Matricola s317814

POLITECNICO DI TORINO

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA GESTIONALE

Analisi del rischio cibernetico in Italia

Relatore:
Prof. Laura Abrardi

Presentata da:
Simone Parolin

Anno Accademico 2024/2025

Sommario

Introduzione

L'evoluzione della tecnologia digitale ha portato enormi benefici in termini di comunicazione, produttività e accesso alle informazioni, tuttavia, dall'avvento di Internet sono emerse minacce informatiche che mettono a repentaglio la sicurezza dei dati e dei sistemi informativi. Oggi gli attacchi degli hacker sono una delle principali sfide a livello globale, le aziende e i consumatori sono costantemente esposti a minacce informatiche sempre più sofisticate che possono causare danni economici, violazione della privacy e perdita di dati sensibili, questi attacchi non sono più un incidente isolato, ma un problema strutturale che riguarda settori strategici, organizzazioni pubbliche e private. Le infrastrutture critiche, i sistemi finanziari e le piattaforme digitali sono diventati obiettivi primari per gli hacker che utilizzano metodi sempre più sofisticati e automatizzati, la crescita dell'economia digitale ha ampliato la superficie di attacco e reso necessaria l'implementazione di strategie di difesa sempre più sofisticate.

In Italia, diversi fattori strutturali e comportamentali rendono aziende e consumatori particolarmente esposti a queste minacce, le imprese, soprattutto le PMI (Piccole Medie Imprese), devono affrontare sfide complesse per la protezione della loro infrastruttura digitale e sono spesso carenti in termini di difese informatiche avanzate, ciò è aggravato dall'errore umano, un fattore critico che può mettere a rischio anche i sistemi di sicurezza più solidi, la sensibilizzazione e la formazione svolgono quindi un ruolo centrale nel rafforzamento della resilienza organizzativa.

In questo contesto, il ruolo della regolamentazione diventa cruciale, la legislazione dovrebbe mirare a rafforzare gli standard della protezione dei dati e a promuovere una maggiore attenzione delle aziende e organizzazioni in materia di cybersicurezza.

La velocità con cui emergono le minacce significa che le strategie di difesa devono essere costantemente aggiornate e la consapevolezza di tutti gli interessati, l'introduzione di nuove tecnologie come l'intelligenza artificiale e il machine learning hanno trasformato il panorama della sicurezza informatica, consentendo di rilevare e prevenire gli attacchi in maniera rapida e in tempo reale. Tuttavia, anche i criminali informatici stanno sfruttando queste innovazioni per migliorare le loro capacità di attacco, creando una sorta di corsa agli armamenti digitali.

L'obiettivo di questa tesi è analizzare il contesto del rischio cibernetico in Italia, studiando le vulnerabilità esistenti, le motivazioni alla base degli attacchi e le strategie di mitigazione adottate dalle aziende.

Verrà dedicato un focus particolare sull'analisi dei modelli economici della cybersecurity per comprendere il mercato che caratterizza il rapporto tra imprese, consumatori e hacker, comprendere

le dinamiche economiche della sicurezza informatica è fondamentale per sviluppare strategie efficaci di protezione e mitigazione del rischio.

Questo approccio ci permetterà di esplorare le dinamiche della domanda e dell'offerta che caratterizzano la criminalità informatica e di identificare le migliori strategie di difesa per affrontare le sfide emergenti della sicurezza informatica, solo una combinazione di tecnologia avanzata, regolamentazione adeguata e consapevolezza degli utenti permetterà di creare un ecosistema digitale più sicuro e resiliente.

1. Il contesto del rischio cibernetico: Dalle origini agli scenari attuali

1.1 Evoluzione degli attacchi informatici

Il cybercrime, o crimine informatico, fa riferimento a qualunque attività illegale che coinvolge l'uso di tecnologie digitali come strumento o obiettivo, si tratta di una categoria ampia e in continua evoluzione, che comprende una varietà di reati volti a rubare dati, compromettere sistemi, causare danni economici o sfruttare le vulnerabilità tecnologiche per scopi illegali. L'evoluzione degli attacchi cibernetici segue di pari passo lo sviluppo tecnologico della società, negli ultimi anni, la criminalità informatica si è trasformata in un'industria multimiliardaria, facendo diventare la sicurezza informatica una delle principali preoccupazioni globali.

Questa crescita ha portato alla formazione di veri e propri ecosistemi criminali altamente organizzati, strutturati come aziende legittime, in grado di offrire servizi su richiesta, assistenza tecnica e persino un servizio clienti.

Con la proliferazione degli attori statali nella criminalità informatica, i cyberattacchi stanno diventando sempre più sofisticati, Hacker indipendenti e organizzazioni criminali agiscono con strategie mirate e lanciano attacchi sempre più critici contro aziende, istituzioni finanziarie e governi, tale scenario ha reso la sicurezza informatica una priorità per le aziende e le organizzazioni di tutto il mondo.

Sebbene il concetto di crimine informatico sia associato principalmente all'era di Internet, il primo attacco informatico registrato ha avuto luogo in Francia nel 1834, alla fine del 1700 lo Stato francese aveva creato una rete di telecomunicazioni a livello nazionale attraverso i telegrafi ottici, che consistevano in torri di segnalazione con bracci mobili che trasmettevano messaggi da località remote attraverso segnali visivi criptati. Due banchieri di Bordeaux, i fratelli François e Louis Blanc, trovarono il modo di utilizzare il sistema telegrafico per ottenere informazioni sulla borsa di Parigi prima dei loro concorrenti. Dei complici monitoravano i movimenti del mercato azionario e passavano le notizie a operatori del telegrafo corrotti, che a loro volta trasmettevano queste informazioni nascoste nella corrispondenza ufficiale intercettata dai fratelli Blanc, il sistema consentiva ai due fratelli di conoscere i movimenti del mercato azionario parigino in poche ore, mentre normalmente le Poste avrebbero impiegato cinque giorni con cavalli e carrozze, e permetteva loro di guadagnare investendo in anticipo.

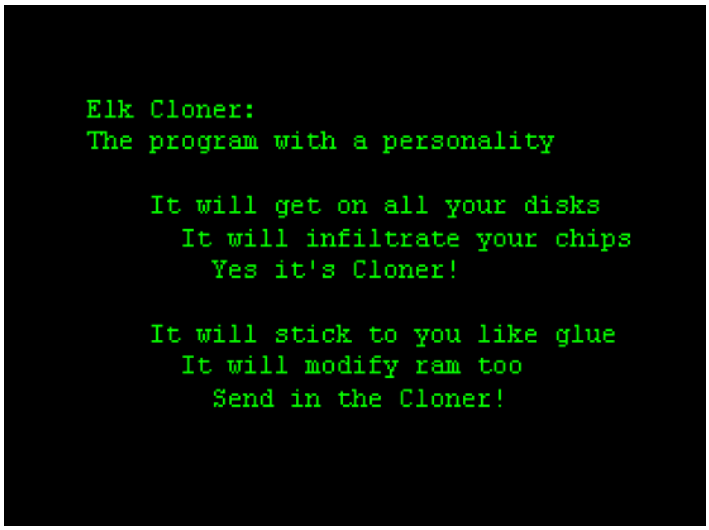
La frode fu scoperta due anni dopo e i fratelli Blanc furono perseguiti, ma non condannati perché la Francia non aveva ancora leggi contro l'uso improprio delle reti di dati.

Per arrivare al primo malware informatico dobbiamo andare avanti nel tempo di quasi due secoli, al 1971 con “Creeper”, scritto da Bob Thomas, un ingegnere che lavorava per la BBN Technologies (una delle aziende che ha contribuito alla creazione e allo sviluppo di ARPANET, la rete precedente a Internet), il programma non era destinato a causare danni, ma era un esperimento per dimostrare la possibilità di sviluppare un codice che potesse trasmettersi autonomamente tra computer connessi.
Infatti, Creeper si limitava a spostarsi da un computer a un altro senza danneggiare in alcun modo dati o il sistema, ma limitandosi a proiettare a schermo un messaggio che recitava:

(Figura 1 -output del primo malware creato)

(Fonte – https://www.historyofinformation.com/image.php?id=5351)

Questo messaggio, che invitava a prendere Creeper, era tutto ciò che l'utente vedeva sul proprio schermo prima che il programma si trasferisse su un altro dispositivo.
Sebbene questo codice fosse innocuo la sua creazione portò ad una nuova sfida, la sua rimozione dal sistema. Fu così che nel 1972 un altro ingegnere della stessa azienda, Raymond Samuel Tomlinson (inventore della chiocciola @ nelle e-mail), creò Reaper, un programma con il compito di individuare ed eliminare Creeper dai computer violati, diventando il primo software di sicurezza informatica della storia. All’interno del genere malware, che racchiude le varie categorie di programmi maligni, Creeper può essere definito un worm, un tipo di malware con l’abilità di autoreplicarsi.
Il primo virus informatico, che a differenza dei worm ha la capacità di infettare dei file per poter creare delle copie di sé, venne sviluppato una decina di anni dopo, nel 1982, da un quindicenne Richard Schernita. Il virus venne chiamato Elke Cloner ed aveva la capacità di infettare i sistemi Apple II, fu il primo malware a diffondersi in modo automatico attraverso i floppy disk. Quando un utente avviava un computer da un dischetto infetto, il virus si caricava automaticamente nella memoria del sistema e si trasferiva a qualsiasi altro floppy che veniva inserito nel drive.
Una volta attivato, Elke Cloner mostrava un messaggio sullo schermo dell’utente:



(Figura 2– messaggio mostrato dal virus Elk Cloner)

(Fonte - https://www.storiainformatica.it)

Il programma non era un virus distruttivo, tuttavia, rappresentava una nuova tipologia di minaccia, poiché si diffondeva senza il controllo dell'utente. Fino a quel momento, i problemi di sicurezza informatica riguardavano principalmente accessi non autorizzati ai sistemi o errori di programmazione, ma Elk Cloner dimostrò che il software poteva essere progettato per autoriprodursi e propagarsi autonomamente.

Il primo virus informatico ad ottenere fama globale venne creato nel 1986 da due fratelli pakistani, come punizione per chi duplicava illegalmente il loro software. Il virus si chiamava Brain, si diffuse a livello mondiale, e fu il primo caso di virus in grado di compromettere il boot sector del sistema operativo DOS, conteneva anche esso un messaggio nascosto e non corrompeva nessun dato.

Negli anni '90 e 2000, la diffusione di Internet permise ai virus di diffondersi in modo ancora più rapido, passando dai floppy disk alle e-mail e ai file scaricati dalla rete. Nel 1988 Robert Morris Jr. sviluppò un software, che divenne il primo *worm* a trasmettersi attraverso la rete internet, si diffuse rapidamente, replicandosi più volte e infettando circa il 10% dei computer connessi alla rete.

Oltre a propagarsi su nuovi dispositivi, il worm si duplicava ripetutamente anche su quelli già infetti, causando un consumo eccessivo di memoria e il blocco di numerosi PC. Considerato il primo attacco informatico su larga scala nella storia di Internet, l'incidente provocò danni, secondo alcune stime, in milioni di dollari e Robert Morris divenne il primo individuo condannato per frode informatica negli Stati Uniti. In risposta all'attacco venne fondato il CERT (Computer Emergency Response Team) per affrontare crisi analoghe in futuro e portando allo sviluppo di migliori tecnologie per identificare intrusioni nei sistemi informatici.

L'inizio del nuovo millennio si rivelò particolarmente difficile per gli addetti della sicurezza informatica. Nel 2000, Onel de Guzman, di origini filippine, sviluppò ILOVEYOU, questo virus, che

si diffondeva tramite allegati e-mail ingannevoli, è uno dei primi esempi di social engineering e phishing. Usando la psicologia per fare leva sulla curiosità delle persone, inducendole a scaricare allegati e-mail dannosi presentati sotto forma di lettere d'amore.

(Figura 3- messaggio mostrato dal virus ILOVEYOU)

(Fonte - https://www.corriere.it/tecnologia)

Il virus una volta entrato in un computer era in grado di inoltrare il messaggio a tutti gli indirizzi contenuti nella rubrica della vittima ed iniziava a compromettere il sistema, sovrascrivendo i file, rallentando le prestazioni fino a bloccare completamente i dispositivi e, sottraendo le password degli utenti. L'inganno funzionò su larga scala, penetrando anche nelle aziende e causando danni stimati intorno ai 10 miliardi di dollari. Tra le vittime ci furono persino il Pentagono, il Parlamento britannico e la NASA. In Italia, il virus colpì Telecom e il Ministero del Tesoro.

L'attacco era così una novità a livello globale che l'autore del malware fu rilasciato, poiché nelle Filippine non esistevano ancora leggi contro la cybercriminalità.

All'inizio del 2004 comparve un altro worm attraverso gli allegati della posta elettronica, chiamato Mydoom, sviluppato da autori sconosciuti, questo malware detiene il record di velocità di diffusione, arrivando, durante il suo picco, ad essere responsabile di un quarto di tutte le e-mail inviate a livello globale. Mydoom, oltre ad infettare i computer era in grado di lanciare attacchi Ddos (Distributed Denial of Service), che sono attacchi in grado di sovraccaricare un sistema interrompendo le sue funzioni, costringendo numerose aziende e istituzioni a fermare le loro operazioni, causando danni economici nell'intorno di 40 miliardi di dollari.

Pochi anni più tradi, nel 2007, emerse Zeus, un trojan, malware in grado di installarsi nel dispositivo dell'utente in grado di spiare o rendere accessibile a terzi il sistema. Zeus si infiltrava nei browser

delle vittime e registrava ogni informazione digitata, permettendo ai cybercriminali di accedere illegalmente a conti bancari, effettuando transazioni fraudolente per milioni di dollari.
CryptoLocker, comparso nel 2013, è stato tra i primi ransomware di grande impatto, malware in grado di bloccare l'accesso ai dati di un dispositivo criptandoli, gli hacker richiedevano un riscatto di due bitcoin, all'epoca circa 715 dollari, per restituire il controllo dei dati.
Nell'ultimo decennio invece, l'evoluzione della tecnologia informatica ha portato a una crescente dipendenza dai dispositivi digitali, trasformando i virus e i malware in strumenti di attacco strategici. Dal 2010 in poi, il concetto di cyberguerra ha assunto un ruolo centrale nella geopolitica globale, con governi e organizzazioni che utilizzano attacchi informatici per sabotare infrastrutture critiche e ottenere vantaggi economici e militari. Uno degli esempi più noti e rilevanti di questa nuova era è il caso del virus Stuxnet, questo malware, attribuito agli Stati Uniti e a Israele, aveva come obiettivo principale il programma nucleare iraniano, una volta infiltratosi nel sistema, il programma alterava il funzionamento delle centrifughe per l'arricchimento dell'uranio, danneggiandole senza che gli operatori si accorgessero immediatamente del problema. Stuxnet fu il primo esempio noto di un cyberattacco mirato contro un'infrastruttura critica, dimostrando che i virus potevano essere usati come vere e proprie armi di sabotaggio

1.2 Classificazione degli attacchi cibernetici

Per comprendere meglio il panorama delle minacce informatiche, possiamo classificare gli attacchi cibernetici in diverse categorie in base alla loro tecnica e agli obiettivi perseguiti.

1.2.1 Malware

I malware sono programmi o codici dannosi, progettati per compromettere la sicurezza di un sistema informatico arrecando danni o sottraendo informazioni.

Esistono diverse tipologie di malware, ognuno con funzionalità specifiche. Le tipologie più comuni sono le seguenti:

Worm

I worm sono programmi progettati per autoreplicarsi e propagarsi autonomamente attraverso reti e dispositivi, senza richiedere l'intervento diretto dell'utente. Si diffondono attraverso e-mail, reti locali, internet, dispositivi USB e altri vettori. Il più comune è la posta elettronica, spesso attraverso l'utilizzo della psicologia con metodi di social engineering per spingere i destinatari ad aprire gli allegati.

Virus

I virus, invece, si attaccano a file o programmi e si attivano solo quando vengono eseguiti. A differenza dei worm, i virus necessitano di un'azione dell'utente per entrare in funzione e propagarsi. Questa restrizione ha causato una riduzione del numero di virus in circolazione.

Ransomware

I ransomware sono una categoria di malware che crittografano i file presenti su un dispositivo bloccandone l'accesso e chiedono un pagamento (spesso in criptovaluta) per fornire la chiave di decrittazione. Le e-mail di phishing rappresentano il mezzo di diffusione più comune utilizzato dai ransomware, coinvolgendo oltre il 70% dei casi. Poiché gli algoritmi di crittografia moderni sono quasi impossibili da decifrare con la tecnologia attuale, l'unico metodo per recuperare i file cifrati è ripristinarli da un backup, oppure pagare la richiesta di riscatto.

Trojan Horse

Un trojan horse (cavallo di Troia) è un malware che si presenta come un software legittimo per indurre l'utente a installarlo. Una volta eseguito può effettuare attività dannose nel sistema senza che l'utente se ne accorga, come la sottrazione di dati, installazione di altri malware o l'accesso del sistema da parte dell'hacker. Questo tipo di malware non ha la capacità di replicarsi autonomamente. Tuttavia, i Worm vengono spesso utilizzati come mezzo per distribuire e installare i Trojan Horse sui sistemi.

Logic Bomb

Una Logic Bomb è programmata per attivarsi in risposta a condizioni specifiche, come una determinata data, un'azione dell'utente o un evento di sistema. A differenza di altri malware, rimane

inattiva fino al verificarsi della condizione predefinita aumentando le possibilità di infettare altri sistemi senza essere trovata.

Spyware e Keylogger

Gli spyware sono software che acquisiscono informazioni sugli utenti senza il loro consenso, come le credenziali di accesso e cronologia di navigazione, inviandoli agli hacker che potranno poi sfruttarli a loro vantaggio. I keylogger, in particolare, registrano ogni tasto premuto sulla tastiera, consentendo di sottrarre password e dati sensibili. Numerosi software open source disponibili su internet celano in realtà un malware di questo genere, il programma, non è realmente gratuito, ma il suo costo viene coperto dal valore dei dati presi dall'utente.

1.2.2 Social engineering

L'ingegneria sociale è una tecnica che manipola gli utenti per ottenere accesso a informazioni riservate. Gli attacchi di questo tipo si basano sull'inganno piuttosto che su vulnerabilità tecniche.

Phishing

Il phishing consiste nell'invio di messaggi fraudolenti che imitano comunicazioni ufficiali per ingannare l'utente e convincerlo a fornire credenziali di accesso, dati bancari o altre informazioni personali. I principali metodi di diffusione sono attraverso e-mail, siti web fasulli e messaggi SMS. Il phishing rappresenta un rischio rilevante poiché sfrutta l'inganno umano anziché falle nei sistemi informatici. Gli aggressori non hanno bisogno di forzare direttamente le difese o aggirare le misure di sicurezza. Possono semplicemente manipolare gli utenti con accesso legittimo agli obiettivi desiderati, come denaro o dati sensibili, inducendoli inconsapevolmente a compromettere la propria sicurezza.

1.2.3 DDoS

Gli attacchi Distributed Denial of Service (DDoS) hanno l'obiettivo di sovraccaricare le risorse di un server, una piattaforma digitale o un servizio online, causandone l'interruzione delle funzioni, rendendolo inutilizzabile per gli utenti. Questo viene realizzato inviando un'enorme quantità di richieste simultanee da più dispositivi compromessi, spesso facenti parte di una botnet, una rete di terminali infettati da malware e controllati da hacker. Gli utenti spesso non si accorgono che il proprio dispositivo fa parte di una botnet. Questa strategia è ampiamente utilizzata anche per l'elevata possibilità di riuscita: attacchi lanciati da numerose sorgenti distribuite rendono questa tipologia di offensiva particolarmente efficiente e complessa da individuare.

1.2.4 Attacchi a Vulnerabilità di Sistema

Gli attacchi a vulnerabilità di sistema sono intrusioni informatiche che sfruttano punti deboli o falle di sicurezza presenti in software, hardware, reti o configurazioni di sistema. Gli hacker identificano queste vulnerabilità per eseguire azioni dannose, come ottenere accesso non autorizzato, rubare dati, installare malware o compromettere il funzionamento del sistema.

Zero-Day Exploit

Un attacco zero-day sfrutta una vulnerabilità del software ancora sconosciuta. Il termine “zero-day" si riferisce al fatto che gli sviluppatori hanno zero giorni di tempo per risolvere il problema prima che venga sfruttato da cybercriminali. Questi attacchi sono particolarmente pericolosi perché non esistono difese immediate, le vulnerabilità della sicurezza a volte vengono scoperte dopo diverso tempo, durante il quale gli exploit trovati dagli hacker possono essere messi in vendita nel dark web.

SQL Injection

L'SQL Injection è una vulnerabilità di sicurezza che consente a un attaccante di manipolare le query SQL di un'applicazione web per ottenere accesso non autorizzato a un database, alterare o cancellare dati e, in alcuni casi, prendere il controllo del sistema. Questa tecnica sfrutta falle nei moduli di input per eseguire comandi dannosi all’insaputa dell’utente.

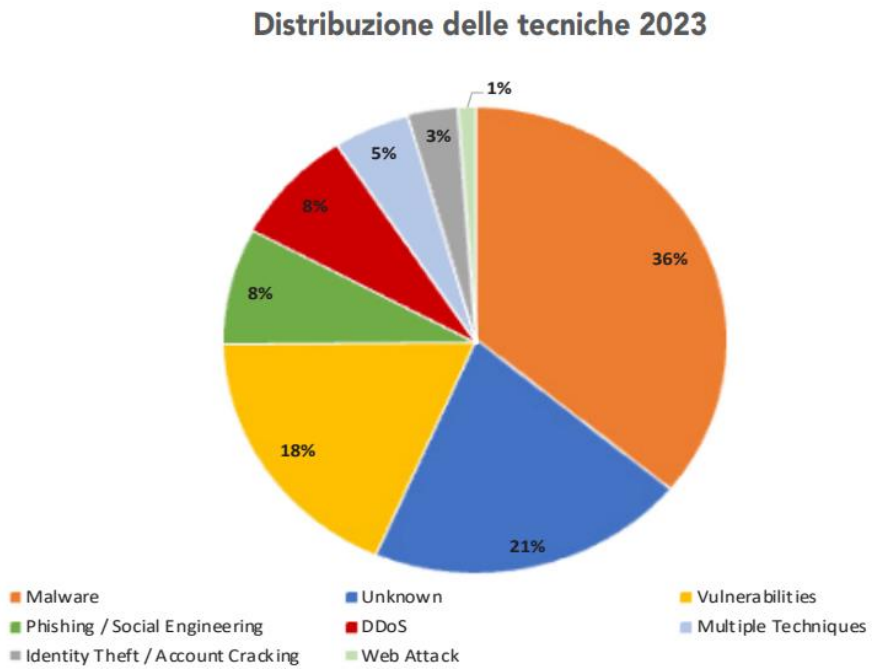
Man-in-the-Middle (MitM)

Man-in-the-Middle è una tecnica in cui un hacker intercetta e manipola le comunicazioni tra due parti per rubare dati sensibili o alterare il contenuto del messaggio. I criminali informatici agiscono come intermediari tra chi invia le informazioni e chi le riceve. Questi attacchi sono comuni nelle reti Wi-Fi pubbliche non protette dove chiunque può accedervi.

Sniffing

Lo sniffing è un attacco passivo, utilizzando software specializzati i criminali hanno la capacità di infiltrarsi in una rete per catturare e analizzare il traffico di dati, tra cui utenze e password non protette. A differenza della tecnica Man-in-the-Middle non ci sono interferenze con la comunicazione.

Dal rapporto clusit sulla sicurezza informatica si possono studiare le distribuzioni delle tecniche di attacco.

