i processi e i dati in mano alle grandi aziende, pubbliche o private che siano, che gestiscono le infrastrutture e i servizi strategici del Paese: dall'energia, alla sanità, dalle infrastrutture alle telecomunicazioni.

8.2.2.1 Il cortocircuito mediatico intorno all'attacco

Eppure, questa volta è scattato un **meccanismo di rincorsa** alla notizia che ha fatto **deflagrare una bomba comunicativa** volta a presentare il nostro come un Paese sotto attacco cibernetico. Da più parti si è persino ipotizzato il coinvolgimento di Stati esteri, ma questa, come molte altre fughe in avanti sono state ridimensionate prima dagli esperti, sia in seconda battuta dal governo.
Da **questo cortocircuito mediatico e comunicativo**, tuttavia, qualcosa di buono è **scaturito**. In primo luogo, i media generalisti sono stati costretti ad approfondire **la tematica della cybersecurity**, offrendo ai cittadini comuni uno spaccato del mondo che noi viviamo quotidianamente.
Dall'altro ha costretto la politica ad analizzare il sistema attuale della difesa cibernetica del Paese e, si spera, a comprendere la necessità di un suo rafforzamento.

8.2.2.2 L'intervento tempestivo dell'ACN

Quotidianamente, infatti, i gruppi di cyber criminali sparsi in tutto il mondo si adoperano per scandagliare il web a caccia di sistemi informativi fallaci o comunque non perfettamente aggiornati. Altrettanto, ma con ben altri scopi, fa l'Agenzia per la Cybersecurity Nazionale (**ACN**) che **provvede** a **segnalare** tempestivamente alle aziende le eventuali **fragilità**, indicando i **rimedi**.
Una collaborazione tanto più efficace quanto rapide e puntuali sono le comunicazioni tra il "centro", l'ACN, e la periferia, le imprese.
L'avviso tempestivo permette anche a chi non aveva applicato la patch ai server VMware ESXi di intervenire e fare in modo che i software malevoli non si attivino e che nessun servizio o sistema risulti gravemente compromesso.

Questo **modus operandi** da parte del mondo istituzionale e produttivo del Paese lo abbiamo sviluppato negli ultimi due anni, da quando è nata l'Agenzia Nazionale e lo **stiamo migliorando giorno dopo giorno**.

Ad Aprile, ad esempio, è entrata in vigore la **nuova tassonomia che classifica gli incidenti** ai danni dei sistemi informativi delle imprese private e pubbliche, inserite nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), **imponendo a queste ultime di comunicarli alla stessa ACN entro 72 ore dall'evento**. Tutti tasselli che vanno a rafforzare la nostra rete di protezione.

8.2.2.3 Una rete di protezione che però deve essere ampliata

Il sistema produttivo italiano è composto da lunghe filiere integrate che spesso operano in veri e propri distretti. Filiere che comprendono grandi aziende, a volte persino quotate, ma anche piccole e medie imprese fornitrici di componenti o servizi. Realtà, **queste ultime, che oggi non sono tutte adeguatamente attrezzate** per rispondere a questo tipo di **minacce** e finiscono pertanto per rappresentare una **criticità nel sistema**.

I numeri sono tutt'altro che trascurabili. Secondo l'ultimo rapporto curato da Confindustria e Unicredit, sul **nostro territorio operano circa 160mila PMI, aziende italiane, che impiegano tra i 10 e i 249 dipendenti** e generano un valore aggiunto pari a 204 miliardi di euro l'anno.

A queste si aggiungono circa 90mila microimprese che operano in settori strategici dell'economia nazionale o si trovano all'interno di una filiera complessa nei comparti dell'energia, della logistica, della cooperazione internazionale. **Tutte realtà che oggi sono sprovviste per la quasi totalità di figure preposte alla predisposizione di piani di sicurezza contro le minacce cyber.**

Eppure, se consideriamo il modo con cui i gruppi criminali operano, monitorando il web palmo a palmo in cerca di spiragli nei quali infiltrarsi, comprendiamo come sia necessario alzare anche lì il livello di guardia.