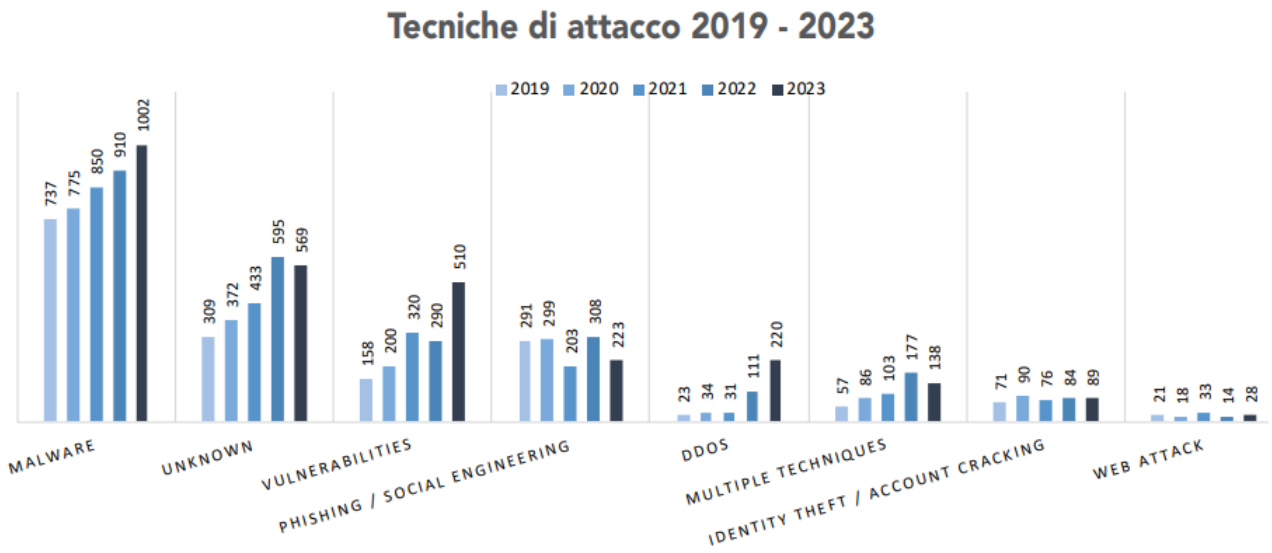


(Figura 4– distribuzione delle tecniche di attacco 2023)

(Fonte – Clusit)

Nel 2023, i criminali informatici continuano a fare largo uso di malware, impiegato in circa il 36% degli attacchi. Questa categoria come visto precedentemente racchiude numerosi tipi di software dannosi. Al secondo posto si collocano le tecniche sconosciute, per le quali non sono disponibili dettagli pubblici su come siano state messe in atto. Infine, a concludere il podio, il ricorso alle vulnerabilità dei sistemi, che possono essere sia conosciute sia sconosciute.

Se si confrontano i dati del quinquennio 2019-2023 (Fig. 5), si nota che il trend degli attacchi è in costante crescita per quasi tutte le tipologie di attacco, tranne che per gli attacchi di Phishing / Social Engineering hanno una diminuzione di circa il 30% con un andamento altalenante nei 5 anni, anche gli attacchi sconosciuti sono in leggera diminuzione dopo una crescita continua. I malware è l'unica tipologia di aggressione che non ha mai subito cali, con un aumento del 35% nel quinquennio. L'aumento più grande è stato fatto dai Ddos e dalle vulnerabilità, che sono praticamente raddoppiati nell'ultimo periodo.



(Figura 5– distribuzione tecniche di attacco nel periodo 2019-2023)

(Fonte – Clusit)

1.3 Le motivazioni degli hacker

Nella percezione comune, il termine hacker è spesso associato a una connotazione negativa, come la definizione di pirata informatico. Tuttavia, l'origine del termine è ben diversa, andando indietro nel tempo, scopriamo che già nel XIII secolo la parola *hacker* veniva usata come soprannome per indicare taglialegna o persone che costruivano strumenti da taglio. Con il passare dei secoli, il termine ha subito un'evoluzione fino ad arrivare al mondo digitale.

La storia moderna dell'hacking prende forma nei primi anni Sessanta al Massachusetts Institute of Technology (MIT) di Cambridge, inizialmente, il termine aveva un'accezione del tutto positiva e veniva utilizzato per descrivere individui con straordinarie competenze informatiche, capaci di potenziare e ampliare le funzionalità dei programmi oltre i limiti previsti dalla loro progettazione.

Tra gli anni Ottanta e Novanta, con la diffusione dei computer e di internet al pubblico gli hacker cominciarono a sfruttare le proprie abilità per scopi di lucro personali ai danni della comunità. Fu proprio la comparsa di questi cybercriminali che iniziò il graduale cambiamento del termine hacker da positivo a negativo.

Successivamente, gli stessi hacker cercarono di prendere le distanze criminali della loro comunità, portando ad una divisione di categoria.

-Gli **Hackers** etici (white hat o cappello bianco), sono esperti di informatica e programmazione che utilizzano le loro competenze per sviluppare nuovi software, migliorare sistemi esistenti o individuare vulnerabilità nei programmi, segnalandole ai proprietari. In molti casi, il loro operato ha un valore sociale significativo, poiché contribuiscono a rendere le applicazioni e le infrastrutture informatiche più sicure e resistenti agli attacchi.

-I **Cracker** (Black Hat o cappello nero), che deriva dal verbo "to crack" col significato di "distruggere", sfruttano le loro competenze informatiche per scopi illegali o dannosi. Il loro obiettivo principale è eludere le restrizioni imposte dai sistemi di sicurezza, ma a differenza dei White Hat, non agiscono per segnalare vulnerabilità, ma operano per ottenere un ritorno economico personale.

Per lo stato italiano però, in caso di violazione di un sistema informatico senza autorizzazione, sia i White e i Black Hat infrangono la legge, infatti, nella legislazione italiana non esiste questa distinzione, queste due figure sono entrambe colpevoli. In altre legislazioni invece, come ad esempio negli Stati Uniti, solo se vengono causati danni economici o commessi comportamenti penalmente perseguibili l'intrusione in un sistema informatico viene sanzionata. Ad oggi il termine Hacker viene

utilizzato universalmente per definire qualunque soggetto che compie un'azione illecita realizzata tramite strumenti digitali.

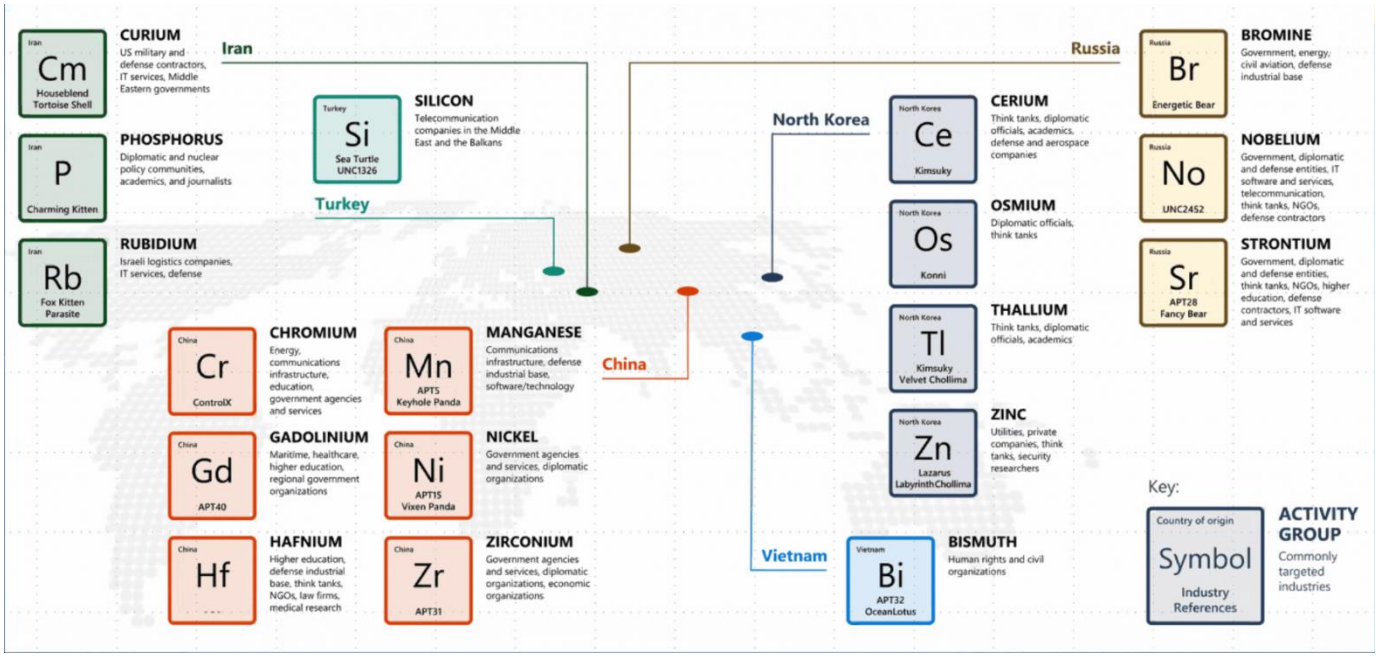
Il motivo più comuni dietro gli attacchi informatici è il guadagno economico. I cybercriminali sfruttano vulnerabilità nei sistemi per commettere truffe, rubare dati, estorcere denaro o vendere informazioni sensibili sul mercato nero. Il criminale informatico negli anni si è evoluto, formando gruppi organizzati che agiscono come aziende multinazionali ottenendo fatturati miliardari.

Spesso questi gruppi hacker sono sponsorizzati direttamente dagli stati, unendo motivazioni economiche a quelle politiche e di spionaggio. Questa situazione richiama le "lettere di corsa" concesse dai governi europei ai corsari tra il XVII e XVIII secolo. Uno dei vantaggi del cyberwarfare è la facilità di nascondere le proprie tracce da parte dell'attaccante, aumentando le difficoltà nell'attribuire l'origine e responsabilità dell'attacco. Nel summit Nato del luglio del 2016 il cyberspazio è stato aggiunto come dominio di guerra dopo aria, terra, mare e spazio.

Il conflitto militare tra Russia e Ucraina scoppiato nel febbraio del 2022 è l'esempio su come la guerra non si combatte solo sui campi di battaglia, ma anche nel cyberspazio. Tra il 2015-2016 c'è stato un grave attacco al settore energetico ucraino lasciando senza corrente centinaia di migliaia di persone, il giorno stesso dell'invasione, le emittenti televisive ucraine sono state colpite, sottraendo dati sensibili e bloccando le trasmissioni, nel tentativo di silenziare le notizie sull'offensiva russa. La risposta ucraina non si è fatta attendere, con operazioni di hacking contro siti governativi e aziende russe.

Uno dei metodi di identificare l'origine delle principali organizzazioni cybercriminali è quello di associare ai gruppi di una nazione il nome di un animale: per la Russia i Bear (orso), i Panda per la Cina, L'Iran i Kitten (gattino) ed infine i Cobra per la Corea del Nord.

Microsoft invece, classifica i gruppi sostenuti da stati utilizzando la tavola periodica degli elementi, come mostrato nell'immagine sottostante, a ciascun gruppo viene assegnato il nome di un elemento chimico, includendo anche le altre denominazioni attribuite da analisti della sicurezza.



(Figura 6- principali gruppi cybercriminali state-sponsored)

(Fonte - Microsoft)

Il maggior numero di attacchi informatici da gruppi finanziati dal governo proviene dalla Russia, tra i gruppi hacker più famosi è presente *Fancy Bear* (Strontium), con possibili legami con i servizi segreti militari russi del GRU. Uno degli attacchi più noti attribuitegli è stato l'infiltrazione nel 2016 nei sistemi informatici del partito Democratico degli Stati Uniti e della campagna di Hillary Clinton, evento che si ipotizza abbia influenzato l'esito delle elezioni presidenziali statunitensi.

Nella Repubblica Popolare Cinese è presente *Hafnium*, le sue operazioni sono rivolte principalmente a entità negli Stati Uniti, colpendo vari settori industriali. È considerato il responsabile dell'attacco ai server di Microsoft Exchange avvenuto nel 2021, e che ha avuto un impatto su oltre 30 000 organizzazioni negli Stati Uniti e altre diverse decine di migliaia in tutto il mondo.

Nonostante l'arretratezza tecnologica e l'isolamento internazionale la Corea del Nord ha costruito una delle cyber-force più sofisticate al mondo, tra le organizzazioni è presente *Lazarus Group* (Zinc), finanziato e controllato dal governo nordcoreano, a differenza di altri gruppi state-sponsored Lazarus è principalmente impegnato in attività cybercriminali finalizzate alla raccolta di fondi illeciti per sostenere il regime ed eludere le sanzioni internazionali, tra i suoi attacchi informatici più famosi ci sono il furto informatico più grande della storia, in cui sono stati sottratti 82 milioni di dollari alla Banca Centrale del Bangladesh nel 2016 e l'attacco a Sony Pictures Entertainment (2014), un attacco devastante che ha compromesso i server della compagnia, diffuso dati sensibili e cancellato file

interni, in risposta alla produzione del film satirico *The Interview*, che prendeva di mira il regime nordcoreano.

Un'altra faccia del mondo hacker è rappresentata dagli hacktivisti (combinazione tra le parole "hack" e "attivismo"), ossia individui o gruppi che impiegano tecniche di hacking per sostenere cause politiche o sociali, spesso contro organizzazioni o governi che considerano repressive o ingiuste.

Sia i comuni hacker che gli hacktivisti sfruttano gli stessi exploit e cercano le stesse vulnerabilità, ma mentre gli hacktivisti tendono a colpire un'azienda, un governo o un'istituzione specifica per manifestare il loro dissenso, gli hacker esaminano ampie sezioni della rete senza un obiettivo definito, sperando di trovare falle nella sicurezza. Sebbene le loro attività possano essere considerate illegali, gli hacktivisti si ritengono come difensori della libertà di espressione e oppositori dei regimi autoritari.

Tra gli esempi più noti di hacktivisti figurano le operazioni condotte da Anonymous, il cui motto è:

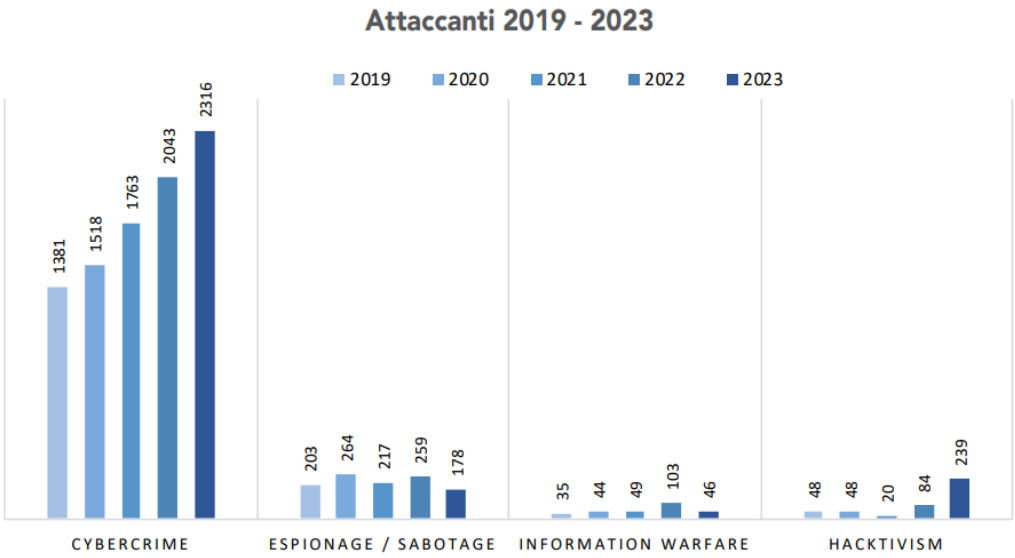
"We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

Il gruppo è responsabile di attacchi ad organizzazioni come Scientology, ISIS e vari governi, tra cui quello russo dopo l'invasione dell'Ucraina, protestando contro la censura, la corruzione e altre problematiche sociali.

Un ulteriore caso di interesse è WikiLeaks, una piattaforma che pubblica documenti riservati che denunciano operazioni governative segrete e abusi di potere, fondata da Julian Assange, WikiLeaks mira a promuovere la trasparenza e la libertà di informazione e fornisce una piattaforma sicura per gli informatori che vogliono denunciare crimini, corruzione e abusi di potere.

Tra i documenti pubblicati ci sono quelli relativi a Guantanamo Bay, che rivelano il trattamento disumano dei detenuti. L'impatto dell'hacktivismo è oggetto di dibattito controverso, da un lato, queste azioni possono sensibilizzare le persone e stimolare il dibattito su questioni importanti, dall'altro, sollevano dubbi etici e legali, soprattutto se comportano la violazione della privacy o danneggiano soggetti estranei all'obiettivo prefissato.

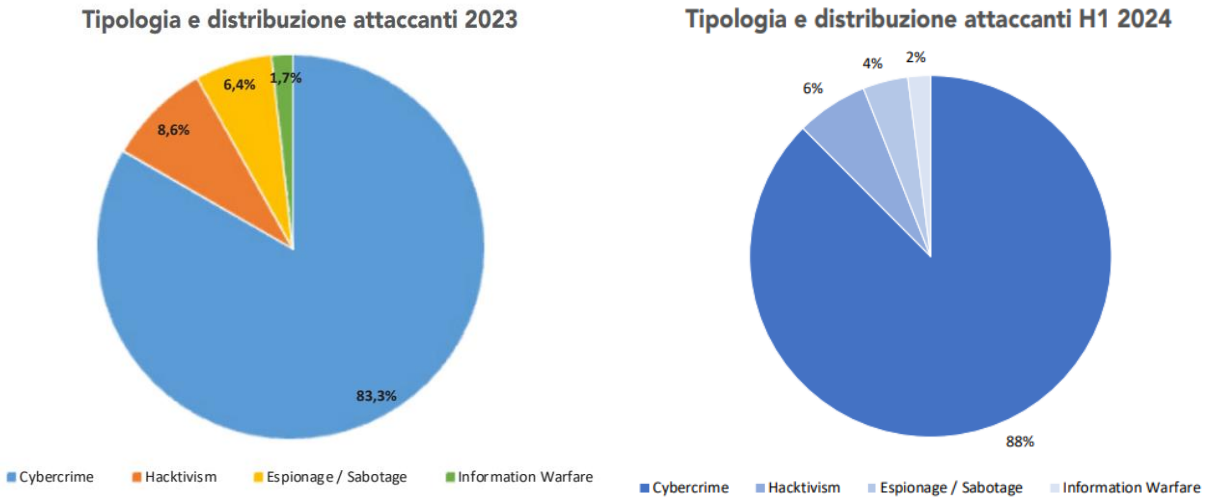
Dal rapporto Clusit sulla sicurezza informatica viene mostrato in modo evidente che il cybercrime è la motivazione principale degli attaccanti.



(Figura 7– distribuzione aggressori dal 2019 al 2023)

(Fonte - Clusit)

Invece i fenomeni di spionaggio informatico (Espionage) e guerra dell'informazione (Information Warfare), dopo il picco raggiunto con lo scoppio della guerra in Ucraina, registrano un calo significativo tra il 2022 e il 2023, gli attacchi legati all'hacktivismo mostrano un aumento di quasi il triplo, questa impennata di attacchi è anche dovuta in risposta all'invasione in Ucraina della Russia.



(Figura 8– Distribuzione percentuale degli aggressori nel 2023 e H1 2024)

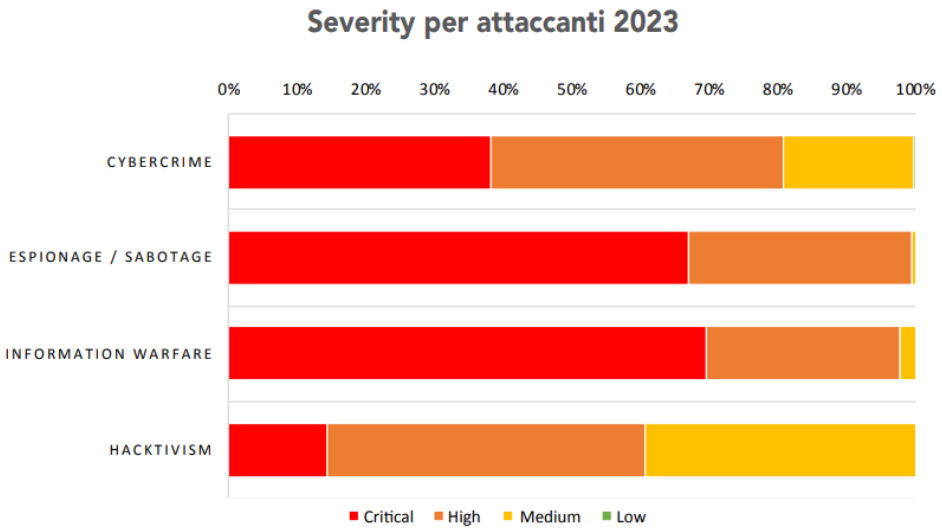
(Fonte - Clusit)

L'aumento del numero di incidenti è alimentato principalmente dalla crescita del Cybercrime, che rappresenta l'88% del totale (con un incremento di oltre 5 punti percentuali rispetto al 2023),

evidenziando come grazie alla digitalizzazione e al grande valore delle informazioni custodite nei sistemi informativi, il crimine informatico sia sempre di maggior interesse per le organizzazioni criminali. Il fenomeno di espionage/sabotage continua la sua flessione, registrando un calo di oltre 2 punti percentuali rispetto al 2023, confermando la tendenza già osservata l'anno precedente. Anche l'Hacktivism, dopo aver registrato un'impennata nel 2023, mostra una contrazione nei primi sei mesi del nuovo anno di circa 3 punti percentuali.

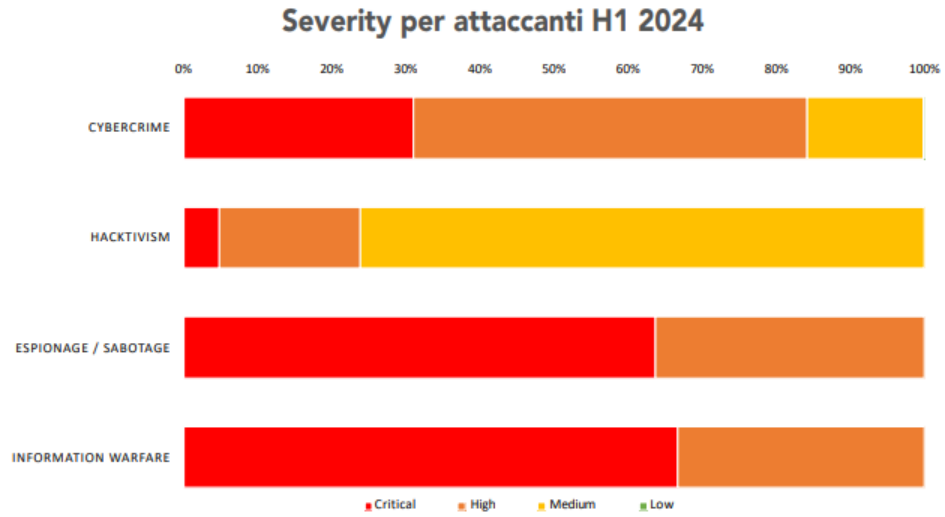
Severity degli attacchi

Non tutti gli attacchi hanno lo stesso effetto, l'analisi della gravità (severity) degli incidenti valuta l'effettivo impatto degli attaccanti, con una scala che varia da low fino a critical.



(Figura 9– distribuzione gravità attacchi 2023)

(Fonte - Clusit)



(Figura 10– distribuzione gravità attacchi H1 2024)

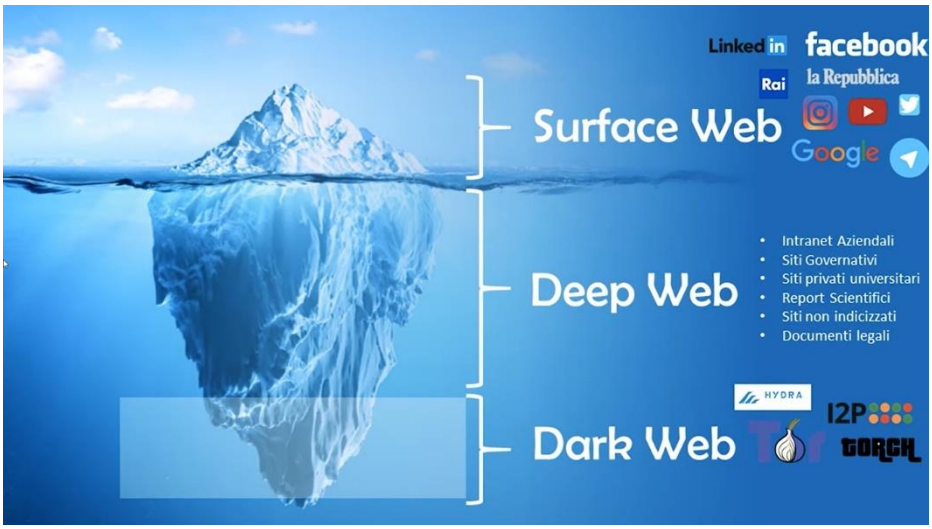
(Fonte - Clusit)

Per quanto riguarda la gravità degli incidenti in relazione alla tipologia di attaccante, nel primo semestre del 2024 (Fig. 10), dal rapporto Clusit, le distribuzioni risultano, nella maggior parte dei casi, quasi identiche a quelle osservate nel 2023. Gli attacchi a basso impatto di fatto svaniscono, risulta anche chiaro che gli attacchi legati a Espionage e Information Warfare vengono pianificati ed attuati con l'obiettivo di massimizzare il successo e il danno dell'aggressione digitale. Infatti, nessuna di queste due tipologie ha una gravità inferiore ad alta.

1.4 Il ruolo del dark web nel favorire gli attacchi informatici

Il Dark Web rappresenta una porzione sommersa di Internet, accessibile solamente tramite software specifici (come la rete Tor o I2P) e configurazioni di sicurezza avanzate che consentono la navigazione anonima. L'anonimato offerto da queste piattaforme non è di per sè un fenomeno negativo: in contesti di forte censura governativa o in situazioni di rischio per l'incolumità personale, esso diventa un importante strumento di protezione per giornalisti, dissidenti politici e minoranze. D'altro canto, le stesse caratteristiche che salvaguardano la libertà di espressione forniscono terreno fertile per attività criminali di vario genere, compreso il cybercrimine.

La storia del Dark Web è strettamente legata allo sviluppo di tecnologie per la tutela dell'anonimato e, più in generale, alla nascita di protocolli che permettono di celare l'identità e la posizione geografica di chi invia e riceve informazioni su Internet.
La tecnologia dell'onion routing, elemento centrale che permette a Tor di mantenere l'anonimato dei suoi utenti, fu ideata e finanziata nella seconda metà degli anni Novanta dal governo federale degli Stati Uniti. All'epoca, la rete Onion era destinata a proteggere gli operatori dell'intelligence e a consentire loro comunicazioni sicure e non rintracciabili. Successivamente la rete venne rilasciata pubblicamente, ed ebbe un ruolo importante nel proteggere i sostenitori della democrazia negli stati autoritari.
Il termine "Darknet" risale invece ai primi anni di Arpanet (precursore di internet), e identificava quelle reti parallele rispetto a quella principale, che sfuggivano all'indicizzazione da parte dei motori di ricerca, rimanendo così nascoste e non accessibili al grande pubblico.
Per comprendere meglio la struttura di Internet, spesso la si paragona a un iceberg composto da tre livelli di profondità



(Figura 11– struttura ad iceberg di internet)

(Fonte - https://www.cybersecurity360.it)

- 1 livello - Il **Surface Web** (o Clear Web), cioè la parte visibile e indicizzata, accessibile a tutti tramite i motori di ricerca (social network, siti web di notizie, e-commerce e così via).

- 2 livello - Il **Deep Web**, un insieme di risorse non indicizzate e quindi non raggiungibili in maniera diretta, quali intranet privati aziendali ed accademici o pagine web recenti non ancora scansionati.

- 3 livello – Il **Dark Web** (o Darknet), ovvero il livello più nascosto, al quale non si può accedere con un browser tradizionale. Per entrare in questo strato servono software specifici come l'Onion routing di Tor, oppure altri sistemi, per esempio I2P o Freenet.

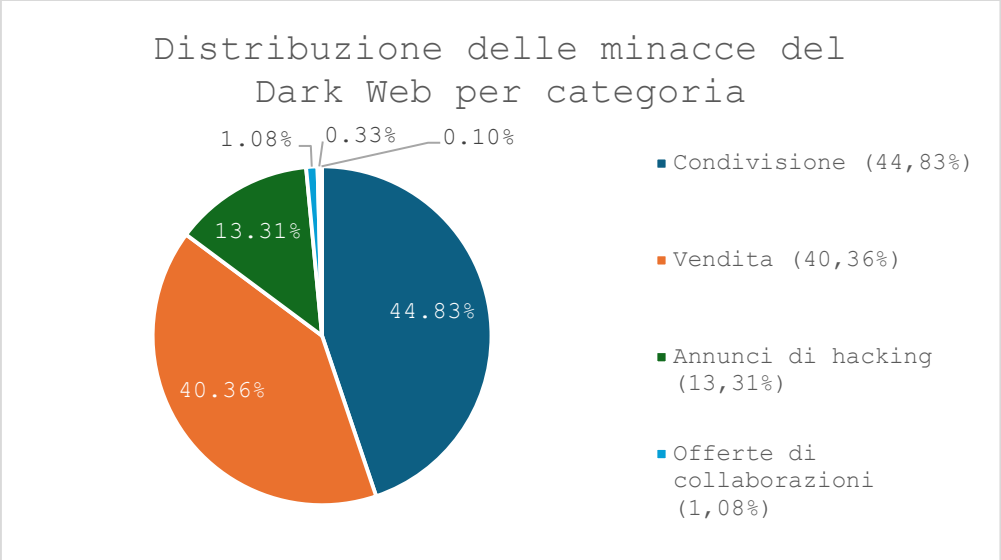
Secondo alcune stime di esperti, il Surface Web costituisce solo una piccola parte della rete, circa il 5%, mentre per il resto è composta dal Deep Web, di cui il Darknet è una porzione minore.
Sul Dark Web operano vere e proprie piattaforme di e-commerce, spesso strutturate in modo simile ai normali siti di compravendita online. Al posto dei prodotti legittimi, però, vi si trovano tool di hacking, malware personalizzato, exploit per vulnerabilità zero-day e altri strumenti utili a perpetrare attacchi informatici. Uno degli esempi più famosi è quello di Silk Road, la cosiddetta "Via della seta", si trattava di un vero e proprio mercato virtuale dove gli utenti potevano acquistare droghe, armi (sia convenzionali sia informatiche), documenti falsi, medicinali e sostanze stupefacenti, tutte organizzate in categorie ben definite. Dopo un paio di anni dalla sua creazione l'FBI riuscì a chiuderlo, sequestrando i server e arrestando il presunto fondatore, Ross Ulbricht, con una stima di più di un

miliardo di dollari scambiati sulla piattaforma. La chiusura di Silk Road non mise fine ai mercati virtuali illegali, sul Dark Web presero rapidamente piede altri marketplace dalle caratteristiche analoghe, colmando il vuoto lasciato.

Per effettuare i pagamenti e le transazioni le criptovalute svolgono un ruolo cruciale nel Dark Web, poiché semplificano le transazioni anonime. Pur essendo registrate su una blockchain, queste transazioni non rivelano l'identità reale di chi le effettua, agevolando i criminali informatici che intendono operare nell'ombra. Un altro aspetto rilevante è la loro natura decentralizzata, che elimina la necessità di intermediari o autorità centrali e riduce sensibilmente la possibilità di congelare i fondi nel momento in cui dovessero emergere attività illecite. Inoltre, la rapidità di conversione offerta dalle piattaforme di scambio permette di trasformare le criptomonete in valute legali (o in altre criptovalute) con un semplice click, rendendo estremamente complesso il lavoro delle forze dell'ordine. Infine, la forte richiesta di queste valute digitali all'interno dei marketplace clandestini, dove spesso sono l'unico metodo di pagamento accettato, ha creato un vero e proprio ecosistema economico parallelo che alimenta e sostiene gran parte delle attività criminali online.

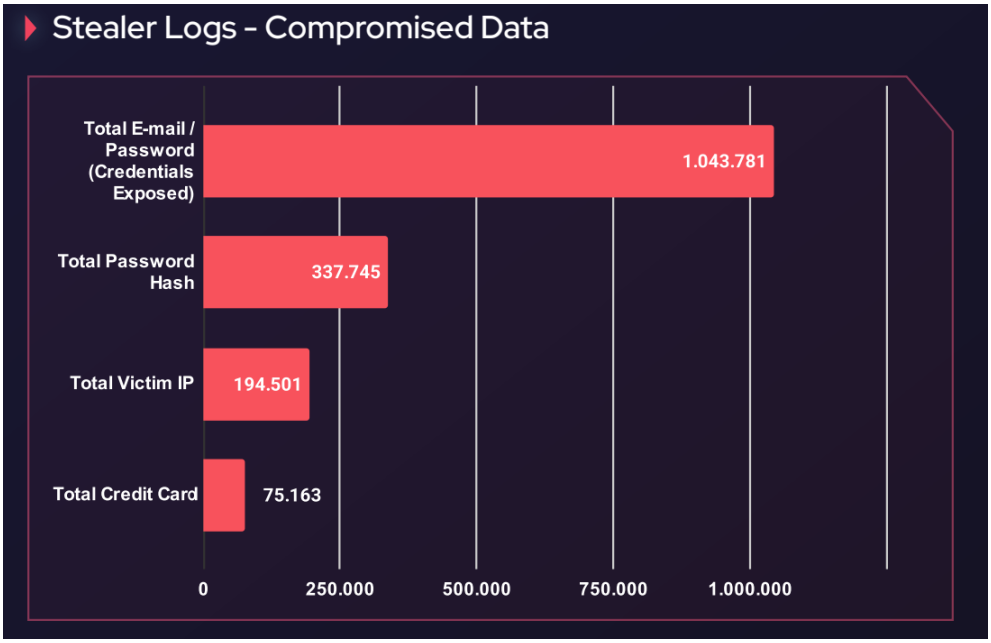
In passato si riteneva che Bitcoin fosse del tutto impossibile da tracciare, ma oggi sono noti metodi di investigazione che ne rivelano i passaggi. Per questo i criminali stanno migrando verso monete digitali più difficilmente tracciabili, come Monero, rendendo ancora più complesse le attività di contrasto delle forze dell'ordine.

Dal report annuale sul Dark Web stilato dalla piattaforma di Cyber Security Socradar, gli Stati Uniti è stato il paese più colpito dalle minacce del Darknet con quasi il 20% dei post nei forum mirati contro di esso, l'India è stata la seconda nazione con una percentuale del 8,5% seguita dal Regno Unito al 4%, l'Italia rimane fuori dalla top 10 con meno del 2%. Le principali categorie di minacce invece sono le seguenti.



(Grafico 1- Distribuzione delle minacce del Dark Web per categoria)

La condivisione gratuita di dati e strumenti illeciti è l'attività più diffusa, indicando che molti cybercriminali pubblicano risorse per attirare nuovi membri o per aumentare la loro reputazione nella comunità hacker. L'altra categoria più importante è la vendita di servizi o prodotti illegali, sulla quale si basa la maggior parte dei ricavi del Dark Web, gli annunci di hacking sono l'ultima categoria con una percentuale significativa, sono informazioni su attacchi informatici, violazioni di dati o nuovi strumenti di hacking. L'acquisto e gli attacchi mirati hanno una presenza molto ridotta nei forum pubblici, probabilmente perché queste operazioni avvengono tramite comunicazioni private.
La distribuzione della tipologia di dati compromessi invece risulta essere.



(Figura 12– distribuzione dati compromessi nel dark web 2024)

(Fonte - https://socradar.io)

Oltre un milione di credenziali e-mail / password sono state compromesse nell'ultimo anno, permettendo agli aggressori di accedere a vari account delle vittime come e-mail, social media, servizi bancari e aziendali. La maggior sicurezza del password hash (quando un utente crea una password, il sistema la converte in una stringa criptata attraverso un algoritmo di hash, e salvata nel database invece della password in chiaro, che deve poi essere decifrata per poterla usare) la si può notare dai dati, le violazioni sono state tre volte meno rispetto alle password tradizionali. Gli indirizzi IP delle vittime possono essere sfruttati per attacchi mirati, frode online o per bypassare restrizioni geografiche nei cyber attacchi, e contano quasi duecentomila indirizzi rubati. I dati delle carte di credito rubate vengono utilizzati per acquisti fraudolenti, vendite sul Dark Web o per creare identità false.
Nel Dark Web non vengono venduti soltanto dati frutto di attacchi esterni, ma talvolta anche informazioni sottratte da dipendenti infedeli. Queste figure, chiamate "insider", accedono ai sistemi

aziendali dall'interno, sfruttando privilegi d'accesso per sottrarre dati e rivenderli poi a criminali informatici. Ciò rende ancora più difficile per le organizzazioni difendersi, poiché la minaccia proviene da utenti con legittime credenziali d'accesso.
Tutti questi dati una volta che sono stati rubati vengono poi messi in vendita su forum o mercati online. Nella tabella seguente sono riassunti i valori indicati dallo studio sul prezzo medio delle informazioni personali.

Informazioni personali e Documenti	Prezzo medio (USD)
Nome nubile della madre	15
Patente di guida	8
Credit score	7
Numero previdenza sociale	6
Report personale	4
Varie informazioni personali	3,5
Numero di telefono	2
Indirizzo di residenza	2

(Tabella 1- Prezzo medio in dollari delle informazioni personali nel Dark Web)

Il nome da nubile della madre ha il prezzo medio più alto, 15 dollari, probabilmente perché è una delle domande di sicurezza più comuni per il recupero degli. Questo lo rende un'informazione molto preziosa per gli hacker, che possono sfruttarla per bypassare i sistemi di autenticazione, in seconda e terza posizione troviamo patenti di guida e punteggi di credito, che possono essere utilizzati per aprire conti falsi, richiedere prestiti o effettuare frodi finanziarie. Le restanti informazioni invece, possono essere sfruttate per effettuare furti di identità o crearne di false ed accedere a servizi riservati.
Oltre alla vendita di dati e prodotti, sul Dark Web emergono sempre più frequentemente i cosiddetti servizi di "cybercrime as a service". In questo modello, gli attori malevoli offrono l'intera infrastruttura e il supporto necessari a condurre un attacco, con differenti livelli di sofisticazione. I prezzi variano in base all'efficacia, alla rarità e al livello di pericolosità dello strumento.

Malware e servizi	Prezzo medio (USD)
Exploit	5345
Loader	3566
RAT	2171
Stealer (abbonamneto)	1024

(Tabella 2- Prezzo medio in dollari di malware e strumenti di hacking nel Dark Web)

Gli Exploit sono tra gli strumenti più costosi e sofisticati disponibili sul Dark Web, si tratta di codici o programmi progettati per sfruttare vulnerabilità nei software, nei sistemi operativi o nelle reti aziendali, bypassando le misure di sicurezza ed aprendo le porte per ulteriori attacchi. I Loader sono strumenti progettati per facilitare la distribuzione di malware, permettendo di installare trojan, ransomware o spyware sui dispositivi delle vittime in modo discreto. Un altro strumento molto diffuso è il RAT (Remote Access Trojan), un tipo di trojan che consente agli hacker di prendere il controllo remoto di un computer o di una rete senza che la vittima se ne accorga, uno degli utilizzi principali riguarda lo spionaggio industriale, ricatti e furti di informazioni bancarie. Infine, gli Stealer sono software che funzionano in background, specializzati nel raccogliere e sottrarre informazioni sensibili.

Tra gli exploit più pericolosi ci sono gli 0-Day, vulnerabilità del sistema non ancora scoperte o risolte dai produttori, sono particolarmente preziosi perché consentono agli attaccanti di infiltrarsi in sistemi senza essere rilevati. Il prezzo di questi exploit può arrivare anche fino a 200.000 dollari quando riguardano sistemi operativi come windows o VPN aziendali.

La disponibilità di questi software dannosi rende sempre più difficile per aziende e utenti proteggere le proprie informazioni, alimentando un'economia sommersa che continua a evolversi con nuove tecniche e minacce.

Per quanto riguarda servizi di hacking più specifici i prezzi medi sono stati raccolti nella tabella seguente.

Servizi di Hacking	Prezzo medio (USD)
Certificazione di firma del codice	2.420
Disattivazione Antivirus	1.500
Droppler settimanale	500
Crittografia Malware	484
Droppler singolo utilizzo	83
Test Antivirus (per file)	10
Verifica carta di credito	0,15

(Tabella 3- Prezzo medio in dollari dei servizi di hacking nel Dark Web)

I certificati di firma del codice sono i servizi più costosi, poiché permettono agli hacker di superare le misure di sicurezza facendo apparire il malware come software legittimo. La disattivazione

dell'antivirus è il secondo servizio più costoso, in grado di aumentare notevolmente il successo di un attacco, il Dropper è un programma progettato per distribuire e installare malware su un sistema senza essere rilevato, il suo prezzo varia in base all'utilizzo, dai 500$ per aggiornamenti settimanali costati agli 83$ del singolo uso. La crittografia dei malware permette di proteggere il malware dalle scansioni dei servizi di sicurezza. Per controllare se un file è efficace contro vari sistemi di difesa esiste il servizio di antivirus test a 10$ a file, mentre per verificare la validità di una carta di credito rubata il prezzo è di 15 centesimi per carta.

La lotta al cybercrimine e al ruolo del Dark Web nelle attività illecite richiede uno sforzo globale. La sfida per governi e autorità consiste nel trovare un equilibrio tra la tutela dei diritti e la necessità di reprimere le attività criminali. Solo attraverso una cooperazione internazionale, l'aggiornamento continuo delle competenze e un approccio di sicurezza informatica proattivo, si potrà fronteggiare in modo efficace la minaccia rappresentata dal Dark Web e dagli attacchi informatici che ne scaturiscono.

1.5 Misure di difesa e vulnerabilità della sicurezza informatica

Le tecniche di attacco sono in continuo mutamento, diventando sempre più difficili da contrastare, di conseguenza il panorama della sicurezza informatica si è dovuto evolvere, utilizzando misure sempre più sofisticate per affrontare i cybercriminali. Le strategie di difesa non si limitano a soluzioni isolate, ma adottano un approccio integrato e stratificato che unisce tecnologie avanzate, processi organizzativi e una costante formazione del personale, ogni punto del sistema viene quindi protetto attraverso strumenti specifici. La trasformazione globale avvenuta tramite la digitalizzazione ha delineato la sicurezza informatica come un elemento imprescindibile per garantire la continuità operativa e la protezione di dati e risorse, portando il mercato globale della cybersecurity a superare i 200 miliardi di dollari, con stime di crescita future notevoli, con il nostro paese che nel 2023, ha speso 2,149 miliardi di euro, pari a circa 0,12% del PIL, in cybersicurezza.

1.5.1 Misure di difesa

Come per gli attacchi informatici anche le misure di difesa possono essere classificate in base alle loro tecniche e obiettivi.

Difesa degli accessi

La gestione delle identità digitali e il controllo degli accessi rappresentano un aspetto cruciale nella difesa informatica. L'utilizzo di password complesse, con una combinazione di diversi caratteri speciali, numeri e lettere minuscole e maiuscole, rappresenta uno dei metodi più semplici ed efficaci per garantire la sicurezza informatica. Tecniche più sofisticate, come l'autenticazione a più fattori (MFA) richiedono che gli utenti confermino la propria identità attraverso più di un elemento, ad esempio, password, token hardware, dati biometrici, rendendo molto difficile per un potenziale attaccante sfruttare eventuali credenziali rubate. Il Single Sign-On (SSO) semplifica l'esperienza utente, permettendo di accedere a diverse applicazioni con un'unica autenticazione, mentre sistemi centralizzati di gestione delle identità, come Active Directory o LDAP, garantiscono che i diritti di accesso siano assegnati e monitorati in maniera sicura.

Difesa della rete

Uno dei primi strumenti che vengono implementati per proteggere un'infrastruttura è rappresentato dal firewall. Questo dispositivo, che può assumere sia forma hardware che software, è progettato per monitorare e filtrare il traffico in ingresso e in uscita sulla rete, applicando una serie di regole predefinite. Il concetto alla base di un firewall è quello di creare una barriera tra la rete interna, considerata sicura, e l'ambiente esterno, potenzialmente ostile. Le regole implementate consentono

di bloccare tentativi di accesso non autorizzati e di suddividere il traffico, riducendo la possibilità che un attaccante possa sfruttare una vulnerabilità per penetrare nel sistema.

Accanto ai firewall, i sistemi di rilevamento (IDS) e prevenzione (IPS) delle intrusioni, sono in grado di analizzare il traffico di rete in tempo reale, confrontando i dati osservati con modelli di comportamento noti o con firme di attacchi già documentati. Mentre l'IDS si limita a segnalare anomalie e potenziali minacce, l'IPS interviene attivamente, bloccando automaticamente il traffico sospetto. Questo duplice approccio consente non solo di identificare le minacce, ma anche di contenere eventuali attacchi prima che possano propagarsi e compromettere ulteriori porzioni della rete.

Per garantire che le comunicazioni a distanza avvengano in sicurezza, le reti aziendali fanno ricorso alle Virtual Private Network (VPN), creando canali crittografati che proteggono i dati trasmessi tra utenti remoti e la rete centrale, rendendo praticamente impossibile l'intercettazione da parte di soggetti non autorizzati. La segmentazione della rete è una tecnica che suddivide l'infrastruttura in zone isolate, che in caso di compromissione, il danno rimane confinato e non si estende in tutto il sistema.

Difesa degli endpoint

Gli endpoint o dispositivi finali, quali computer e smartphone, rappresentano spesso il punto di ingresso principale per le minacce informatiche, gli antivirus e gli antimalware costituiscono il primo livello di difesa, essendo in grado di rilevare e neutralizzare software dannosi grazie a un continuo aggiornamento delle impronte digitali degli attacchi informatici conosciuti, ma, in un contesto in cui le minacce evolvono rapidamente, è necessario adottare soluzioni più sofisticate, come gli strumenti di Endpoint Detection and Response (EDR), che offrono un monitoraggio continuo e una capacità di risposta immediata in caso di attività sospette. Uno degli aspetti spesso sottovalutati riguarda la gestione delle patch e degli aggiornamenti, mantenere aggiornati i sistemi operativi e le applicazioni è una misura preventiva essenziale per eliminare le vulnerabilità note e ridurre il rischio di exploit.

Difesa dei dati

La protezione dei dati è un pilastro fondamentale della sicurezza informatica. La crittografia, applicata sia ai dati in transito sia a quelli memorizzati, garantisce che informazioni sensibili siano illeggibili a chiunque non possieda le chiavi di decriptazione. L'adozione di protocolli sicuri come TLS/SSL per la trasmissione dei dati e l'utilizzo di algoritmi di crittografia robusti per la protezione dei file memorizzati sono pratiche standard che impediscono accessi non autorizzati e mitigano il rischio di furti di dati.

Accanto alla crittografia, le soluzioni di Data Loss Prevention (DLP) monitorano il flusso di informazioni all'interno dell'organizzazione, identificando e prevenendo la fuoriuscita di dati

sensibili.

Inoltre, l'utilizzo di backup è essenziale per garantire la continuità operativa, la creazione di copie dei dati periodiche permette di ripristinare i sistemi in caso di attacchi, come i ransomware, riducendo al minimo i tempi di inattività e le perdite economiche.

1.5.2 Vulnerabilità della sicurezza

Le vulnerabilità in ambito informatico sono presenti in diverse forme che variano dalle soluzioni di difesa adottate al fattore umano. L'utilizzo di password deboli, crittografia non adeguata e tecnologie obsolete, sia hardware che sistemi digitali non aggiornati, sono tra le principali ragioni di un'esposizione maggiore a rischi significativi, non potendo proteggere adeguatamente all'evoluzione costante delle minacce informatiche.

Il fattore umano invece, può essere un anello debole in molti sistemi di sicurezza, nelle tipologie di attacchi di social engineering non si tenta di forzare direttamente le difese, ma ingannare gli utenti per ottenere le credenziali di accesso e permettendo ai cybercriminali di bypassare anche le migliori misure di sicurezza. La formazione diventa quindi uno degli strumenti più efficaci per mitigare i rischi. Per le aziende, oltre al rispetto di standard di sicurezza minimi e normative, la formazione del personale è una strategia a lungo termine per ridurre l'incidenza di errori umani, rendendo ogni dipendente consapevole del proprio ruolo nel proteggere le risorse digitali. Anche per i consumatori l'educazione informatica assume un ruolo cruciale, le istituzioni tramite campagne di sensibilizzazione rivolte al grande pubblico, rendendo i cittadini consapevoli delle minacce riducendo le vulnerabilità agli attacchi.