Certo, dotarsi di un security manager per una piccola impresa diventa un costo, ma è un costo che si auto compensa

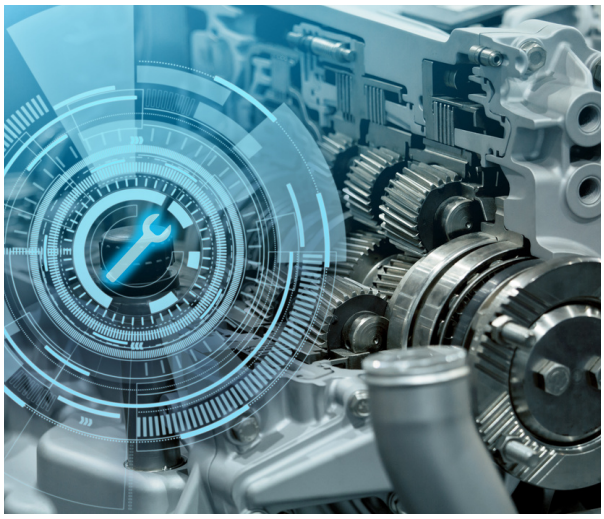
8.2.2.4 Sviluppi Futuri

Una **soluzione** potrebbe **arrivare**, in questo senso, dai **623 milioni di euro previsti dal PNRR** per finanziare il rafforzamento delle difese cyber. Anche se, di questi fondi, 301 milioni sono già destinati alla Pubblica amministrazione, mentre 150 milioni alle Istituzioni nazionali (Ministero degli Interni, Consiglio di Stato, ecc). **Prevedere**, però, una **linea di credito** che **consenta anche alle imprese private**, a **cominciare** da quelle **inserite nelle filiere strategiche**, di **consolidare le proprie difese cibernetiche**, sarebbe un'operazione lungimirante. Così come rendere obbligatoria, progressivamente, la presenza di un responsabile della security in azienda. Proprio come accade oggi per l'RSPP, il Responsabile del Servizio di Prevenzione e Protezione, il DPO, Data Protecion Officer o il Dirigente preposto alla certificazione dei bilanci.

Tutto questo nella consapevolezza che **il rischio zero non esiste, è un'utopia**. Ma, come diceva Eduardo Galeano: "L'utopia è là nell'orizzonte. Mi avvicino di due passi e lei si distanzia di due passi. Cammino 10 passi e l'orizzonte corre 10 passi. Per tanto che cammini non la raggiungerò mai. A che serve l'utopia? Serve per questo: perché io non smetta mai di camminare".

8.2.3 CYBERSECURITY 360

La **redditività media** degli **attacchi cyber**, dopo l'inizio della guerra si è **spostata verso le microimprese**. È un semplice fatto di evoluzione tecnologica del cyber crime: oggigiorno è conveniente attaccare le ME, per svariati motivi.



L'**automazione degli attacchi**, la relativa facilità con la quale questo tipo di vittime paga i riscatti, l'enorme valore dei loro dati, la facilità di incappare in brevetti non adeguatamente protetti e, non ultima, il **timore** diffuso nelle microimprese di **dover chiudere** l'attività a seguito di un **attacco cyber.**

Questi fattori vanno affiancati alla **migliore capacità di automatizzare gli attacchi altamente targettizzati**. Ad esempio, tramite tecniche di intelligenza artificiale, è già possibile automatizzare larga parte delle campagne di social engineering o di highly targeted o spear phishing

Ma non solo, la penetrazione nel tessuto sociale ed economico è anche una conseguenza della elevatissima redditività del crimine informatico, da quando è apparso il COVID: **molti micro-soggetti criminali sono interessati a questo tipo di attività,** come dimostrato dal recente vertiginoso incremento di attacchi in Italia spesso anche da parte di soggetti italiani.

Infine, occorre anche considerare la minaccia latente per le microimprese di finire invischiati in un attacco a qualche ente che ne gestisce i dati. Ne è un esempio il recentissimo presunto attacco all'Agenzia delle Entrate da parte di LockBit 3.0.