La gestione del rischio cibernetico richiede quindi una valutazione completa di tutte le possibili vulnerabilità esistenti, integrando metodologie tecniche e finanziarie. Con il costante aumento degli attacchi informatici e delle loro conseguenze economiche, le assicurazioni hanno assunto un ruolo di rilievo nella mitigazione dei rischi. Queste polizze coprono una vasta gamma di rischi, i principali sono rappresentati dai costi di ripristino, dalle eventuali spese legali e generare una maggior fiducia nei partner commerciali, come tutte le assicurazioni contengono delle limitazioni, che devono essere valutate attentamente le coperture nei vari scenari.

Le assicurazioni, la formazione e le misure di difesa non devono essere considerate come soluzioni alternative, ma dovrebbero essere integrati in una strategia complessiva, mentre le tecniche di difesa puntano e la formazione consentono di prevenire e contenere gli attacchi, le assicurazioni offrono una sicurezza finanziaria e supporto operativo in caso di violazioni.

1.6 Il quadro normativo e leggi sulla sicurezza cibernetica

La portata globale e la dimensione immateriale di Internet complicano notevolmente la possibilità di perseguire i reati commessi online. Le difficoltà aumentano quando si ha a che fare con i cosiddetti "paradisi fiscali", poiché le forze di polizia faticano a ottenere la cooperazione necessaria dalle autorità locali. Inoltre, la rete è stata a lungo percepita come uno spazio privo di restrizioni, in cui l'anonimato viene considerato una forma di tutela della riservatezza, piuttosto che una minaccia.

A differenza dei crimini che hanno luogo in spazi fisici e coinvolgono persone e oggetti tangibili, i crimini informatici hanno luogo in spazi virtuali e spesso prendono di mira risorse e informazioni intangibili. Gli sviluppi tecnologici hanno esposto infrastrutture, dati e sistemi informativi a minacce sempre più complesse e numerose, ed in assenza di una chiara base giuridica, gli operatori del settore pubblico e privato rischiano di non adottare misure di sicurezza adeguate o di trascurare gli obblighi fondamentali in materia di protezione dei dati e continuità operativa. La regolamentazione quindi si pone gli obiettivi di fissare standard minimi di sicurezza e a stabilire requisiti tecnici e organizzativi per la protezione di reti e sistemi, garantire la protezione dei dati personali, il rispetto dei diritti e le libertà dei cittadini e protegge la riservatezza e l'integrità delle informazioni.

Promuove inoltre la condivisione delle responsabilità, coinvolgendo soggetti pubblici e privati nella definizione di procedure comuni e nello scambio di informazioni sulle minacce. Infine, imporre punizioni per i comportamenti illeciti, prevedendo sanzioni amministrative e penali in caso di violazioni gravi.

1.6.1 Il quadro normativo dell'Unione Europea

La natura senza confini territoriali dei crimini informatici rende fondamentale l'adozione di norme quanto più possibili uniformi tra i vari Paesi. In Unione Europea, il primo incontro del Consiglio d'Europa dedicato a reati collegati all'uso delle tecnologie informatiche, ebbe luogo nel 1999. Il riconoscimento dell'importanza globale del fenomeno del cybercrime si è concretizzato con la ratifica della Convenzione di Budapest da parte del Consiglio d'Europa il 23 novembre 2001, la Convenzione di Budapest è il primo trattato internazionale che regola i reati commessi attraverso Internet e le reti informatiche, e negli ultimi anni, l'Unione europea (UE) ha accelerato gli sforzi per creare un mercato digitale sicuro e resistente, sono stati adottati diversi strumenti giuridici per uniformare gli standard di sicurezza e garantire un livello di protezione uniforme in tutti gli Stati membri.

La direttiva (UE) 2016/1148, nota come Direttiva NIS (Network and Information Security), è il primo strumento giuridico a livello europeo dedicato alla sicurezza dei sistemi di rete e di informazione, successivamente, la Direttiva NIS 2 2022/2555 ha ampliato l'ambito di applicazione e rafforzato i

requisiti per includere più settori vitali per la società e l'economia. L'obiettivo è garantire che gli attori principali, come le aziende che forniscono servizi critici (energia, finanza, trasporti, sanità) e grandi servizi digitali, adottino standard di prevenzione e risposta agli incidenti in collaborazione con le autorità competenti e con le altre aziende.
Accanto alla Direttiva NIS, meritano particolare attenzione anche il GDPR (Regolamento Generale sulla Protezione dei Dati) e il Cybersecurity Act.
Il primo si concentra sulla protezione della privacy e dei diritti fondamentali dei cittadini europei e obbliga le organizzazioni ad adottare misure tecniche e organizzative adeguate per proteggere i dati personali, il GDPR prevede l'obbligo di notifica alle autorità di controllo e agli interessati in caso di violazione o perdita di dati e sanzioni molto severe in caso di violazione del regolamento. Il Cybersecurity Act (Regolamento (UE) 2019/881), invece, mira a stabilire un quadro europeo di certificazione per la sicurezza informatica di prodotti, servizi e processi e rafforza i poteri dell'ENISA (Agenzia dell'Unione Europea per la Cybersecurity) nel suo ruolo di coordinamento e supporto tecnico.

1.6.2 Il quadro normativo in Italia

La prima iniziativa legislativa italiana mirata a contrastare i reati informatici risale al 1993, con l'approvazione della Legge n. 547/93. Fino a quel momento, infatti, i comportamenti illeciti rivolti contro i sistemi informatici erano inquadrati nelle fattispecie penali già previste dal Codice Penale, una prassi che sollevava dubbi in quanto potenzialmente in contrasto sia con il principio di legalità sia con il principio di tassatività. Il primo, sancito dall'articolo 1 del Codice Penale, stabilisce che non è possibile punire alcun fatto se non previsto espressamente dalla legge, il secondo, invece, vieta sia al legislatore sia al giudice di estendere l'applicazione delle norme penali oltre i casi specificamente contemplati. In tal modo si intende evitare che il potere giudiziario possa intervenire in modo arbitrario nella definizione dei reati.
Successivamente, in linea con le direttive e i regolamenti comunitari, l'Italia si è dotata di una serie di norme volte a sostenere la resilienza dei propri sistemi informativi. Un passaggio fondamentale è stata l'implementazione della Direttiva NIS mediante il D.Lgs. n. 65/2018, che ha classificato gli enti responsabili di servizi essenziali e i provider di strumenti digitali obbligati a rispettare specifici requisiti di sicurezza e di notifica degli incidenti. Con la costituzione dell'Agenzia per la Cybersicurezza Nazionale (istituita dal D.L. 14 giugno 2021, n. 82, convertito in legge con L. 4 agosto 2021, n. 109), l'Italia ha voluto dotarsi di un soggetto autorevole, autonomo e specializzato, con il compito di indirizzare e coordinare le politiche nazionali di cybersicurezza. L'Agenzia, infatti,

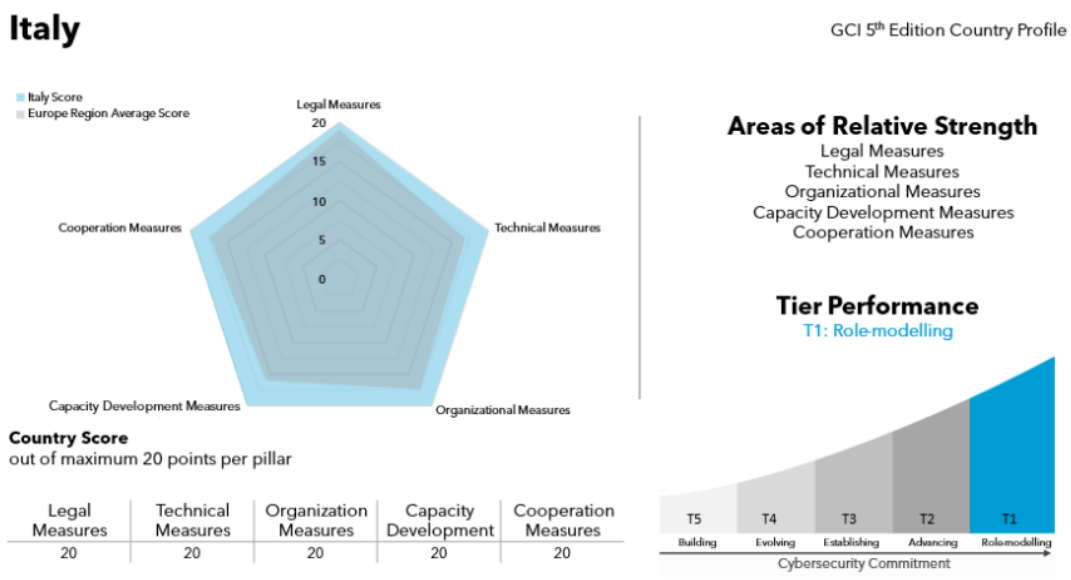
definisce la strategia nazionale, promuove la collaborazione tra pubblico e privato, e assicura l'adeguamento alle normative internazionali.

Un altro tassello rilevante nel panorama italiano è rappresentato dal Piano Nazionale di Ripresa e Resilienza (PNRR), che destina risorse per quasi 10 miliardi di euro alla digitalizzazione della Pubblica Amministrazione e alla sicurezza cibernetica. L'obiettivo è garantire infrastrutture più moderne e sicure, migliorare la protezione dei dati dei cittadini e promuovere l'adozione di tecnologie di monitoraggio e prevenzione degli attacchi informatici. Inoltre, il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) contiene disposizioni che, pur non riguardando esclusivamente la cybersecurity, si occupano di vari aspetti relativi alla digitalizzazione della Pubblica Ammistrazione, come la gestione sicura dei documenti informatici e la validità delle firme digitali.

Nella prassi, i soggetti che rientrano nel perimetro delle normative europee e italiane devono garantire la robustezza dei propri sistemi attraverso l'adozione di misure tecniche di difesa, come firewall, sistemi di rilevamento delle intrusioni, crittografia, backup sicuri, piani di disaster recovery. La formazione costante del personale, elemento cruciale per prevenire comportamenti a rischio. Ed infine, la notifica tempestiva degli incidenti di sicurezza, con una comunicazione trasparente verso le autorità competenti e, ove previsto, verso gli interessati in caso di compromissione dei dati.

Il panorama normativo, però, è in continua evoluzione. L'introduzione di nuove tecnologie quali 5G, intelligenza artificiale, blockchain e Internet of Things apre scenari inediti sul fronte delle opportunità e dei rischi. È quindi plausibile attendersi ulteriori aggiornamenti legislativi volti a chiarire responsabilità e obblighi, a promuovere standard di sicurezza ancora più elevati e a incentivare la cooperazione internazionale. Dal momento che le minacce informatiche non conoscono confini, la collaborazione tra Stati, agenzie di sicurezza, organizzazioni private e singoli esperti risulta essenziale. Senza un approccio integrato e condiviso, infatti, né le aziende né i governi saranno in grado di rispondere efficacemente alla complessità e alla rapidità con cui si evolvono gli attacchi.

L'Italia negli anni ha avuto un'evoluzione positiva nel campo della cybersecurity, puntando a rimanere competitiva a livello internazionale, non soltanto attraverso quadri normativi e tecnici robusti, ma anche tramite lo sviluppo di competenze e sinergie con gli attori nazionali e internazionali. Questa crescita negli anni è confermata dal Global Cybersecurity Index (GCI).



(Figura 13– performance dell'Italia nel Global Cybersecurity Index)

(Fonte – Global Cybersecurity Index)

L'indice GCI misura l'impegno dei paesi nei confronti della sicurezza informatica nel contesto delle misure attraverso i cinque pilastri: misure legali, misure tecniche, misure organizzative, sviluppo di capacità e misure di cooperazione. Con ogni pilastro che può arrivare a un livello massimo di 20 punti, il nostro paese ottiene il massimo dei voti in ogni pilastro, collocandosi nella posizione più elevata di performance, T1: Role-modelling, ovvero il livello massimo di impegno e prestazioni in termini di cybersecurity. Per mantenere e rafforzare questo ruolo di primo piano, sarà cruciale continuare a investire in ricerca, competenze digitali, cooperazione internazionale e aggiornamento costante degli strumenti di difesa (tecnologici, legali e organizzativi). Inoltre, la diffusione di una cultura di cybersecurity tra i cittadini e le imprese rimane un fattore determinante per garantire la resilienza complessiva del sistema.

2 Analisi dei dati sugli attacchi cibernetici in Italia

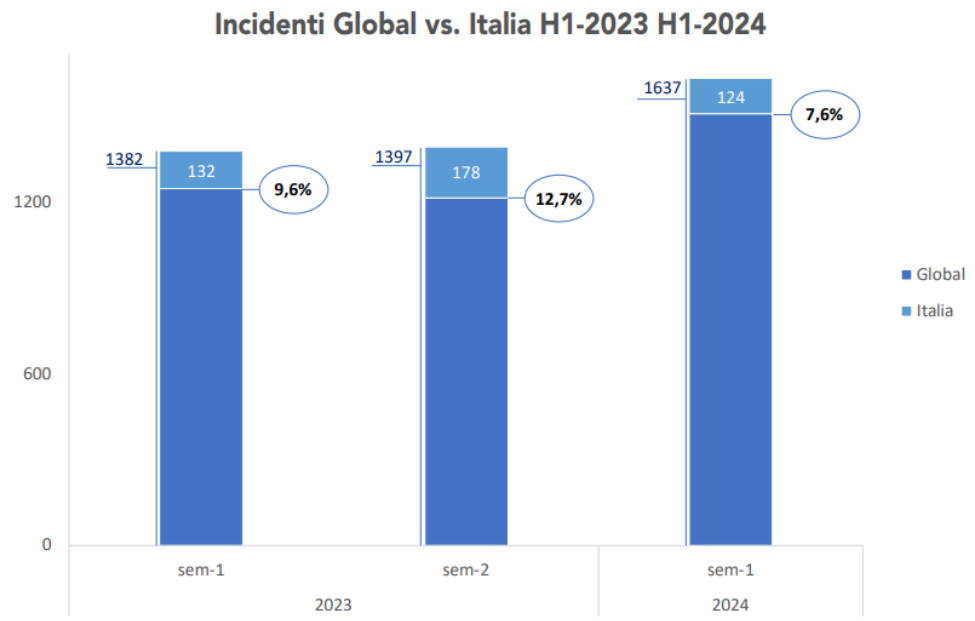
Negli ultimi anni l'Italia ha registrato un aumento considerevole degli attacchi cibernetici, a testimonianza di una tendenza globale che vede la criminalità informatica in costante crescita.

Fino alla metà degli anni Duemila, l'Italia non presentava un livello particolarmente elevato di criminalità informatica rispetto ad altri Paesi europei, a causa di una digitalizzazione ancora parziale di molti servizi e di una minore diffusione di reti ad alta velocità. Negli ultimi dieci-quindici anni, però, il panorama è radicalmente cambiato. La digitalizzazione di processi e servizi, l'adozione su larga scala di soluzioni cloud e l'uso massiccio di dispositivi connessi, dall'Internet of Things alle infrastrutture critiche digitali, hanno contribuito a rendere imprese, pubbliche amministrazioni e cittadini sempre più esposti a minacce online. In questo capitolo cercheremo di fornire una panoramica completa dei dati disponibili, delle principali tipologie di attacco e dei settori più colpiti.

I dati utilizzati per l'analisi si riferiscono solo a crimini informatici portati a termine con successo, attacchi avvenuti e confermati e divenuti di pubblico dominio, risultando quindi una rappresentazione inevitabilmente incompleta rispetto all'ampiezza reale del fenomeno. Anche nel caso in cui ci sia obbligo di segnalazione alle autorità competenti, quest'ultime spesso non rendono pubbliche le segnalazioni ricevute. Lo stesso discorso vale per le denunce presentate alle forze dell'ordine, alle compagnie assicurative e per le informazioni raccolte dai provider di connettività, questi dati risultano sicuramente di grande interesse, ma generalmente restano accessibili solo a tali operatori. Le fonti utilizzate sono state, l' ACN: Agenzia per la Cybersicurezza Nazionale ed il rapporto Clusit sulla Sicurezza Informatica, che si avvale della collaborazione del Security Operations Center (SOC) gestito da FASTWEB e delle rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni.

Situazione italiana

"Italia sotto assedio" afferma il rapporto sulla Sicurezza Informatica di Clusit (Associazione italiana per la Sicurezza Informatica), dal punto di vista numerico, negli ultimi cinque anni la situazione è significativamente deteriorata, evidenziando una tendenza di crescita quasi invariata nel tempo. Nel 2023, gli incidenti informatici a livello globale hanno registrato un incremento del 12% rispetto all'anno prima, mentre in Italia l'aumento è stato ancora più marcato, raggiungendo il 65%. Sempre nel 2023 l'11% degli attacchi registrati nel mondo sono stati rivolti verso l'Italia, mentre nel 2012 erano meno dell'8% e nel 2011 meno del 3,5%. La tendenza globale nella prima metà del 2024 evidenzia un'ulteriore crescita rilevante, con un aumento del 17% rispetto al semestre precedente.

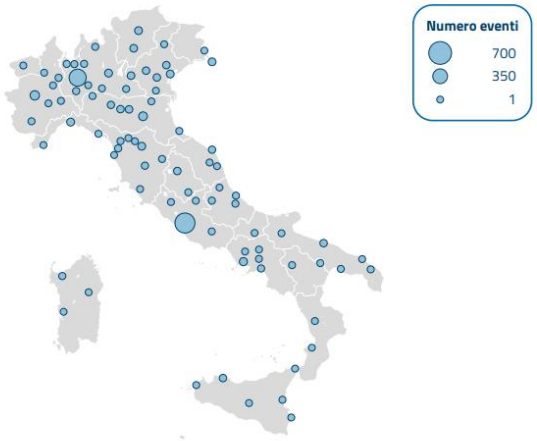


(Figura 14– percentuale degli attacchi in Italia rispetto al livello mondiale)

(Fonte – Clusit)

Nei primi sei mesi del 2024, i crimini informatici andati a buon fine contro il territorio italiano rappresentano il 7,6% del totale degli eventi registrati a livello globale, pari a 1.637. La quota degli incidenti italiani risulta in leggero miglioramento in confronto ai due semestri precedenti, rispettivamente il 9,6% e 12,7%, un segnale incoraggiante ma che potrebbe solo essere legato ad una fluttuazione nelle attività dei cybercriminali, dato che anche nel H1 del 2023 gli attacchi (132) sono risultati inferiori rispetto al periodo H2 (178). Ad ogni modo, anche nella prima metà del 2024, il numero di attacchi subiti dal nostro Paese rimane significativamente elevato rispetto alla popolazione e al PIL nazionale in rapporto agli stessi valori globali, segnalando una possibile debolezza che rende l'Italia un bersaglio privilegiato per i cybercriminali.

Per quanto riguarda la distribuzione geografica dei soggetti interessati dagli attacchi informatici (Fig.15) le regioni settentrionali, caratterizzate da un tessuto economico e una digitalizzazione più sviluppate, con numerose aziende ed infrastrutture critiche, sono quelle più colpite. Anche la regione della capitale registra un numero elevato di aggressioni, date dal suo ruolo di centro amministrativo. Le regioni meridionali e le isole risultano le meno colpite.



(Figura 15- Distribuzione geografica dei soggetti impattati dagli eventi cyber)

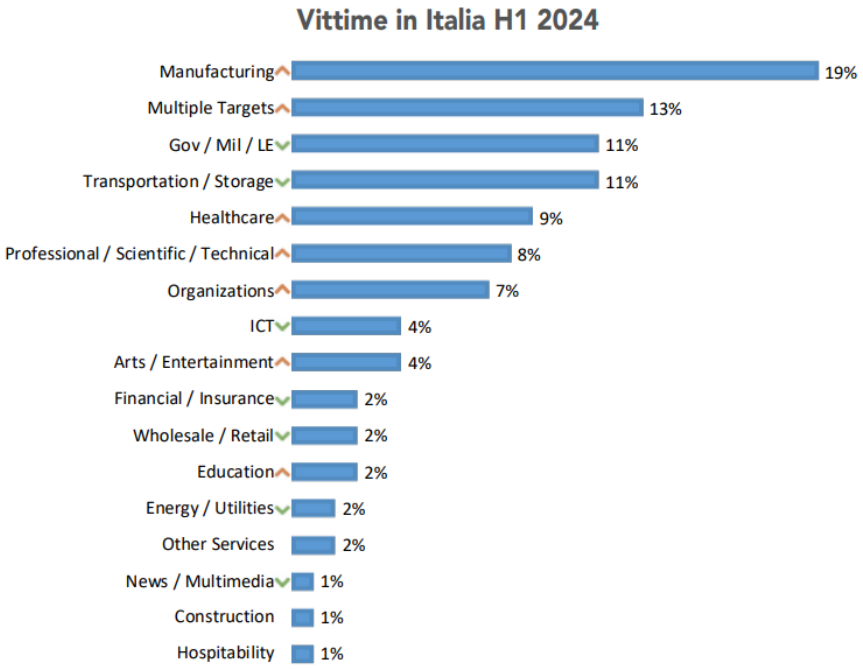
(Fonte - ACN: Agenzia per la Cybersicurezza Nazionale)

Dal punto di vista delle motivazioni dietro agli attacchi contro il nostro paese le categorie di Espionage/Sabotage o Information Warfare non sono presenti in modo rilevante, gli eventi sono da attribuire maggiormente al conflitto russo-ucraino, e nonostante l'affiliazione dei vari gruppi responsabili al governo russo sia probabile, non ci sono prove certe. La categoria responsabile del maggior numero di assalti informatici è quella del Cybercrime, nel primo semestre del 2024 rappresenta il 71%, in crescita rispetto al 2023 dove si attestava al 65%. La percentuale negli anni è in calo, nel 2021 era il 100% e il 93% nel 2022, la situazione non è comunque positiva, in valori assoluti, il numero di attacchi è in costante aumento, passando dai 29 del 2020 fino ad arrivare a 197 del 2023. L'altra categoria responsabile degli incidenti in Italia è quella del Hacktivism, con una quota del 29%, ma che hanno subito una notevole crescita, nel 2021 non sono stati registrati attacchi significativi in questa categoria, per poi passare a 13 nel 2022 ed a 112 nel 2023. Dati preoccupanti, e che peggiorano ulteriormente in relazione all'analisi del totale degli attacchi corrispondenti ad Hacktivism a livello globale, circa il 34% è avvenuto contro nostro paese, mentre nel 2023 era ben il 47% del totale. Dimostrando una particolare vulnerabilità del nostro paese ad azioni di natura politica o sociale.

2.1 Distribuzione attacchi per settore

Gli attacchi informatici colpiscono diverse aree dell'economia italiana in modo variabile, durante il 2023 il settore più colpito è stato quello Governativo / Militare / Forze dell'ordine, con una quota del 19%, la prima posizione è principalmente dovuta al boom di aggressioni di tipo Hacktivism. In seconda posizione troviamo il manifatturiero, settore industriale dedicato alla produzione di beni attraverso la trasformazione di materie prime in prodotti finiti, con il 13%, l'aspetto critico di questa

categoria è che a livello mondiale subisce circa un quarto degli attacchi totali. La medaglia di bronzo va alla logistica, con una percentuale del 11,6%. A livello globale invece nel 2023 la situazione risulta diversa, la categoria con il maggior numero di attacchi riguarda i target multipli (più settori colpiti contemporaneamente, senza un obiettivo specifico), con il 19,4%, seguito dalla sanità al 14,3% e dal Governativo / Militare / Forze dell'ordine al 11,7%.
Nel primo semestre del 2024 la distribuzione ha subito diverse variazioni.



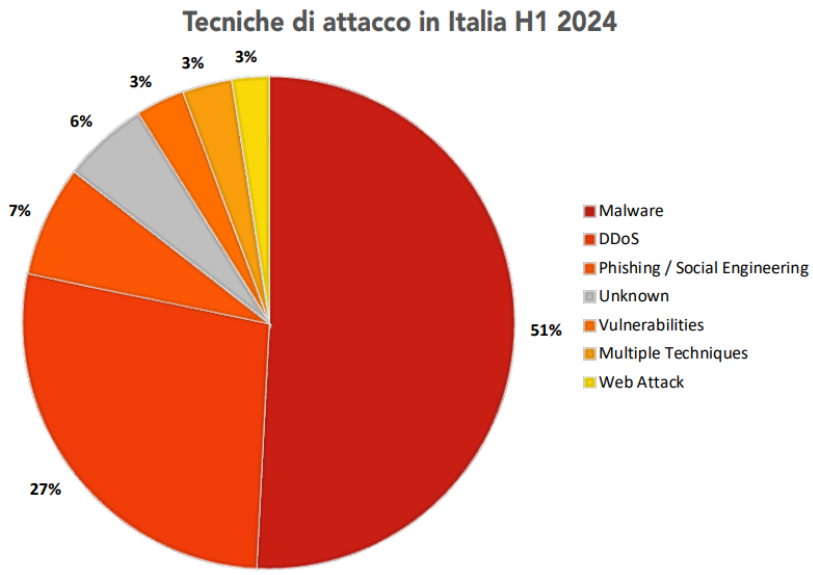
(Figura 16– distribuzione degli attacchi per settore)

(Fonte – Clusit)

Il settore manifatturiero con il 19% occupa per la prima volta la cima dell'elenco, ottenendo sempre una quota molto elevata (28%) sul totale a livello globale. I target multipli avanzano anche loro di posizione, aumentando di 2 punti percentuali e raggiungendo il 13%. L'attenuarsi dell'Hacktivism ad inizio 2024 può essere una delle cause della caduta del Governativo / Militare / Forze dell'ordine in terza posizione (11%), va tenuto presente però, che nella seconda metà del 2023 gli eventi di Hacktivism riusciti sono quasi raddoppiati rispetto ai primi sei mesi dell'anno. Il ranking a livello mondiale risulta nuovamente diverso rispetto al panorama italiano, la sanità conquista il primato (18%), superando i target multipli (16%) che retrocedono al secondo posto, mentre il gradino più basso del podio rimane invariato, Governativo / Militare / Forze dell'ordine si attesta al 13%.

2.2 Modalità di attacco

Le modalità con cui vengono condotti gli attacchi informatici forniscono una chiave di lettura per individuare le vulnerabilità più sfruttate dai cybercriminali.



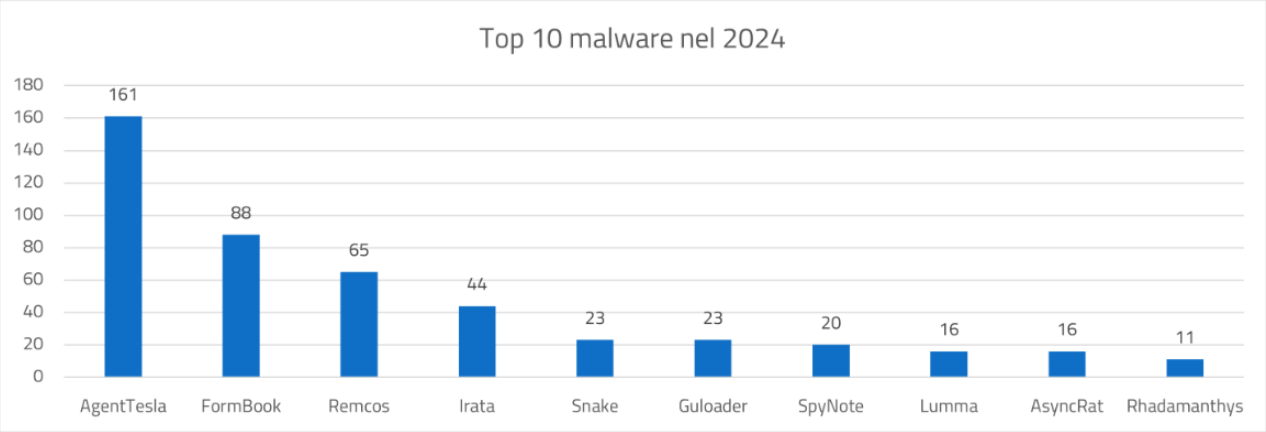
(Grafico 2– distribuzione modalità di attacchi informatici)

Nei primi sei mesi del 2024 la categoria malware, che comprende tutti i software dannosi progettati per compromettere sistemi informatici, rubare dati o causare danni, tra cui le principali varianti sono virus, trojan, worm e ransomware, riconquista in maniera incontrastata il primo posto in classifica, essendo responsabile della metà (51%) degli attacchi, mentre durante il 2023 si trovava seconda, fermandosi al 31%. Il fenomeno dell'Hacktivism torna ad influenzare la distribuzione, gli attacchi Ddos vengono spesso impiegati dagli attivisti per paralizzare i servizi dell'obiettivo preso di mira, attirando l'attenzione e consentendo di amplificare il messaggio di protesta alla popolazione. La tecnica Ddos che nel 2023 ha registrato il maggior numero di incidenti, rappresentando il 36%, ad inizio del 2024 si riduce di 9 punti percentuali arrivando al 27%, nonostante la riduzione rimane comunque molto più elevata l'incidenza rispetto al livello mondiale, dove si ferma al 7%. Gli attacchi basati su Phishing / Social Engineering, basati sulle debolezze del fattore umano, occupano la terza posizione con una quota del 7%. Le tecniche Unknown (le metodologie impiegate nell'attacco non sono di pubblico dominio), anche grazie a normative che impongono la segnalazione delle specifiche categorie di incidenti, diminuiscono rispetto all'anno precedente in cui erano posizionate terze, passando dal 17% al 6%.

La distribuzione su scala globale per il gradino più alto del podio è equivalente a quella italiana, Il malware resta il metodo più utilizzato, posizione che mantiene da oltre cinque anni, raggiungendo il 34%. Anche la seconda posizione a livello mondiale è stabile da anni, la categoria Unknown rappresenta poco più di un quarto dei casi. Terzi classificati troviamo gli attacchi che sfruttano falle di sicurezza presenti nei sistemi informatici, detti Vulnerabilities, al 14%.

Nel corso del 2024 il reparto CERT (Computer Security Incident Response Team) per conto dell'AgID (Agenzia per l'Italia Digitale) ha condiviso circa 20'000 Indicatori di Compromissione (la prova che qualcuno potrebbe aver violato i sistemi informatici di un'organizzazione) e identificato e contrastato 1767 minacce informatiche, in linea con il valore del 2023, 1713. La suddivisione di questi attacchi è stata 639 Malware e 1128 Phishing, che hanno avuto come scopo primario il furto di informazioni di autenticazione bancarie, di codici di accesso ad e-mail e, il furto di documenti di identità.

Tra queste classi di attacchi sono state rilevate diverse famiglie per Malware e Phishing, 69 per i primi e 133 per i secondi. Nella tipologia Malware il 67% è stato identificato nella classe di Infostealer, progettati per rubare informazioni sensibili, ed il restante 33% in quella RAT (Remote Access Trojan), che consentono agli Hacker di prendere il controllo remoto del dispositivo.

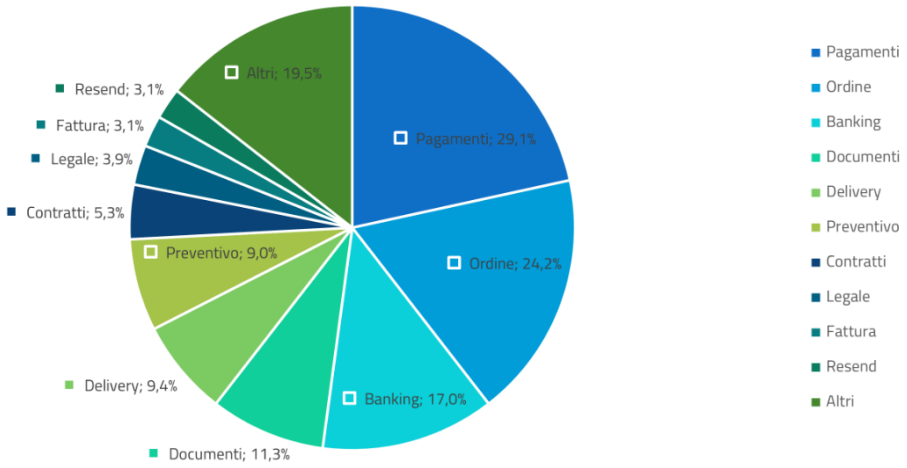


(Figura 17– top 10 famiglie di Malware operanti in Italia)

(Fonte - CERT-AGID)

Tra le principali famiglie di Malware operanti nel territorio italiano durante il 2024 in prima posizione troviamo AgentTesla, un Infostealer ed un Malware-as-a-service, ovvero venduto o affittato, attivo dal 2014 è stato costantemente aggiornato per migliorare la sua efficacia, si diffonde principalmente tramite e-mail di phishing con allegati infetti. Nella seconda posizione troviamo Formbook, appartenente alla stessa tipologia di Malware di AgentTesla, mentre in terza posizione, Remcos appartenente alla tipologia RAT. Nella top 10 è anche presente SpyNote, spyware progettato per dispositivi Android.

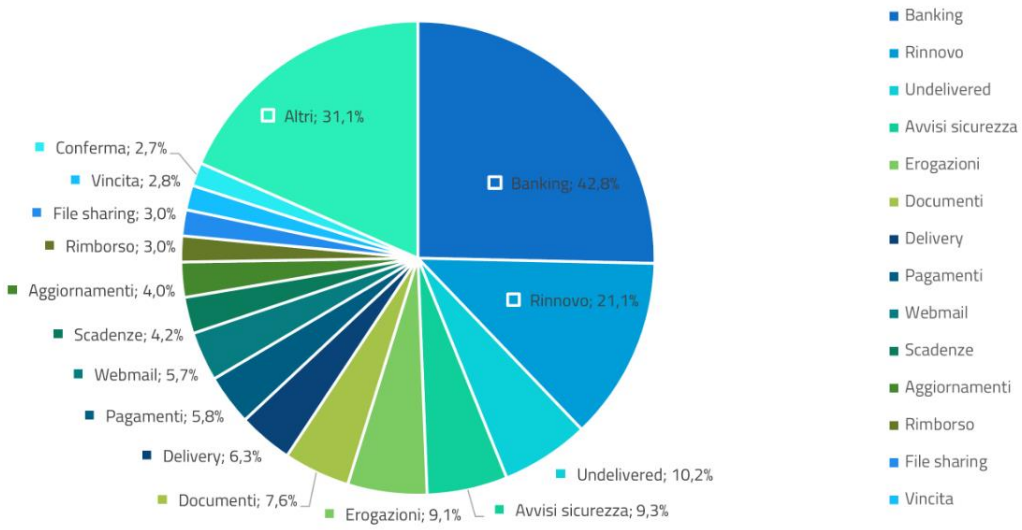
Per quando riguarda le motivazioni usate per la diffusione dei Malware durante il 2024.



(Figura 18– principali motivazioni per la diffusione di Malware in Italia)

(Fonte - CERT-AGID)

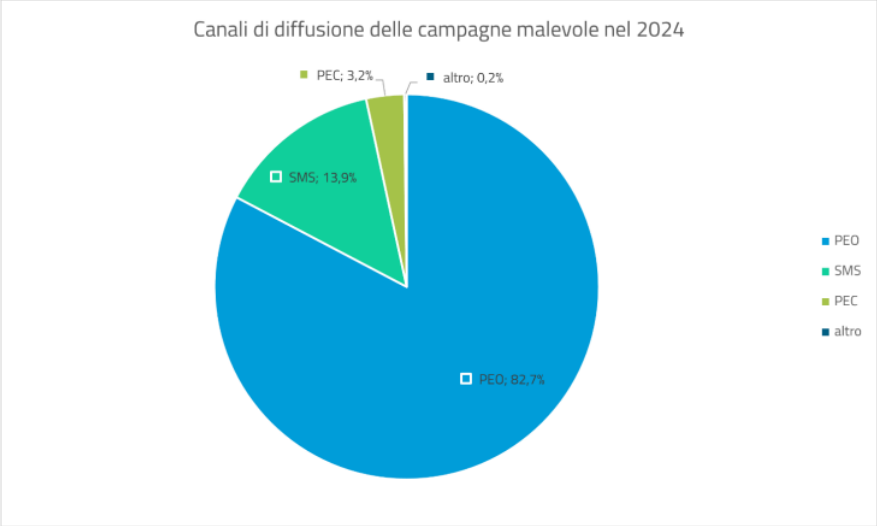
Le argomentazioni principali riguardano pagamenti, ordini e banking, questa tendenza si conferma abbastanza stabile durante gli anni. La diffusione sempre maggiore di pagamenti elettronici e Internet banking ha reso questo settore un bersaglio preferenziale come argomento per colpire le vittime.
Sul tema dei Phishing invece, le principali motivazioni utilizzate per la loro trasmissione differiscono in parte rispetto ai malware, rimane comunque in modo simile come motivazione principale l'ambito bancario.



(Figura 19– principali motivazioni per la diffusione di Phishing in Italia)

(Fonte - CERT-AGID)

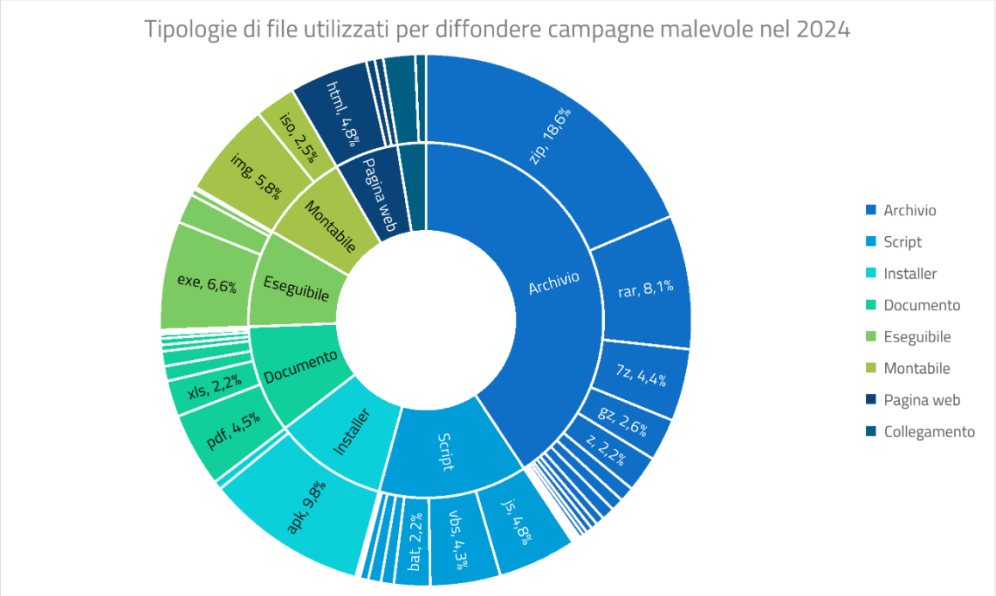
Come canali principali di diffusione degli attacchi informatici troviamo tre principali tipologie.



(Figura 20– principali canali di diffusione attacchi informatici)

(Fonte - CERT-AGID)

Il canale più utilizzato, in prima posizione stabile da anni, è quello della Posta Elettronica Ordinaria (PEO), utilizzato da milioni di utenti, sia privati che aziendali, rappresenta la superficie di attacco più estesa a disposizione dei criminali informatici. Rispetto al 2023 l'utilizzo della Posta Elettronica Certificata (PEC) è triplicato, colpendo soprattutto il settore bancario. L'utilizzo di SMS con la tecnica smishing (combinazione delle parole SMS e phishing), cercando di imitare istituzioni ufficiali con collegamenti link dannosi, è diminuito di 9 punti percentuali dall'anno precedente.



(Figura 21– principali tipologie di file per diffondere malware)

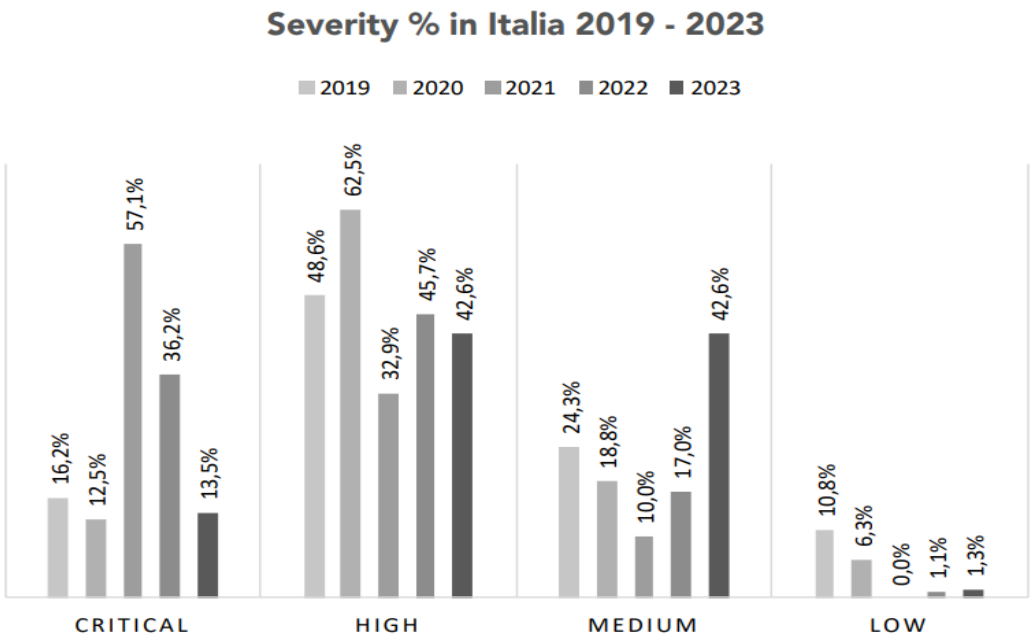
(Fonte - CERT-AGID)

I file di archivi compressi, soprattutto zip e rar, continuano ad essere il modo principale per diffondere malware, con una percentuale di circa il 41% dei file dannosi analizzati. I file script, in vari formati,

rappresentano la seconda tipologia più utilizzata per la diffusione di malware, totalizzando quasi il 14% degli attacchi. Analogamente ai file eseguibili EXE, questi script possono essere avviati con un semplice clic, consentendo l'esecuzione di comandi dannosi. L'uso di documenti PDF, fogli Excel, documenti Word e altri formati del pacchetto office, rappresentano una quota del 10%. L'utilizzo di file APK, utilizzati per l'istallazione di applicazioni su sistemi Android, è incrementato negli anni, arrivando anche loro ad occupare una porzione del 10%.

2.3 Gravità degli attacchi

Tutte queste metodologie di attacco hanno un impatto diverso sulle vittime, nel corso degli anni l'andamento degli effetti si è intensificato arrivando quasi alla completa scomparsa del livello più basso di Severity.



(Figura 22 - Severity degli incidenti in Italia nel periodo 2019-2023)

(Fonte – Clusit)

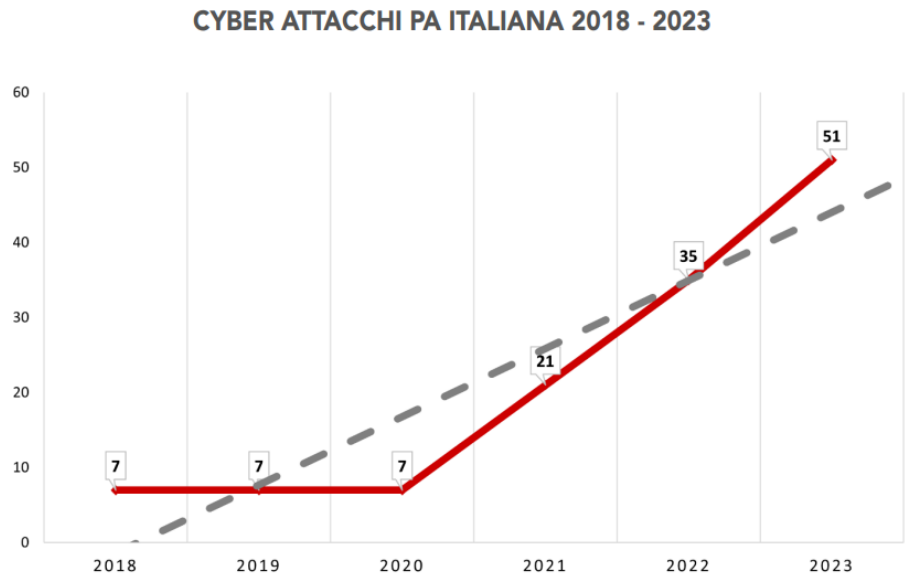
L'Hacktivism, come visto in precedenza, è tra le tecniche di attacco che il nostro paese subisce maggiormente, fortunatamente questa tipologia di aggressione non ha spesso ripercussioni critiche, generalmente gli vengono attribuiti livelli di gravità medio o alti. Un discorso simile può essere fatto per le tecniche Ddos, utilizzate spesso anche dagli attivisti, nella maggior parte dei casi non comportano gravi conseguenze sul lungo periodo, ma più momentanei disagi e disservizi. La categoria critica è di nuovo in riduzione, e diverge in maniera importante rispetto al campione globale dove rappresenta il 38%, gli attacchi legati a Espionage e Information Warfare, che non hanno un peso rilevante in Italia, sono quelli principalmente legati a questo livello di severity. Nonostante i dati

presentino una situazione migliore rispetto al resto del mondo, affermare che la gravità media degli incidenti informatici in Italia sia inferiore non sarebbe corretto, attacchi che in altri paesi riescono ad essere evitati o contenuti, senza quindi emergere nelle statistiche, nel nostro paese riescono a raggiungere livelli di severity media e nei casi peggiori alta. Evidenziando la necessità di ulteriori investimenti in cybersicurezza.

2.4 Pubblica Amministrazione

La crescente digitalizzazione dei servizi pubblici ha ampliato l'esposizione agli attacchi hacker, la sicurezza informatica nella Pubblica Amministrazione italiana evidenzia un settore particolarmente

esposto ai cyberattacchi, spesso a causa di infrastrutture obsolete, scarsa manutenzione e limitate risorse dedicate alla cybersecurity.

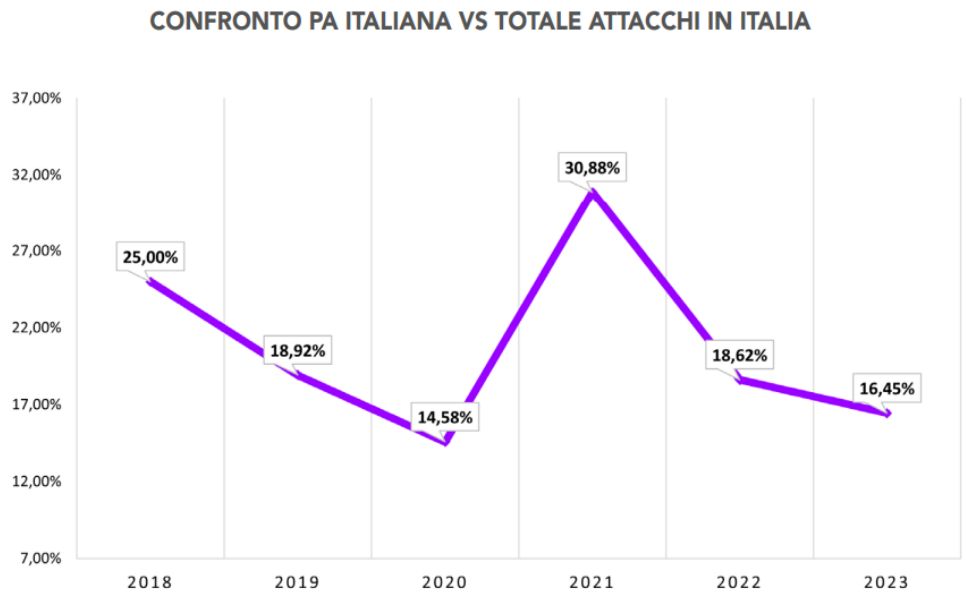


(Figura 23– attacchi informatici contro la pubblica amministrazione)

(Fonte – Clusit)

Il numero totale di attacchi diretti contro la Pubblica Amministrazione è in continua crescita dal 2020, si può notare un picco negli attacchi tra il 2020 e il 2021, la causa principale è stata la pandemia di Covid-19, emergenza sanitaria che ha portato l'Amministrazione Pubblica ad una massiccia digitalizzazione improvvisa e forzata, con l'adozione di strumenti digitali, spesso senza un'adeguata protezione.