8. 3 Formazione e sensibilizzazione

"È come una trasformazione culturale"

Il **futuro della cybersecurity** si sta delineando con sempre maggiore chiarezza nel panorama mondiale, in quanto **le organizzazioni iniziano a guardare oltre le minacce**, piuttosto verso i potenziali impatti positivi che possono ottenere integrando in modo profondo il pensiero e le azioni relative alla sicurezza informatica nelle loro attività.

Alcuni dati significativi riguardano la sempre maggiore importanza che le tematiche relative alla cybersecurity stanno assumendo in azienda: secondo recenti studi condotti da varie aziende di consulenza **il 70% delle organizzazioni sentite ha riferito che le attività di individuazione delle minacce sono ordinarie durante le riunioni del proprio consiglio di amministrazione su base mensile o trimestrale.**

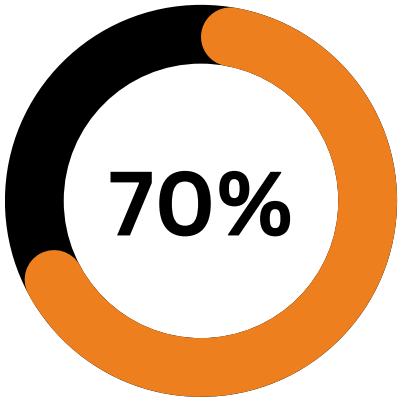
Infatti, la grande maggioranza degli intervistati ha individuato **un forte legame** tra il **cyber** e l'**impatto sul business**, con **l'86%** che ha dichiarato che **le iniziative cyber** hanno **contribuito** in modo significativo e positivo ad almeno una **priorità aziendale**. In base a questo dato, la maggior parte delle organizzazioni sta cercando di sfruttare questa proposta di valore, con il **58%** che **prevede di aumentare i propri investimenti informatici** nel prossimo anno.

Altri dati confermano ulteriormente questa tendenza in crescita, riguardante il grado di sensibilizzazione e diffusione dei principi di sicurezza informatica:

Entro il **2025, il 60% delle organizzazioni userà il profilo della sicurezza informatica** come fattore principale per valutare transazioni con terze parti e rapporti commerciali seguendo una tendenza che ha iniziato ad affermarsi qualche anno fa, quando le aziende più sensibili all'argomento hanno misurato il costo degli incidenti di cybersecurity.

Nel **2025, il 40% dei consigli direttivi delle aziende avrà un comitato dedicato alla cybersecurity** che risponderà direttamente a un membro del consiglio.

Entro il **2025, il 70% dei CEO svilupperà una cultura aziendale di resilienza per proteggere la propria organizzazione da cyberattacchi**, catastrofi metereologiche, eventi sociali e instabilità politica ed essere pronti ad affrontare le crisi improvvise.



Le aziende avranno quindi un ruolo sempre più attivo nella sensibilizzazione, ma alla fine la responsabilità ricadrà sull'utente finale, che dovrà imparare a utilizzare nuovi strumenti, rispettare norme di comportamento e proteggere i propri dati sia in azienda sia in casa.
La situazione paventata per il 2023 non era delle migliori. **Secondo i principali player** di mercato si **potrebbe creare** una voragine **tra le aziende attente alla cyber** - in grado di formare bene i dipendenti e dotarsi di tecnologie adeguate - e **le altre realtà, che potrebbero diventare facile preda dei cyber criminali** sempre più alla ricerca di soldi (e dati personali), anche per colpa della crisi economica, che sta spingendo diverse persone con competenze tecniche, soprattutto nei paesi poveri, a fare soldi sulla via del cyber crime.

Proprio perché gli **attacchi e truffe** si basano sempre più spesso su **tecniche** che sfruttano le debolezze del **fattore umano**, sono in grande ascesa tutte le iniziative mirate ad aumentare la consapevolezza e la formazione sul tema, necessaria anche da un punto di vista normativo con il costante aumento della pressione di compliance sui temi della cyber security, si pensi ad esempio all'impatto di NIS/NIS2 e PSNC, oltre ovviamente al GDPR.
Per tutti questi motivi, CE ed Enisa stanno definendo la necessità di prevedere l'inserimento di figure specializzate e piani di formazione.