Dal punto di vista percentuale, sugli attacchi totali arrecati al nostro paese (Fig.23), la Pubblica Amministrazione negli anni in media ha subito circa un quinto delle aggressioni, durante il 2021, per i motivi spiegati precedentemente c'è stato un picco, per poi calare progressivamente negli ultimi due anni. Questa riduzione potrebbe erroneamente suggerire una situazione in miglioramento, ma se si guarda il numero assoluto, gli attacchi continuano a crescere. La riduzione della quota riguardante la Pubblica Amministrazione è dovuta ad un aumento maggiore delle attività criminali contro il settore privato, solitamente più redditizio, riducendo così il peso percentuale sul totale.



(Figura 24– rapporto tra il numero di attacchi contro la PA e il totale)

(Fonte – Clusit)

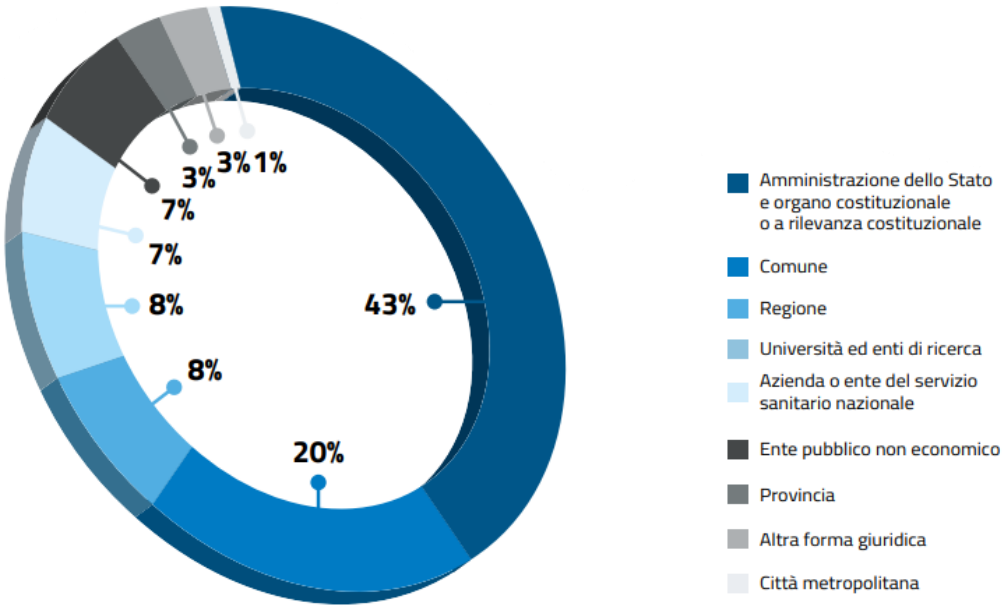
Le motivazioni degli attacchi verso la Pubblica Amministrazione nell'ultimo anno sono opposte rispetto all'andamento generale a livello nazionale, L'Hacktivism rappresenta all'incirca il 70% dei casi contro il 30% del Cybercrime. Negli anni precedenti però, quest'ultima categoria ha rappresentato la principale minaccia con un incidenza costante di oltre la metà degli attacchi.

La severity degli incidenti invece, rispetta la tendenza nazionale, con i livelli alto e medio a farla da padrone ed una quota di grado critico minore, poco più del 10%. Questi risultati rispecchiano anche le principali tecniche di attacco verso la Pubblica Amministrazione, i malware, le tecniche sconosciute e i Ddos sono le principali sfide verso il settore pubblico, con quest'ultima tecnica che ha avuto un aumento di 8 volte nel 2023, da attribuire ai maggiori attacchi a scopo simbolico-propagandistico degli attivisti.

Tecnica di Attacco	2018	2019	2020	2021	2022	2023
DDoS	0	0	0	3	4	34
Unknown	6	5	6	3	5	4
Malware	0	0	1	14	15	4
Vulnerabilities	0	0	0	1	6	3
Web Attack	1	0	0	0	1	3
Identity Theft / Account Cracking	0	0	0	0	2	2
Phishing / Social Engineering	0	1	0	0	2	1
Multiple Techniques	0	1	0	0	0	0

(Tabella 4– distribuzione tecniche di attacco contro la Pubblica Amministrazione)

Nello specifico della struttura della Pubblica Amministrazione durante il 2023 il ramo più colpito è quello dell'Amministrazione dello stato e organi costituzionali, con il 43% degli attacchi, bersagli privilegiati dalla loro importanza nel funzionamento dello stato. Al secondo posto preoccupa la presenza dei comuni, con il 20%, evidenziando una vulnerabilità diffusa nei servizi digitali locali, probabilmente dovuta a risorse limitate per la cybersecurity. Un discorso analogo può essere fatto anche per le regioni (8%), mentre il settore sanitario e la ricerca mettono in luce l'importanza della protezione dei dati critici, con il rischio sempre più crescente degli attacchi ransomware.

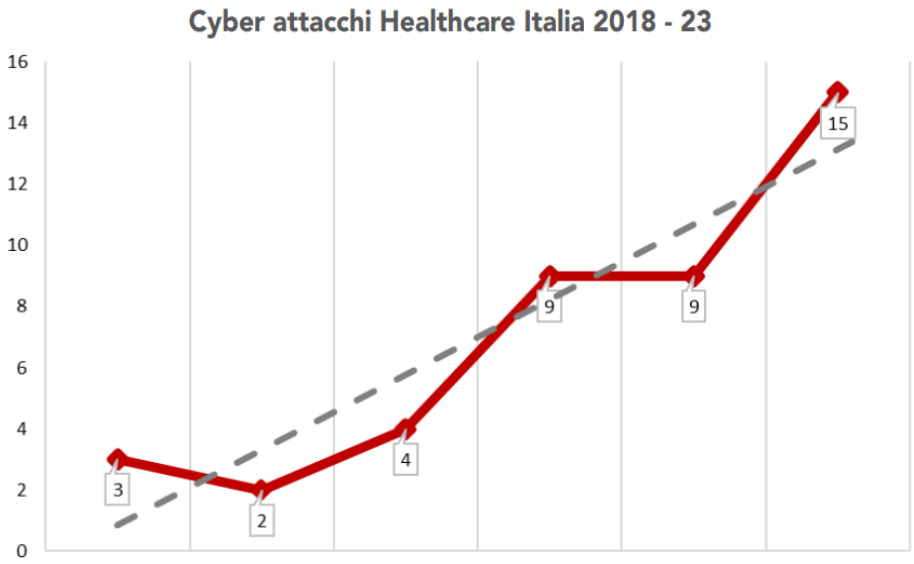


(Figura 25– distribuzione dei cyberattacchi contro la Pubblica Amministrazione)

(Fonte - ACN: Agenzia per la Cybersicurezza Nazionale)

2.5 Settore Sanitario

Negli ultimi anni, il settore sanitario è diventato uno dei bersagli privilegiati dei cybercriminali, il più colpito a livello mondiale. Gli ospedali e le strutture sanitarie custodiscono enormi quantità di informazioni personali e mediche, come cartelle cliniche, dati bancari, piani terapeutici e storie sanitarie dei pazienti. Questi dati hanno un valore elevatissimo sul dark web, poiché possono essere usati per frodi, furti di identità o richieste di riscatto. In Italia la sanità si trova in una situazione migliore, rispetto al totale delle intrusioni, è in ottava posizione nella classifica dei settori più colpiti, con una quota di poco più del 4% nel 2023.



(Figura 26- cyber attacchi verso il settore sanitario in Italia)

(Fonte – Clusit)

Se in termini percentuali il settore sanitario non sembra essere in grave rischio, dal punto di vista quantitativo gli attacchi sono aumentati quasi raddoppiando di anno in anno, accendendo un campanello d'allarme. Tra le motivazioni degli hacker nel 2023 è presente una novità, con il 7% dei casi associati ad Hacktivism, mentre il restante 93% è dovuto al Cybercrime. In questo settore la situazione è opposta rispetto alla pubblica amministrazione, la sanità è generalmente considerata neutrale e legata a servizi essenziali per la popolazione. Un attacco da parte di attivisti contro ospedali o infrastrutture sanitarie potrebbe danneggiare persone innocenti, minando la credibilità e l'etica del movimento.

Le tecniche di attacco sono composte dal 73% dai Malware, strumento più utilizzato dai cybercriminali di cui in particolare i ransomware, si stiano consolidando tra le minacce più efficaci per gli attaccanti. Con un'incidenza del 13%, in calo rispetto al 2022 (22%), le tecniche "Unknown"

si trovano in seconda posizione, mentre con una quota del 7% ciascuno chiudono la classifica Phishing/Social Engineering e Web Attacks.
Uno degli elementi di rilevanza allarmante riguarda la Severity degli attacchi, non c'è stata nessuna aggressione con un impatto basso e solo il 7% è stato classificato come medio. Oltre il 90% dei casi ha avuto effetti gravi, di cui tra questi il 60% ricade nella categoria critico, livello massimo della scala di Severity. Poiché l'interruzione dei servizi, come l'accettazione o interventi sanitari e il furto di dati sensibili rappresentano una minaccia significativa, queste situazioni espongono maggiormente le strutture sanitarie a ricatti ed estorsioni

2.6 Settore Manifatturiero

Il settore manifatturiero rappresenta una delle colonne portanti dell'economia italiana, contribuendo in modo significativo alla crescita del PIL, all'occupazione e alla competitività del Paese a livello

internazionale. l'Italia è al quinto posto mondiale per surplus del settore manifatturiero, dietro solamente alla Germania in Europa. Secondo il rapporto "Analisi dei Settori Industriali" di Intesa Sanpaolo Il fatturato dell'industria italiana sia circa sui 1160 miliardi di euro a fine anno 2024. Questo ramo dell'economia del nostro paese, caratterizzato da molteplici aziende, spesso di medie e piccole dimensioni, a cui la crescente digitalizzazione porta ad aumento della superficie di attacco per i cybercriminali. L'integrazione di vecchie infrastrutture con nuove tecnologie, molte volte non supportata da adeguate misure di sicurezza, può lasciare aperte vulnerabilità critiche.

La sua fragilità in certi segmenti e l'importanza economica hanno portato il manifatturiero ad essere la vittima del maggior numero di attacchi informatici a livello nazionale (19%), nei primi sei mesi del 2024, conquistando per la prima volta la vetta dopo essere stato in seconda posizione con il 13% nel 2023. Il peso significativo del manifatturiero italiano a livello internazionale è messo in luce anche dalla differenza con il campione globale degli attacchi per settore, categoria in cui il manifatturiero si posiziona settimo sia ad inizio 2024 che nel 2023, con una percentuale stabile nell'intorno del 5%. Un'altra statistica preoccupante osservando il campione mondiale riguarda l'incidenza delle aggressioni contro aziende manifatturiere italiane, oltre un quarto del totale. Nella tabella sottostante sono riassunti i principali attacchi registrati.

Tipologia Attaccanti	2018	2019	2020	2021	2022	2023	1H 2024	TOTALE
Cybercrime	0	0	8	12	35	41	21	117
Espionage / Sabotage	2	2	1	0	0	0	0	5
Information Warfare	0	0	0	0	0	0	0	0
Hacktivism	0	0	0	0	0	0	1	1
Totale	2	2	9	12	35	41	22	123

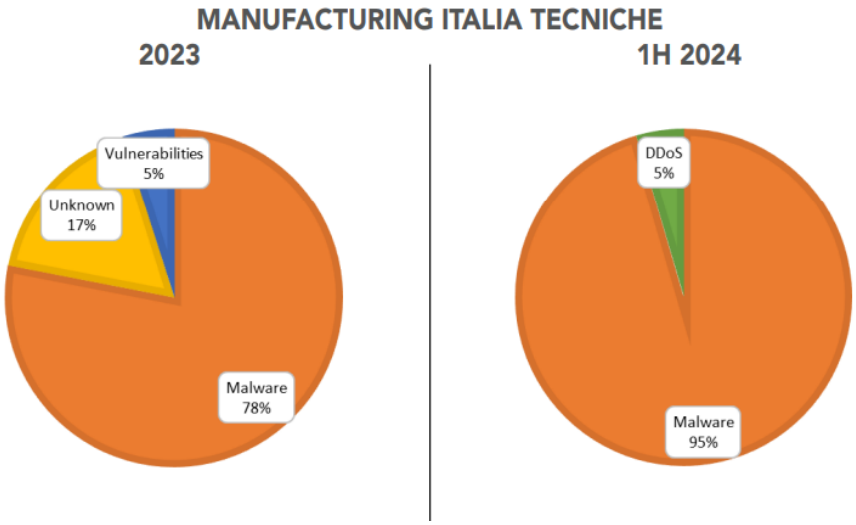
(Tabella 5- di attacchi verso il settore manifatturiero italiano)

Riassumendo le tendenze si può notare che anche per questo settore la pandemia di Covid-19 ha influito nell'adozione rapida e massiccia di strumenti digitali da parte delle aziende, che oltre ai vari benefici tecnologici ha portato a maggiori possibilità di incidenti informatici, accendendo sempre più l'interesse dei cybercriminali, dal 2020 al 2023 gli attacchi registrati sono aumentati più di quattro volte, con il picco tra il 2021 e 2022 dove sono raddoppiati. Nei primi sei mesi del 2024 la situazione sembra stabile, raggiungendo circa la metà del totale dell'anno precedente.

(Figura 27– crescita percentuali degli attacchi verso il manifatturiero)

(Fonte – Clusit)

Il cybercrime rimane la minaccia più significativa per il settore, con un'incidenza che raggiunge quasi il 100% ogni anno, tra i vari motivi, il settore manifatturiero non può permettersi interruzioni prolungate della produzione che possono comportare gravi perdite economiche e rendendo gli operatori del settore più disposti a pagare gli aggressori per riavviare le operazioni. Inoltre, l'interconnessione tra aziende e partner industriali rende il settore manifatturiero ancora più vulnerabile, un singolo attacco può potenzialmente compromettere la supply chain, incentivando ulteriormente i criminali informatici a prendere di mira questo settore.



(Figura 28– tecniche di attacco contro il settore manifatturiero)

(Fonte – Clusit)

Con la tipologia di attaccanti composta quasi esclusivamente da cybercriminali, il Malware (che nella maggior parte dei casi è della tipologia ransomware) è la tecnica di aggressione più utilizzata, arrivando al 95% dei casi ad inizio 2024. Le vulnerabilità conosciute e sconosciute presenti nel 2023 sembrano essere state risolte, non comparendo più in classifica. La presenza dei Ddos può essere associata al fenomeno dell'Hacktivism. Rispetto al panorama globale l'Italia presenta una distribuzione più omogenea con meno varietà di tecniche di attacco.

La Severity degli attacchi nel H1 2024 pare in miglioramento, con la momentanea scomparsa del livello critico, rispetto ad un 30% nel mondo, ma con un 95% nella categoria alto che non deve essere preso alla leggera.

2.7 Conseguenze degli attacchi informatici

Come visto precedentemente, negli ultimi anni, gli attacchi informatici sono diventati un fenomeno sempre più diffuso ed in aumento, l'evoluzione delle tecnologie digitali e la crescente connettività hanno infatti ampliato la superficie esposta a rischi con impatti notevoli sia in termini di costi diretti sia indiretti.

2.7.1 Costi diretti

Gli attacchi informatici generano conseguenze immediate e tangibili, che si manifestano sotto forma di costi diretti.

Queste spese hanno un impatto diretto sulle aziende e sui consumatori, incidendo sia sulle risorse finanziarie che sulle operazioni quotidiane, in caso di violazione con furto di dati sensibili, la priorità è ripristinare l'integrità dei sistemi informatici. Ciò può comportare una serie di attività costose, come l'acquisto di nuovi dispositivi hardware, l'installazione di software di sicurezza e l'assunzione di consulenti interni o esterni per identificare le vulnerabilità.

Secondo il "Global Cybersecurity Outlook" del 2024 del World Economic Forum, il costo medio di una violazione delle informazioni è aumentato del 10%, passando da 4,45 a 4,88 milioni di dollari. Si tratta dell'aumento più significativo dai tempi della pandemia e dimostra come il pericolo e la sofisticazione del crimine informatico si siano evoluti, l'aumento dei costi è dovuto a diversi fattori, primo fra tutti l'interruzione dell'attività, che incide sulla produttività e sulla continuità aziendale.

I costi da sostenere nel post-violazione come il ripristino dei sistemi informatici, il supporto clienti che in caso di informazioni personali rubate potrebbe essere necessario attivare servizi di monitoraggio più eventuali risarcimenti, che vanno poi sommati ai costi legali connessi all'eventuale avvio di procedure giudiziarie. Nelle legislature più avanzate, come quella dell'Unione Europea, vengono fissati standard rigorosi in tema di privacy e trattamento dei dati.

Le imprese che non rispettano questi obblighi e subiscono gravi violazioni rischiano delle costose sanzioni economiche ma spesso accade, una pratica adottata da oltre il 50% delle aziende, l'onere delle perdite economiche viene scaricato sul consumatore, aumentando ulteriormente il costo complessivo per l'economia.

Uno degli aspetti più importanti della fuga di informazioni è il tempo necessario per individuare e contenere un attacco, sempre secondo il World Economic Forum, occorrono in media 292 giorni per rilevare e risolvere una violazione che coinvolge credenziali rubate, un lasso di tempo che espone le aziende a rischi prolungati e a un maggiore impatto economico, anche gli attacchi di phishing e di social engineering, due dei metodi più comuni utilizzati dai criminali informatici, richiedono più tempo per essere rilevati, rispettivamente 261 e 257 giorni. Ciò significa che in molti casi le aziende

vengono a conoscenza di una violazione delle informazioni solo dopo quasi un anno dall'attacco, quando i dati sono già stati rubati e spesso rivenduti sul dark web. Se le autorità vengono coinvolte rapidamente, i tempi di risposta potrebbero ridursi da 297 a 281 giorni, con un risparmio medio di 1 milione di dollari in costi di gestione degli incidenti, a dimostrazione che la cooperazione tra pubblico e privato può mitigare gli effetti degli attacchi e ridurne l'impatto economico. Nel caso dei ransomware, la questione se pagare o meno per riavere i dati è spesso un problema non da poco, pagare un riscatto può sembrare una soluzione rapida, ma presenta diversi rischi. Da un lato, non vi è alcuna garanzia che i criminali restituiscano l'accesso al sistema dopo aver ricevuto il denaro e, dall'altro, il pagamento del riscatto può incoraggiare ulteriori attacchi. Pertanto, il pagamento di un riscatto è una spesa immediata e importante, che non risolve alla radice la vulnerabilità della rete aziendale e in ogni caso non esime l'azienda dalla necessità di adottare misure di sicurezza adatte, comprendere la portata di tali spese e monitorare costantemente i rischi associati è un passo importante verso l'adozione di misure preventive efficaci.

2.7.2 Costi indiretti

Oltre all'insieme di perdite nel breve periodo e quantificabili, esiste un insieme di costi più difficili da misurare eppure estremamente rilevanti, i costi indiretti. Essi intaccano la competitività, la stabilità e la stessa percezione dell'azienda nel lungo periodo, con ripercussioni che possono durare ben oltre la conclusione dell'incidente.

Uno degli elementi più sensibili dei costi indiretti è il deterioramento della credibilità dell'azienda. Quando un cliente scopre che i suoi dati personali sono stati sottratti o compromessi, la prima conseguenza è la perdita di fiducia nell'impresa. In un mercato sempre più orientato al digitale, la reputazione è un asset prezioso e può bastare un singolo incidente per incrinarla. L'eventualità che l'organizzazione subisca un nuovo attacco in futuro diventa più concreta agli occhi del pubblico, spingendo i consumatori a rivolgersi altrove. Recuperare la credibilità richiede solitamente investimenti in campagne di comunicazione e trasparenza. Il danneggiamento della reputazione non riguarda solo la clientela, anche partner e fornitori possono reagire negativamente, temendo eventuali danni a catena sia economici che di immagine. Dopo aver subito un attacco, solitamente l'azienda deve dirottare parte delle risorse destinate a progetti di sviluppi futuri sulla messa in sicurezza dei sistemi e sulla gestione dell'emergenza. Rischiando di perdere terreno rispetto alla concorrenza, con eventuali perdite di clientela e quote di mercato che possono portare ad un ulteriore aggravarsi della situazione. Un elemento spesso sottovalutato è l'effetto sull'ambiente di lavoro, si può creare un clima

teso tra il personale, specialmente se la violazione sia avvenuta per negligenza o errore umano. Con il possibile scaturirsi di conflitti interni peggiorando il clima aziendale e la qualità della vita lavorativa. Investimenti in formazione o consulenza possono aiutare a mitigare la situazione.

2.8 Tendenze future del rischio cibernetico

La sicurezza informatica è diventata un pilastro fondamentale per la stabilità economica e sociale di ogni Paese. Con l'accelerazione della digitalizzazione e l'adozione massiccia di nuove tecnologie, il panorama delle minacce è destinato a evolversi rapidamente e a presentare sfide inedite.

L’adozione sempre più diffusa in tutti i settori di dispositivi IoT (internet of things), cioè la connessione di oggetti fisici a Internet, permettendo loro di raccogliere, scambiare ed elaborare dati senza l’intervento umano, e l’espansione della connettività a livello globale con il 5G e sistemi satellitari come Starlink, che consentiranno una connettività ad alta velocità e più capillare, porterà ad aumentare considerevolmente la superfice d’attacco disponibile per i cybercriminali. Sarà importante sviluppare questi sistemi non solo in ottica di standardizzazione e contenimento dei costi, ma anche in prospettiva di cyber resilienza.

L’intelligenza artificiale (IA) sta già trasformando molte aree, dalla sanità alla manifattura, migliorando i processi aziendali e l’analisi dei dati. Sul fronte della sicurezza cibernetica, però, emergono due dinamiche parallele. L’IA potrà essere utilizzata come strumento difensivo tramite sistemi di machine learning e reti neurali in grado di identificare anomalie nel traffico di rete e prevenire intrusioni, rilevando attività malevole con maggiore tempestività. O come strumento offensivo, i criminali informatici possono sfruttare algoritmi sofisticati per automatizzare la ricerca di vulnerabilità, generare campagne di phishing personalizzate capaci di risultare sempre più autentiche o sviluppare malware in grado di mutare il proprio comportamento. Queste due dinamiche porteranno ad un continuo aggiornamento delle tecniche di difesa e di attacco.

La competizione a livello globale per la supremazia tecnologica e l’accesso alle risorse digitali ha da tempo generato uno scenario di guerra ibrida, in cui gli attacchi informatici diventano un’arma strategica. Questa tendenza non sembra rallentare per il futuro, e saranno necessari accordi internazionali, con regole sulla sicurezza condivise e un maggiore scambio di informazioni tra governi per cercare di arginare gli attacchi.

Un’altra frontiera tecnologica, al momento ancora in fase iniziale di sviluppo, ma che già incide e inciderà sempre di più sul rischio cibernetico del futuro è il quantum computing. I computer quantistici potrebbero raggiungere in futuro una potenza di calcolo tale per cui molte delle tecniche di protezione dei dati utilizzate oggi, che i computer tradizionali impiegherebbero migliaia o milioni di anni per decifrare queste protezioni, diventeranno obsolete. Uno degli scenari attuali più preoccupanti è quello definito "Harvest Now, Decrypt Later" (Raccogli ora, decifra dopo), questo concetto si basa su una strategia adottata da cybercriminali e attori statali, che consiste nel rubare e archiviare grandi quantità di dati cifrati, con l’intento di decriptarli in futuro non appena la tecnologia quantistica sarà sufficientemente sviluppata. Il rischio risulta grave per molte informazioni sensibili, che rimangono invariate negli anni, come dati anagrafici e identificativi. Per fronteggiare questa minaccia, la comunità scientifica sta sviluppando nuovi algoritmi crittografici resistenti ai computer quantistici, noti come crittografia post-quantistica, i preparativi devono iniziare con largo anticipo per evitare una corsa all’ultimo minuto quando la minaccia quantistica diventerà reale.

3. Modelli di mercato

In questo capitolo verranno costruiti dei modelli di mercato a tre versanti, evidenziandone i presupposti e le implicazioni principali. Vedremo come si definiscono e interagiscono i tre attori prescelti (impresa, consumatore e hacker), analizzandone i ruoli e le dinamiche di influenza reciproca.