È divenuta ormai **imprescindibile**, infatti, la necessità di dotarsi di piani di **formazione strutturata** per gestire la vulnerabilità derivante dal fattore umano con l'attivazione di iniziative di sensibilizzazione rivolte ai possibili impatti diretti e concreti cyber delle attività dei dipendenti, come confermano i seguenti dati:
le grandi organizzazioni in Italia si sono rese conto della necessità di introdurre iniziative di formazione (siamo al 99%), tra questi alcuni hanno un programma strutturato (80%), solo l'1% dichiara che non sono previste.

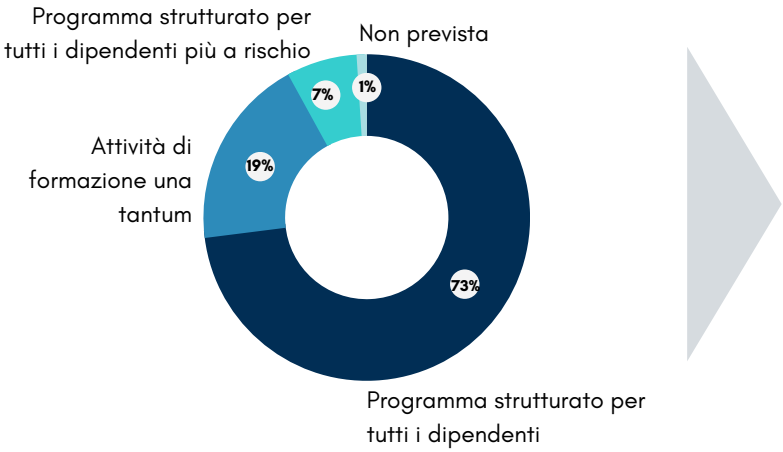


Figura 10 - Formazione Italia - Fonte: Osservatori.net 2023

LE PRINCIPALI INIZIATIVE DI FORMAZIONE

- Simulazione di attacchi phishing
- Programmi di lezioni interattive
- Piattaforme online di newsletter
- Eventi periodici dedicati

LE SFIDE DA AFFRONTARE

Valutazione dell'efficacia dei piani di formazione implementati
Gestione del budget e rotazione tra più funzioni aziendali

Le aziende cercano di dare un'impronta concreta a tali iniziative di formazione, ad esempio cercando di **ricreare uno scenario di attacco di phishing** e vedere la risposta dell'utente aziendale, oppure attraverso lezioni o eventi periodici dedicati interattivi per favorire il confronto sul tema e capire come la propria attività quotidiana potrebbe potenzialmente esporre l'azienda a un rischio cyber.
È fondamentale, infatti, non solo che tali iniziative vengano implementate, ma che siano soprattutto efficaci e valutabili attraverso specifiche metriche.
Questo richiede una stretta **collaborazione tra diverse funzioni aziendali,** in modo che, un tema di tale importanza, non venga affidato solo all'HR ma coinvolga anche la funzione cyber.

9. CONCLUSIONE

Negli ultimi anni, le minacce alla sicurezza informatica sono diventate sempre più sofisticate e le organizzazioni hanno faticato a tenere il passo. L'avvento delle nuove tecnologie ha reso più facile per i criminali informatici lanciare attacchi e rubare dati sensibili.
La rapidissima evoluzione delle minacce e dei rischi Cyber porta le aziende a dover affrontare nuove sfide, alcune di queste sono:

- ***Criminalità informatica***

La criminalità informatica è una minaccia crescente per le aziende di tutte le dimensioni. I criminali informatici stanno diventando sempre più sofisticati, rendendo difficile per le aziende tenere il passo con le ultime minacce.