3.1 Teoria dei giochi: concetti base

La teoria dei giochi è una branca della matematica applicata che studia le decisioni strategiche di più soggetti che interagiscono tra di loro. In situazioni dove le scelte di un "*giocatore*" influenzano direttamente i risultati ottenuti dagli altri, la teoria dei giochi diventa uno strumento per comprendere e prevedere comportamenti, e per progettare meccanismi di incentivazione adeguati.

Elementi fondamentali di un modello sono i giocatori, le strategie e i payoff. I giocatori sono i decisori razionali coinvolti nel gioco. Ogni giocatore si presume abbia obiettivi definiti, tendenzialmente volti a massimizzare (o minimizzare) una funzione di utilità o di payoff. Una strategia è un piano d'azione a disposizione di un giocatore, definendo come egli agirà in ogni possibile situazione contemplata dal gioco. Il payoff (detto anche utilità) misura il risultato ottenuto da un giocatore, sulla base della combinazione di strategie adottate da tutti i giocatori. Può trattarsi di un valore monetario, ma anche di qualunque misura di benessere o preferenza.

I giochi possono essere cooperativi, quando i giocatori possono stringere alleanze vincolanti e coordinare le proprie azioni per ottenere risultati condivisi. L'analisi si concentra sui modi di formare coalizioni e di distribuire il valore generato dalla cooperazione. Oppure non cooperativi, ogni giocatore agisce per conto proprio e non esistono accordi vincolanti che possano costringere i giocatori a collaborare.

Anche le informazioni a disposizione hanno forme diverse, se i giocatori conoscono perfettamente la struttura del gioco si tratta di informazione completa, se invece alcuni parametri non sono noti a tutti è incompleta.

Un concetto cardine della teoria dei giochi è l'equilibrio di Nash, definito come un insieme di strategie, una per ciascun giocatore, tali che nessuno ha incentivo a deviare unilateralmente dalla propria strategia, dati i piani d'azione degli altri. Rappresenta una configurazione stabile nella quale, se gli altri giocatori mantengono la loro strategia, ogni singolo giocatore ottiene il proprio massimo payoff possibile, restando con la strategia attuale.

Un esempio classico è quello del Dilemma del Prigioniero, due individui arrestati per un crimine vengono interrogati separatamente. Ciascuno ha la possibilità di confessare o di rimanere in silenzio. Se entrambi tacciono, ricevono una pena lieve, se uno confessa e l'altro no, il primo ottiene un beneficio maggiore e il secondo subisce una pena più dura. Se confessano entrambi, ricevono una

condanna intermedia. L'analisi mostra che l'unico equilibrio di Nash è che entrambi confessino, pur essendo un esito subottimale per la coppia.

3.2 Modello di mercato a tre versanti

In un tradizionale modello di mercato a due versanti, l'interazione principale avviene tra imprese e consumatori, dove le prime offrono beni o servizi e i secondi li acquistano. Con l'evoluzione del panorama digitale e l'emergere di nuove dinamiche economiche, per questa tesi si è deciso di aggiungere un terzo attore, l'hacker, costruendo un modello teorico più complesso e articolato. Il mercato a tre versanti può offrire una prospettiva dell'economia digitale moderna. Le interazioni tra i tre giocatori e le loro decisioni influenzano la sicurezza e il profitto finale tramite diverse dinamiche. I tre attori principali del modello possono essere definiti:

Impresa: le imprese offrono servizi e prodotti, rappresentano sia il principale bersaglio degli attacchi che il principale investitore in misure di difesa. Le aziende variano in termini di vulnerabilità soprattutto a seconda delle loro dimensioni e del livello di digitalizzazione. Il loro obiettivo è quello di minimizzare i costi totali (costi della cybersecurity e danni dagli attacchi) e massimizzare i profitti derivanti dai consumatori.

Consumatore: Il consumatore, è il destinatario finale dei beni e servizi, pur non essendo l'obiettivo primario in molti casi, soffre le conseguenze di attacchi rivolti alle imprese. Il loro obiettivo è massimizzare la propria utilità minimizzando i costi e i rischi.

Hacker: criminali informatici, che tramite l'utilizzo in modo illegale di strumenti tecnologici hanno l'obiettivo di sfruttare le vulnerabilità del sistema per ottenere guadagni economici minimizzando i propri costi e sforzi.

Le strategie di rilievo per i giocatori sono, per le imprese la scelta del livello di investimenti in cybersecurity, che aumenta i costi diretti ma riduce le probabilità di attacco incrementando la fiducia dei consumatori che può portare a maggiori ricavi. I consumatori scelgono quale prodotto o servizio acquistare in base al proprio livello di utilità che dipende sia dai benefici del consumo che dal rischio percepito di attacchi. Infine, gli hacker decidono quali obiettivi colpire, con lo scopo di massimizzare il proprio guadagno in caso di attacco riuscito, tenendo conto del costo dell'aggressione ed i rischi connessi ad essa.

Le azioni di un giocatore possono avere degli effetti, detti esternalità, che influenzano il comportamento degli altri giocatori. Le esternalità possono essere positive quando la strategia di un giocatore migliora i payoff anche degli altri. Ad esempio, un'impresa che effettua ingenti investimenti nella sicurezza informatica non solo tutela i propri sistemi, ma contribuisce indirettamente alla

protezione dei consumatori e altre imprese con cui interagisce. Questi benefici, non essendo esclusivamente sfruttati dall'impresa che compie l'investimento, essa potrebbe non essere incentivata ad investire al livello ottimale dal punto di vista collettivo, portando a situazioni di inefficienza economica o fallimenti di mercato.

Le esternalità sono invece negative quando le azioni di un giocatore peggiorano il payoff degli altri. Nella sicurezza informatica, se un'impresa non investe a sufficienza nella protezione dei propri sistemi incrementa il rischio anche per le altre imprese e consumatori con cui è interconnessa.

Gli effetti delle esternalità non sono uguali per tutti gli attori presenti nel modello, un aumento degli investimenti nella sicurezza dei sistemi informatici ha risultati positivi sui consumatori che interagiscono con l'azienda, ma ha ripercussioni negative per gli hacker che devono aumentare le proprie risorse per avere successo nell'attacco.

I modelli economici disponibili nella letteratura riguardante gli investimenti in sicurezza informatica e del loro impatto sul welfare collettivo sono molteplici e ramificati. Una delle possibili suddivisioni, effettuata da Fedele e Roner è la seguente:

Indipendenza delle imprese, rappresenta il caso più semplice, discusso da Gordon e Loeb (2002), si considera la presenza di un'unica impresa che valuta autonomamente il livello ottimale di risorse da destinare alla sicurezza informatica, assumendo l'indipendenza di questa scelta rispetto a possibili fattori esterni.

Interdipendenza strutturale, tramite le ricerche effettuate da Kunreuther e Heal (2003) e Varian (2004), vengono indagati scenari in cui più aziende operano attraverso strutture informatiche condivise, ma non sono in concorrenza sul mercato dei servizi o prodotti. La presenza di una infrastruttura condivisa crea un'esternalità positiva detta spillover tecnico, in cui ogni attore trae vantaggio dagli investimenti effettuati dagli altri membri dello stesso sistema. In questo scenario alcune imprese potrebbero decidere di non investire in sicurezza, sfruttando le misure adottate dagli altri partecipanti alla rete, creando il fenomeno del free riding.

Interdipendenza di mercato, con gli studi presentati da Garcia e Horowitz (2007), vengono esaminati i casi in cui le aziende operano su strutture informatiche indipendenti ma competono nello stesso mercato. Ogni azienda, quindi, determina in maniera indipendente il proprio livello ottimale di risorse da utilizzare per la sicurezza informatica, non potendo beneficiare di investimenti comuni.

3.3 Il modello con indipendenza

Funzione dell'impresa

Gli studi sugli investimenti in sicurezza informatica, in assenza di forme di interdipendenza, rappresentano una delle prime e basilari aree di ricerca nell'ambito della cybersicurezza, viene analizzato il processo decisionale delle singole aziende riguardo al livello ottimale di misure di cybersicurezza, esaminando le scelte effettuate in modo indipendente, senza tenere conto dell'influenza o delle conseguenze derivanti dalle decisioni di altre aziende.

In questo ambito, il modello sviluppato da Gordon e Loeb (2002) rappresenta uno dei primi contributi di rilievo. Il suo scopo è quello di offrire una struttura teorica per comprendere come un'azienda possa determinare l'ammontare ottimale da investire in sicurezza informatica, valutando esclusivamente i propri rischi e vantaggi senza considerare fattori esterni come gli spillover. Grazie alla sua chiarezza e facilità di applicazione, questo modello si è affermato come un riferimento nel settore, ponendo le basi per successive ricerche volte ad approfondire le dinamiche più articolate legate alle interdipendenze tra imprese, l'azienda considerata nel modello è neutrale al rischio e deve determinare il livello ottimo di risorse da destinare alla propria protezione digitale.

Per la creazione di un modello di mercato a tre versanti imprese-hacker-consumatori è stata utilizzata come base di partenza la funzione di profitto delle imprese del modello matematico di Gordon e Loeb, dove vengono definiti i seguenti parametri: (i) X è il valore delle informazioni dell'impresa, definite anche come i suoi ricavi; (ii) $v \in [0,1]$ è la probabilità di successo di un cyberattacco (iii) a$\in[0,1]$ è la quota dei ricavi a rischio, con aX la perdita dovuta ad un attacco compiuto con successo. La probabilità di essere colpiti da un attacco informatico viene assunta, per semplicità e senza compromettere la generalità dell'analisi, come pari a 1. L'azienda decide dunque il livello di investimento in cybersicurezza I≥0 per diminuire la probabilità di riuscita dell'attacco v.

La probabilità che un attacco informatico abbia successo dopo l'investimento in cybersicurezza è determinata dalla funzione $\pi(I, v) \in [0, v]$ e presenta le seguenti 3 assunzioni:

A1: $\pi(I, 0)=0$;

A2: $\pi(0, v) = v$;

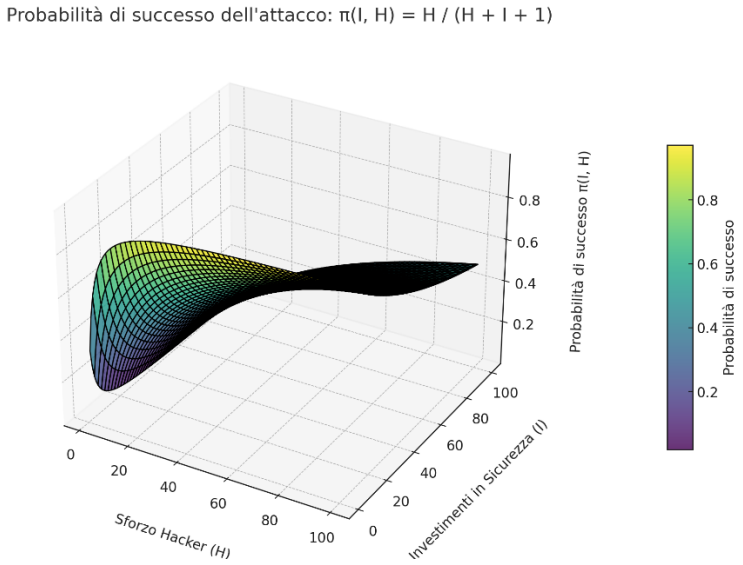
A3: π è due volte derivabile e continua rispetto a I e $0 < v < 1$:

$$\frac{\partial \pi(I,v)}{\partial I} < 0, \quad \frac{\partial^2 \pi(I,v)}{\partial I^2} > 0, e \lim_{I \to \infty} \pi(I,v) = 0$$

All'aumentare degli investimenti in sicurezza il livello di protezione cresce ma con un'efficacia che si riduce progressivamente, e si assume che dopo un certo livello di investimenti in sicurezza il rischio di una violazione possa essere ridotto vicino a zero.
La funzione di utilità dell'impresa può quindi essere espressa nella seguente forma:

$$max_{I\geq 0}\{R(I) - I\} = \{X - [\pi(I, v)]aX - I\}$$

E per ottenere una soluzione chiusa della funzione all'ottimo è stata considerata la seguente forma esplicita di probabilità, che rispetta le assunzioni A1-A3, $\pi(I, v) = \frac{v}{I+1}$.
Il modello di Gordon e Loeb appena descritto, si concentra esclusivamente sull'impresa, senza considerare il ruolo degli hacker e dei consumatori. Per estendere il modello ed includere anche questi due attori, sono state apportate delle modifiche alla struttura originale, adattando la funzione di profitto in modo da rappresentare le dinamiche di interazione tra impresa, hacker e consumatori all'interno di un modello di mercato a tre versanti.
La vulnerabilità v è stata sostituita con una vulnerabilità che tiene in considerazione lo sforzo o investimento dell'attacco dell'hacker H, e diventa $v(H)$, ed i costi sono stati cambiati da lineari a quadratici per rendere il sistema di equazioni più flessibile. Questo cambiamento fa sì che la derivata rispetto ad I sia I anziché una costante, come nel caso lineare, dove la derivata è 1, consentendo così un maggior numero di soluzioni interne ed un equilibrio meno rigido.
Per utilizzare una forma esplicita di probabilità $\pi(I, v(H))$, rispettando sempre le assunzioni A1-A3, è stata utilizzata una funzione simile a quella mostrata precedentemente nel modello di Gordon e Loeb, con la probabilità di successo di un attacco che si modifica in: $\pi(I, v(H)) = \frac{\mathrm{H}}{\mathrm{I+H+1}}$ e $v(H) = \frac{H}{H+1}$.



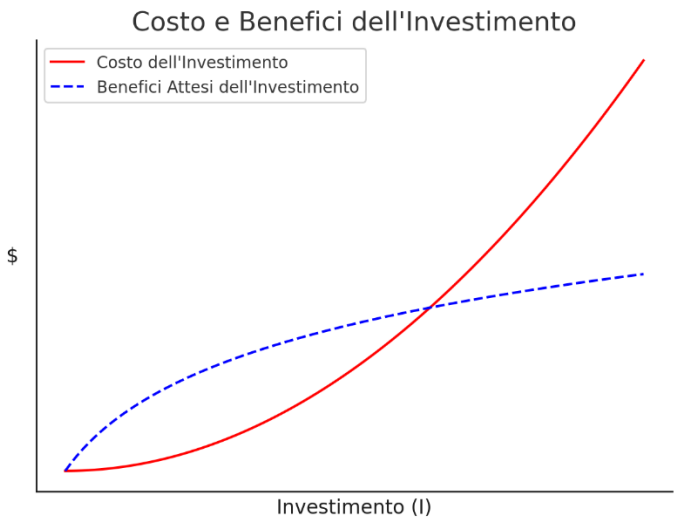
(Grafico 3 – andamento probabilità di attacco al variare di I e H)

La funzione di utilità dell'impresa per il modello di mercato a tre versati diventa quindi:

$$U_I = X - \frac{H}{I + H + 1} aX - \frac{1}{2} I^2$$

La condizione del primo ordine (FOC) per l'azienda è:

$$\frac{\partial U_I}{\partial I} = \frac{H}{(I + H + 1)^2} aX - I$$



(Grafico 4 – Analisi costi benefici per l'impresa)

L'andamento dei costi e benefici attesi dall'impresa in funzione dell'investimento I è composto da due curve, la curva rossa rappresenta il costo dell'investimento, cresce in modo convesso, indicando che i costi aumentano più rapidamente man mano che l'impresa investe maggiori risorse, proteggere

i primi livelli di vulnerabilità è relativamente economico, ma rendere un sistema completamente sicuro diventa progressivamente più oneroso. La curva blu invece, mostra i benefici attesi, che inizialmente aumentano rapidamente per poi tendere a stabilizzarsi, dato dai rendimenti decrescenti dell'investimenti I. Il punto di intersezione rappresenta l'equilibrio ottimale per l'impresa, ovvero il livello di investimento in cui i benefici marginali ottenuti dalla cybersicurezza compensano esattamente i costi marginali sostenuti dall'impresa.

Funzione dell'hacker

Per incorporare l'hacker nel modello, supponiamo che egli possa decidere quanto sforzo o investimento H impiegare nell'attacco, ed analogamente all'impresa, l'hacker agisce razionalmente con l'obiettivo di massimizzare il proprio guadagno atteso, che dipende dalla probabilità di successo dell'attacco e dal valore delle risorse sottratte, al netto dei costi sostenuti. La funzione di utilità dell'hacker deve quindi tenere conto di questi elementi, bilanciando il ritorno economico derivante da un attacco riuscito con il costo dello sforzo necessario per violare il sistema di sicurezza dell'impresa.

L'hacker ottiene un beneficio aX per ogni attacco riuscito e sostiene un costo C(H), con C′(H)> 0 e C″(H)> 0, in modo da rappresentare che un maggior sforzo dell'hacker, aumenti il costo sostenuto e che dopo il raggiungimento di una certa soglia H, investimenti aggiuntivi producono ritorni marginali decrescenti.

La sua funzione di utilità può essere definita come:

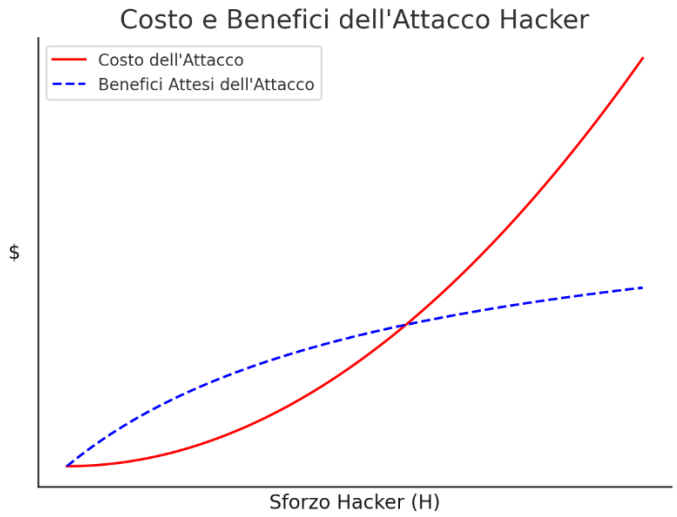
$$U_H = \pi(I, v(H))aX - C(H)$$

La probabilità di successo di un attacco $\pi(I, v(H))$ è stata definita precedentemente con $\pi(I, v(H)) = \frac{\mathrm{H}}{\mathrm{I+H+1}}$ mentre una funzione C(H) che rispetta le assunzioni fatte è $C(H) = H^2$ funzione crescente, positiva e convessa, ed esplicitando questi parametri la funzione U_H diventa:

$$U_H = \frac{H}{I + H + 1}aX - H^2$$

E la condizione del primo ordine (FOC) è:

$$\frac{\partial U_H}{\partial H} = \frac{(I + 1)}{(I + H + 1)^2}aX - 2H$$



(Grafico 5 - Analisi costi benefici per l'hacker)

L'andamento dei costi benefici per l'hacker in funzione del suo sforzo è simile a quello delle imprese, ma in modo leggermente più ripido data la diversa modellazione dei costi nelle funzioni di utilità, e riflette il fatto che aumentare l'intensità di un attacco diventa progressivamente più oneroso, a causa della necessità di competenze e strumenti avanzati. Il punto di intersezione rappresenta sempre l'equilibrio ottimo dello sforzo hacker, ovvero il livello in cui i guadagni marginali dell'attacco sono uguali ai costi marginali sostenuti dall'hacker.

Funzione dei consumatori

Per inserire nel modello i consumatori, si può considerare che il loro beneficio deriva dall'utilizzo del prodotto o servizio offerto dall'impresa, ma è anche condizionato dal livello di sicurezza garantito. Dato che una maggiore sicurezza riduce la probabilità di violazioni e conseguenti rischi per i consumatori, il loro livello di utilità dipenderà sia dalla qualità del servizio ricevuto sia dalla protezione delle informazioni personali, di conseguenza, il loro processo decisionale sarà influenzato non solo dalle caratteristiche intrinseche del prodotto, ma anche dalla percezione della sicurezza offerta dall'impresa. Si possono definire i seguenti parametri: (i) U_0 è l'utilità di base del consumatore derivante dal prodotto o servizio dell'impresa; (ii) $U_1(I)$ rappresenta il beneficio reputazionale o la maggiore fiducia/utilità del consumatore dovuta a un maggiore investimento in sicurezza, con $U_1'(I)>0$ ed $U_1''(I)<0$ per rappresentare i benefici aggiuntivi che diventano sempre più marginali; (iii) $L>0$ è un parametro che misura il danno, in termini di perdita di fiducia o di utilità per i consumatori in caso di attacco riuscito contro un'impresa; (iv) $C \geq 0$ è un parametro che rappresenta l'aumento della complessità di utilizzo per gli utenti all'aumentare della sicurezza, dato che, oltre un certo livello, la sicurezza informatica per i consumatori può essere considerata adeguata, tuttavia, ulteriori

incrementi di cybersicurezza richiedono l'adozione di sistemi sempre più complessi, ad esempio, sistemi con standard militari o tecnologie altamente sofisticate, che risultano poco utili o controproducenti per l'utente finale, inoltre assicura che la derivata parziale della funzione di utilità del consumatore rispetto a I possa annullarsi a un valore finito di I, consentendo l'esistenza di un equilibrio di Nash interno.

Utilizzando sempre la stessa probabilità di successo di un attacco e definendo $U_1(I) = \ln(1+I)$ che è una funzione crescente positiva e concava per riflettere il fatto che dopo un certo livello ulteriori investimenti in sicurezza non migliorano più in modo significativo l'utilità dei consumatori. La funzione di payoff dei consumatori può essere scritta come:

$$U_C = U_0 + \ln(1+I) - L\frac{H}{I+H+1}aX - CI$$

La cui condizione del primo ordine (FOC) è:

$$\frac{\partial U_C}{\partial I} = \frac{1}{I+1} + L\frac{H}{(I+H+1)^2}aX - C$$

EQUILIBRIO OTTIMO A SISTEMA

Per determinare l'equilibrio ottimale dell'investimento in cybersicurezza da parte dell'impresa e dello sforzo dell'hacker, è necessario risolvere il sistema di equazioni che deriva dalle condizioni del primo ordine (FOC) delle tre funzioni di utilità: impresa, hacker e consumatore. L'interazione tra questi tre attori è strategica, poiché le decisioni di ciascuno influenzano direttamente i ritorni e i costi degli altri. L'impresa sceglie il livello di investimento I in cybersicurezza bilanciando i costi sostenuti con la riduzione del rischio di attacco, mentre l'hacker decide lo sforzo H in base alla probabilità di successo e ai benefici attesi. Il consumatore, d'altro canto, è influenzato dalla sicurezza del sistema, valutando i benefici di una maggiore protezione rispetto alle complessità derivanti dall'implementazione di misure più sofisticate.

L'equilibrio si ottiene risolvendo congiuntamente le tre condizioni del primo ordine, trovando i valori ottimali di investimento e sforzo hacker che rendono massime le rispettive funzioni di utilità.

$$\begin{cases} U_I = X - \dfrac{H}{I+H+1}aX - \dfrac{1}{2}I^2 \\ U_H = \dfrac{H}{I+H+1}aX - H^2 \\ U_C = U_0 + \ln(1+I) - L\dfrac{H}{I+H+1}aX - CI \end{cases}$$

L'equilibrio ottimo è definito dai valori (I^*, H^*) che soddisfano contemporaneamente le tre FOC:

$$\begin{cases} \dfrac{H}{(I+H+1)^2} aX = I \\ \dfrac{(I+1)}{(I+H+1)^2} aX = 2H \\ \dfrac{1}{I+1} + L\dfrac{H}{(I+H+1)^2} aX = +C \end{cases}$$

Risolvendo il sistema risulta:

$$\begin{cases} I^* = \dfrac{C - L + \sqrt{(L+C)^2 - 4L}}{2L} \\ H^* = \sqrt{\dfrac{I^*(I^*+1)}{2}} \end{cases}$$

H^* è determinato dall'equilibrio tra la strategia dell'hacker e la risposta della sicurezza aziendale, tenendo conto che maggiori investimenti in sicurezza rendono più costoso e meno probabile il successo di un attacco.