- ***Mancanza di risorse***

Molte aziende non dispongono delle risorse e delle competenze necessarie per implementare misure di sicurezza informatica efficaci. Questo le mette a rischio di attacchi informatici e violazioni dei dati.

- ***Minacce interne***

Le minacce interne rappresentano un rischio significativo per le aziende. I dipendenti che hanno accesso a dati sensibili possono fare un uso improprio di queste informazioni, sia intenzionalmente che involontariamente.

- ***Conformità***

La conformità normativa è una sfida importante per le aziende. Il mancato rispetto delle normative può comportare multe salate e danni alla reputazione dell'azienda.
La sicurezza informatica spesso deve fronteggiare minacce che cambiano frequentemente e attacchi in sequenza questo causa un'enorme difficoltà nella pianificazione a lungo termine e negli investimenti in cybersecurity. Il risultato è una concentrazione sulla difesa tattica che può ostacolare lo sviluppo di una resilienza informatica a lungo termine.

10. BIBLIOGRAFIA

Visione globale vs Italia

1. Rapporto Clusit 2023

Visione Italia

1. Documento programmatico pluriennale per il triennio 2022-2024, Ministero della Difesa
2. Relazione annuale sulla politica dell'informazione per la sicurezza, Presidenza del Consiglio dei Ministri, 2022/2023
3. World Economic Forum Global Cybersecurity Outlook, 2023
4. Information security overview, Accenture, 2023

Resilienza Informatica

1. Assured Cyber Protection, DORA and NIS2 Factsheet, November 2022
2. Direttiva (UE) 2022/2555 (NIS2)
3. Digital Operational Resilience Act (DORA), REGOLAMENTO (UE) 2022/2554

Top IT priorities & Outlook

1. "State of the CIO Survey 2023" di IDG, Inc. company

Focus

1. Deloitte "Global Future of Cyber Survey", 2023
2. Previsioni di cybersecurity dell'azienda di consulenza e ricerca Gartner per il 2023-2025 e riportati dal sito pandasecurity.com, 2023
3. Sole24Ore: "Cybersecurity, come sarà il 2023? Le previsioni degli esperti", dicembre 2022

4. Giorgia Dragoni, “Le competenze della cybersecurity in Italia”, per il convegno “Verso un fronte comune”, dell’osservatorio cybersecurity & data protection, 2023
5. https://www.ai4business.it/intelligenza-artificiale/intelligenza-artificiale
6. https://cyberment.it/sicurezza-iot/il-ruolo-dellintelligenza-artificiale-nella-cybersecurity/#header1
7. https://www.cybersecitalia.events/event/crimes-on-the-network-new-investigative-approaches-and-methodologies-by-means-of-artificial-intelligence/https://www.cybersecitalia.events/event/crimes-on-the-network-new-investigative-approaches-and-methodologies-by-means-of-artificial-intelligence/
8. Wb-Cybersecurity-250123-sku-4003117.pdf, 2023
9. https://www.swascan.com/wp-content/uploads/2023/02/Ransomware-Q4-Final-1.pdf
10. https://www.agendadigitale.eu/sicurezza/attacchi-hacker-la-fragilita-arriva-dalle-pmi-cosi-il-pnrr-potrebbe-risolvere/
11. https://www.cybersecurity360.it/outlook/cyber-security-nelle-microimprese-perche-e-un-problema-e-come-mitigarlo/
12. https://www.cybersecurity360.it/nuove-minacce/information-war-e-cyberwar-caratteristiche-e-tipologie-degli-attacchi-informatici/
13. https://www.flaticon.com/

CONTATTI

Matteo M. Marzan
+39 348 9303095
matteo.marzan@planetica.it

Andrea Rivetti
+39 335 6516375
andrea.rivetti@planetica.it

Team di lavoro

Antonio Alfarano

Francesco Bonvicini

Alessandro Croce

Samantha Franceschin

Riccardo Mandiroli

Marco Nunzi

Per maggiori informazioni:
Tel: +39 02 82785 740 E-mail: segreteria@planetica.it Indirizzo: Via Crocefisso 5, Milano