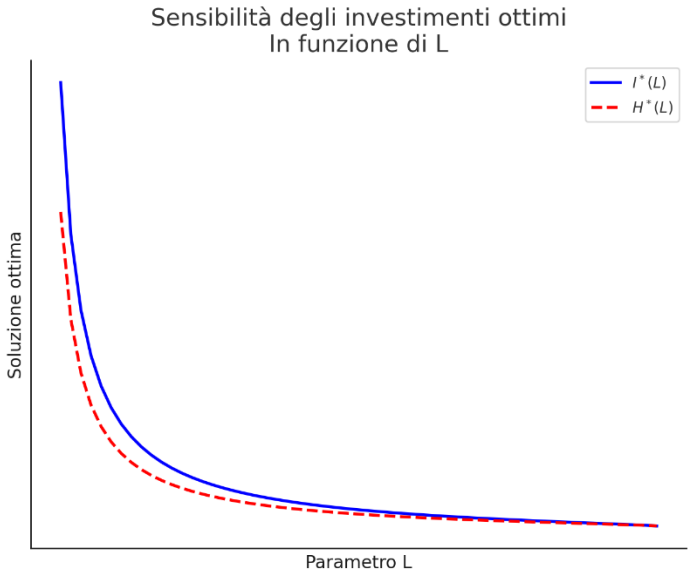
L'investimento in sicurezza I^* (dato dalla soluzione positiva della quadratica) significa che l'impresa decide il livello di sicurezza fino al punto in cui il risparmio in termini di riduzione del danno dell'attacco e della conseguente perdita di utilità e costi del consumatore compensa il costo aggiuntivo dell'investimento.

Il punto di intersezione (I^*, H^*) rappresenta un equilibrio di Nash tra i tre attori, in cui nessuno ha un incentivo a deviare unilateralmente, infatti, l'impresa non migliora la propria utilità modificando I se l'hacker risponde con H^*, l'hacker non può ottenere un maggior guadagno cambiando H dato il livello I^* di sicurezza e il consumatore attraverso i suoi costi benefici fissa indirettamente il livello I^* che influenza l'intero equilibrio.

L'impresa sceglie quindi I per minimizzare il rischio (ossia ridurre $\pi(I, v(H))$) e proteggere il proprio valore aX e la propria reputazione, bilanciando il costo I crescente con il risparmio atteso dalle possibili perdite.

L'hacker decide il proprio sforzo H per aumentare la probabilità di successo dell'attacco, bilanciando il beneficio aX ottenuto in caso di successo con il costo dell'attacco.

I consumatori valutano il prodotto/servizio non solo in funzione della propria utilità di base, ma anche della sicurezza offerta, maggiore I implica minori rischi e maggior fiducia, ma può anche comportare un trasferimento a carico del consumatore di ulteriori complessità.



(Grafico 6 – andamento soluzioni ottime al variare di L)

Il parametro L misura quanto un attacco riuscito danneggia l'utilità o la fiducia del consumatore, e ci si potrebbe aspettare che un valore più alto di L dovrebbe spingere a maggiore sicurezza, ma nell'equilibrio di mercato tra impresa, consumatore e hacker se L cresce aumenta il rischio percepito dal consumatore e ciò può portarlo a ridurre la domanda. Le imprese invece, non investono in sicurezza solo per proteggere il consumatore, ma per anche massimizzare i propri profitti in un mercato dove il consumatore ha il controllo sulla domanda. Con l'utilità dei consumatori che diminuisce all'aumentare di L le imprese hanno meno convenienza ad incrementare gli investimenti I, che aumentando la complessità di utilizzo per il consumatore diminuisce ancora di più la sua utilità. In conclusione, un valore di L più alto rende il consumatore più sensibile al rischio, riducendo la redditività potenziale per l'impresa e, di riflesso, l'interesse dell'hacker. Ne risulta un equilibrio in cui sia I^* che H^* si abbassano.

Per attenuare l'impatto negativo di L, le imprese potrebbero adottare una serie di strategie volte a mitigare il danno percepito. Ad esempio, una comunicazione chiara e trasparente sulla qualità delle misure di cybersicurezza implementate può contribuire a rafforzare la fiducia dei consumatori, evidenziando come i sistemi adottati siano efficaci e continuamente aggiornati, insieme a campagne pubblicitarie che evidenziano il valore della protezione offerta possono ridurre la percezione del rischio, migliorando così la soddisfazione e la fedeltà del cliente. Un ulteriore strategia utile potrebbe essere l'adozione di polizze assicurative, che offrano una rete di sicurezza in caso di attacchi riusciti, attenuando in questo modo l'impatto diretto dei danni e riducendo l'effetto negativo sul mercato. In questo modo, l'impresa non solo si prepara ad affrontare le eventuali perdite, ma contribuisce anche a creare un ambiente di maggiore fiducia, che a sua volta incentiva una domanda più stabile e un miglioramento complessivo dell'efficienza di mercato.

3.4 Il modello con Interdipendenze strutturali

Gli studi sulle interdipendenze strutturali riguardano le imprese che non agiscono in maniera indipendente, ma sono interconnesse tra di loro tramite strutture digitali condivise. L'investimento di un'azienda non porta benefici solo a sé stessa, ma anche alle altre imprese che operano all'interno della stessa struttura digitale. Tali effetti definiti come spillover tecnici, generano la possibilità di free riding, dato che ogni azienda trae vantaggio dagli investimenti in sicurezza, potrebbero essere incentivate a limitare le proprie risorse destinate alla sicurezza e utilizzando le difese fornite dalle altre imprese. Questa decisione strategica rischia di portare a un livello di investimenti in cybersicurezza inferiore a quello socialmente ottimale, che senza un'adozione di misure adeguate, può generare un fallimento di mercato.

Funzione dell'impresa

Fedele e Roner per l'esistenza di interdipendenze strutturali hanno sviluppato un modello teorico per analizzare le decisioni di investimento in sicurezza informatica delle imprese, neutrali al rischio, in relazione ai benefici condivisi dall'utilizzo della stessa struttura informatica, definendo i seguenti parametri: (i) X è il valore delle informazioni dell'impresa, definite anche come i suoi ricavi; (ii) $v \in [0,1]$ è la probabilità di successo di un cyberattacco; (iii) a$\in[0,1]$ è la quota dei ricavi a rischio, con aX perdita dovuta ad un attacco compiuto con successo; (iv) N numero di aziende che utilizzano la stessa struttura digitale condivisa. La probabilità di essere colpiti da un attacco informatico viene assunta, per semplicità e senza compromettere la generalità dell'analisi, come pari a 1. L'impresa decide dunque il livello di investimento in cybersicurezza I$\geq$0 per ridurre la probabilità di riuscita dell'attacco v. La probabilità che un attacco informatico abbia successo dopo l'investimento in cybersicurezza è determinata dalla funzione $\pi(I, v)$ che presenta le stesse assunzioni adottate nel modello di Gordon e Loeb, e presenta la seguente struttura:

$$\pi(I, v) = \frac{v}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + 1}$$

Il parametro e $\in [0,1]$ introdotto rappresenta il livello di interdipendenza strutturale, se è uguale a zero la funzione di probabilità risulta uguale al caso di indipendenza descritto precedentemente, se invece è uguale a 1 gli spillover tecnici sono al loro valore massimo, la funzione di profitto dell'impresa diventa quindi:

$$max_{I_i \geq 0}\{R_S(I_1, \dots, N) - I_i\} = X - \frac{v}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + 1} aX - I_i$$

Con questa configurazione, si rappresenta l'assunzione che l'investimento in sicurezza di un'azienda non solo diminuisce il rischio di un attacco per sé stessa, ma contribuisce anche a ridurre la probabilità di attacco per tutte le altre imprese connesse alla stessa struttura. E nella risoluzione della funzione per trovare l'equilibrio di Nash si considerano le imprese simmetriche, con $I_i = I_j = I$.

Anche il modello di Fedele e Roner appena descritto, si concentra esclusivamente sulle imprese, senza considerare il ruolo degli hacker e dei consumatori. Per estendere il modello ed includere anche questi due attori, sono state apportate delle modifiche alla struttura originale, adattando la funzione di profitto in modo da rappresentare le dinamiche di interazione tra imprese, hacker e consumatori all'interno di un modello di mercato a tre versanti.

La vulnerabilità v è stata sostituita con una vulnerabilità che tiene in considerazione lo sforzo o investimento dell'attacco dell'hacker H, e diventa $v(H)$, ed i costi sono stati cambiati da lineari a quadratici per rendere il sistema di equazioni più flessibile.

Per utilizzare una forma esplicita di probabilità $\pi(I, v(H))$, rispettando sempre le assunzioni del modello di Gordon e Loeb, la probabilità di successo di un attacco è stata modificata in: $\pi(I, v(H)) = \frac{H}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + H + 1}$ e $v(H) = \frac{H}{H+1}$.

La funzione di utilità delle imprese per il modello di mercato a tre versati diventa quindi:

$$U_I = X - \frac{H}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + H + 1} aX - \frac{1}{2} {I_i}^2$$

Considerando, come nel modello di Fedele e Roner, un mercato simmetrico in cui $I_i = I_j = I$, la funzione si modifica:

$$U_I = X - \frac{H}{I + eI(N-1) + H + 1} aX - \frac{1}{2} \mathrm{I}^2$$

E la condizione del primo ordine (FOC) dell'impresa per l'equilibrio di Nash simmetrico è:

$$\frac{\partial U_I}{\partial I} = \frac{H(1 + e(N-1))}{(I + eI(N-1) + H + 1)^2} aX - \mathrm{I}$$

E confrontandola con la FOC del modello con indipendenza dove $\frac{\partial U_I}{\partial I} = \frac{H}{(I+H+1)^2} aX - I$ risulta che $\frac{H(1+e(N-1))}{(I+eI(N-1)+H+1)^2} aX < \frac{H}{(I+H+1)^2} aX$ per qualsiasi valore di $e > 0$, la presenza di spillover tecnici quindi genera quindi il free-riding, che aumenta all'aumentare del valore di e. Anche il numero N delle imprese presenti incrementa il free-riding e il conseguente fallimento di mercato.

Funzione dell'hacker

Per incorporare l'hacker nel modello con interdipendenze strutturali, sono state utilizzate le stesse assunzioni del modello con indipendenza. L'hacker deve quindi bilanciare il ritorno economico derivante da un attacco riuscito con il costo dello sforzo necessario per violare il sistema di sicurezza dell'impresa. La sua funzione di utilità può essere quindi modellizzata come:

$$U_H = \frac{H}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + H + 1} aX - H^2$$

Con la simmetria utilizzata precedentemente si modifica:

$$U_H = \frac{H}{I + eI(N-1) + H + 1} aX - H^2$$

E la condizione del primo ordine (FOC) è:

$$\frac{\partial U_H}{\partial H} = \frac{(1 + I + eI(N-1))}{(I + eI(N-1) + H + 1)^2} aX - 2H$$

Come per la condizione del primo ordine delle imprese, anche la FOC dell'hacker a confronto al modello con indipendenza, possiamo notare che per valori di $e > 0$ ed N≥2 le interdipendenze strutturali creano delle esternalità negative per i criminali informatici, riducendo i loro ricavi marginali e quindi anche gli incentivi ad investire risorse nell'attacco.

Funzione dei consumatori

Come per l'hacker anche per i consumatori sono state adottate le stesse ipotesi e parametri utilizzati nel modello con indipendenza, la sua funzione di utilità rimane sostanzialmente invariata, ma ora il livello di sicurezza considerato non è più quello della singola azienda ma quello relativo alla struttura informatica condivisa, la funzione di utilità del consumatore diventa:

$$U_C = U_0 + \ln(1 + I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j) - L \frac{H}{I_i + \mathrm{e} \cdot \sum_{j \neq i}^{N-1} I_j + H + 1} aX - C I_i$$

Che considerando la simmetria si trasforma:

$$U_C = U_0 + \ln(1 + I + eI(N-1)) - L\frac{H}{I + eI(N-1) + H + 1}aX - C(I + eI(N-1))$$

Con la condizione del primo ordine:

$$\frac{\partial U_C}{\partial I} = \frac{1 + e(N-1)}{1 + I + eI(N-1)} + L\frac{H(1 + e(N-1))}{(I + eI(N-1) + H + 1)^2}aX - C(1 + e(N-1))$$

Che semplificando per $1 + e(N-1)$ può essere riscritta:

$$\frac{\partial U_C}{\partial I} = \frac{1}{1 + I + eI(N-1)} + L\frac{H}{(I + eI(N-1)H + 1)^2}aX - C$$

EQUILIBRIO OTTIMO A SISTEMA

Per determinare l'equilibrio ottimale dell'investimento in cybersicurezza da parte dell'impresa e dello sforzo dell'hacker, è necessario risolvere il sistema di equazioni che deriva dalle condizioni del primo ordine (FOC) delle tre funzioni di utilità: impresa, hacker e consumatore.

$$\begin{cases} U_I = X - \dfrac{H}{I + eI(N-1) + H + 1}aX - \dfrac{1}{2}\mathrm{I}^2 \\ U_H = \dfrac{H}{I + eI(N-1) + H + 1}aX - H^2 \\ U_C = U_0 + \ln(1 + I + eI(N-1)) - L\dfrac{H}{I + eI(N-1) + H + 1}aX - C(I + eI(N-1)) \end{cases}$$

L'equilibrio ottimo è definito dai valori (I^*, H^*) che soddisfano contemporaneamente:

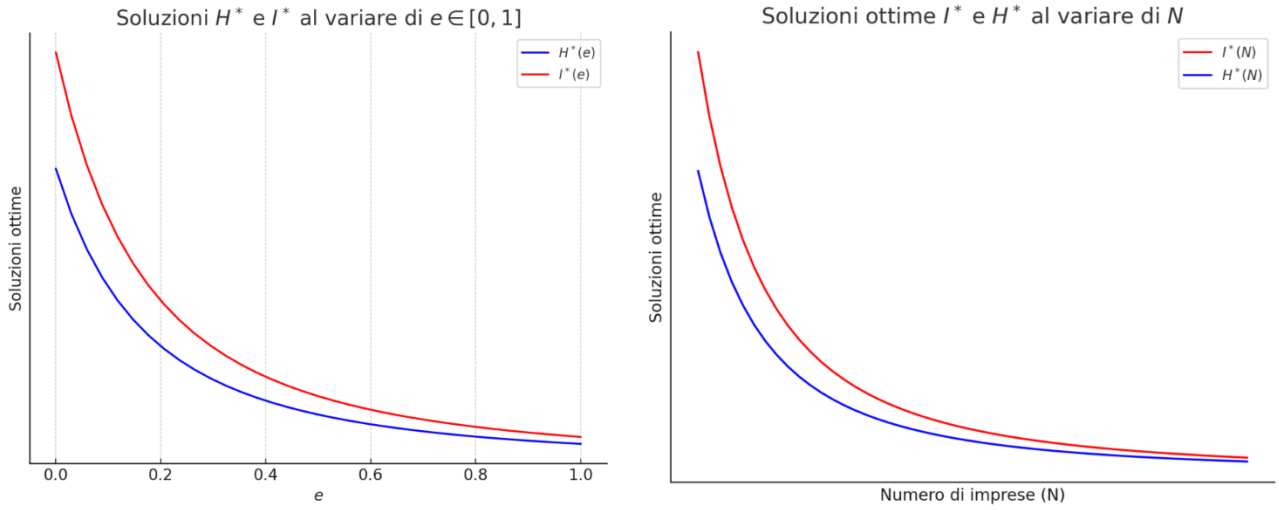
$$\begin{cases} \dfrac{H(1 + e(N-1))}{(I + eI(N-1) + H + 1)^2}aX = \mathrm{I} \\ \dfrac{(1 + I + eI(N-1))}{(I + eI(N-1) + H + 1)^2}aX = 2H \\ \dfrac{1}{1 + I + eI(N-1)} + L\dfrac{H}{(I + eI(N-1)H + 1)^2}aX = C \end{cases}$$

Risolvendo il sistema risulta:

$$\begin{cases} I^* = \dfrac{-1+\sqrt{1+8E^2H^{*2}}}{2E} \\ (H^* + \dfrac{1+\sqrt{1+8E^2H^{*2}}}{2})^2 = \dfrac{aX(1+\sqrt{1+8E^2H^{*2}})}{4H^*} \end{cases}$$

Con $E = 1 + e(N-1)$

L'equazione per H^* non si risolve in forma chiusa e richiede l'uso di metodi numerici per determinare il valore ottimale H^* in funzione degli altri parametri.



(Grafico 7 – andamento soluzioni ottime al variare di e ed N)

Il valore maggiore di aX, che rappresenta l'ammontare dei ricavi a rischio nell'attacco, genera soluzioni ottime I^* ed H^* più elevate, infatti, all'aumentare di aX il danno/ricavo potenziale degli attori è maggiore, e questo contribuisce ad aumentare gli incentivi per maggiori investimenti in sicurezza e nell'attacco.

Per valori incrementali di $e > 0$ e di N, le probabilità di successo dell'attacco da parte dei cybercriminali si riducono, le difese della struttura digitale diventano quindi troppo difficili da superare, diminuendo progressivamente gli incentivi degli hacker ad attaccare le imprese.

La presenza di spillover tecnici dovuti alle interdipendenze strutturali presenta quindi delle esternalità negative per gli hacker, riducendo le loro possibilità di successo nell'attaccare le imprese che condividono la stessa piattaforma digitale.

Per le aziende invece, un valore elevato di e implica una maggiore interdipendenza delle imprese sulla stessa struttura digitale, ampliando gli effetti degli spillover alle aziende interconnesse aumentando i loro benefici generati dagli investimenti in sicurezza altrui.

Anche all'aumentare del numero di imprese N, per valori di $e \neq 0$, la possibilità di sfruttare gli investimenti in cybersicurezza collettivi aumenta notevolmente, riducendo l'incentivo ad investire individualmente.

Entrambi gli scenari riguardano il fenomeno del free riding, che genera un'allocazione delle risorse non in modo efficiente, non producendo il massimo benessere collettivo e portando quindi un risultato subottimale per la società, questo genera un fallimento di mercato.

Una strategia per contrastare questa dinamica negativa è adottare delle politiche economiche adeguate, tra le possibili soluzioni introdurre una regolamentazione sugli investimenti in cybersicurezza, imponendo un livello minime di investimenti nelle difese informatiche eviterebbe che le imprese sottovalutino il problema e si affidino esclusivamente agli sforzi altrui. In alternativa la presenza di incentivi fiscali o sussidi per la cybersicurezza renderebbe più conveniente alle imprese effettuare investimenti in tale direzione, mentre la cooperazione tra aziende ed enti governativi, garantirebbe la definizione di standard minimi di sicurezza informatica che le diverse strutture digitali devono adottare. Tuttavia, anche in un modello teorico semplificato l'introduzione di un sussidio implicherebbe che le autorità dispongano di informazioni perfette sulla struttura del mercato (N) e sul livello di interdipendenza tra le imprese (e), rendere le aziende finanziariamente responsabili per i danni, nel caso in cui le perdite sociali risultino superiori a quelle private potrebbe essere un'ulteriore alternativa.

Se nessuna di queste misure venisse adottata, il rischio sarebbe quello di assistere a una tragedia dei beni comuni, dove ciascuna impresa tende a investire meno del necessario, confidando sugli investimenti altrui. Questo comportamento collettivo, nel caso di investimenti I non simmetrici e quindi con la possibilità delle imprese di adottare un $I_i = 0$, potrebbe portare ad una riduzione della sicurezza generale, aumentando la vulnerabilità del sistema e rendendo gli attacchi hacker sempre più facili e frequenti. Senza interventi correttivi, l'eccessiva interdipendenza strutturale e la frammentazione degli investimenti potrebbero compromettere la sicurezza del mercato.

3.5 Il modello con Interdipendenze di mercato

In questa tipologia di interdipendenze, le imprese operano in strutture informatiche isolate, gli investimenti sulla sicurezza hanno effetti positivi solamente per l'impresa che li effettua. La loro concorrenza avviene nel mercato dei prodotti o servizi, in cui, se un'azienda è vittima di una violazione informatica i consumatori potrebbero non sentirsi più sicuri ed affidarsi ad un'impresa rivale. L'utilizzo di risorse per aumentare le difese ha degli effetti, definiti come spillover di mercato, sulle competitività nel settore, influenzando le decisioni anche delle altre aziende che non intendono

veder diminuire le proprie quote di mercato. Questi comportamenti possono determinare un investimento in sicurezza superiore all'ottimo sociale.

Funzione dell'impresa

Per analizzare le interdipendenze di mercato Fedele e Roner hanno sviluppato un ulteriore modello, sempre solo per le imprese. Vengono considerate un numero di aziende simmetriche $N \geq 2$ e neutrali al rischio, che competono nel mercato dei prodotti/servizi senza utilizzare strutture digitali interconnesse, quindi, gli investimenti in sicurezza delle singole imprese non contribuiscono anche alla difesa dei concorrenti. La probabilità di subire un cyberattacco è uguale per tutte le aziende e viene assunta, per semplicità e senza compromettere la generalità dell'analisi, come pari a 1. Il mercato è stato modellizzato in due fasi: (1) Il parametro X, non riguarda più i ricavi delle singole imprese, ma il ricavo totale del settore, che viene condiviso in modo equo dalle aziende presenti, che quindi generano dei ricavi pari ad $\frac{X}{N}$. (2) Si considera che se un'azienda subisce una violazione dei suoi sistemi informatici perde le proprie quote di ricavo, che vengono assorbite dai rivali che non sono stati compromessi. Il parametro a usato nei modelli precedenti, senza perdita di generalità, viene eguagliato ad 1, evidenziando che tutti i ricavi vengono perduti in caso di intrusione informatica.
Viene inoltre introdotto un parametro K che rappresenta il valore atteso del profitto generato dall'azienda i quando ha l'opportunità di assorbire la quota di ricavi dei rivali colpiti da violazioni della sicurezza ed è riportato nell'appendice.
La funzione di utilità risolta contemporaneamente da ogni impresa può essere formulata come:

$$max_{I_i \geq 0} R_M(I_1, \dots, I_N) - I_i = \frac{X}{N} - \frac{X}{N} \cdot \frac{1}{1 + I_i} + [1 - \frac{1}{1 + I_i}] \cdot K - I_i$$

Il termine $-\frac{X}{N} \cdot \frac{1}{1+I_i}$ rappresenta la perdita dei ricavi in caso di violazione subita dall'azienda i, mentre il termine $+[1 - \frac{\mathrm{H}}{1+\mathrm{H}+I_i}] \cdot K$ invece, rappresenta il valore atteso del guadagno che l'azienda ottiene quando si trova nella condizione di acquisire la quota di mercato dei concorrenti che subiscono una breccia nelle loro difese informatiche.

Come nei paragrafi precedenti, per estendere il modello ed includere anche gli ulteriori due attori, sono state apportate delle modifiche alla struttura originale, adattando la funzione di profitto in modo da rappresentare le dinamiche di interazione tra imprese, hacker e consumatori all'interno di un modello di mercato a tre versanti. Nella rappresentazione della perdita e guadagno di ricavi è stato

considerato lo sforzo dell'hacker H, ed i costi sono stati cambiati da lineari a quadratici per rendere il sistema di equazioni più flessibile. Il parametro a è stato reintrodotto e rappresenta la quota dei ricavi $\frac{X}{N}$ sottratti dai criminali informatici, che quindi non viene reintrodotta nel mercato, per rappresentare questa modifica il parametro K è stato modificato con K_a anche esso riportato in appendice. La funzione di utilità delle imprese di modifica nel modo seguente:

$$U_I = \frac{X}{N} - \frac{X}{N} \cdot \frac{\mathrm{H}}{1 + \mathrm{H} + I_i} + [1 - \frac{\mathrm{H}}{1 + \mathrm{H} + I_i}] \cdot K_a - \frac{{I_i}^2}{2}$$

Funzione dell'hacker

Le strategie dell'hacker nel modello con interdipendenze di mercato sono le stesse, deve bilanciare il ritorno economico derivante da un attacco riuscito con il costo dello sforzo necessario per violare il sistema di sicurezza dell'impresa. La sua funzione di utilità può essere modellizzata come:

$$U_H = \mathrm{a}\frac{X}{N} \cdot \frac{H}{1 + \mathrm{H} + I_i} - H^2$$

Utilizzando nuovamente la simmetria, per cui $I_i = I$ la FOC per l'hacker risulta:

$$\frac{\partial U_H}{\partial H} = \mathrm{a}\frac{X}{N} \cdot \frac{1 + I}{(1 + \mathrm{H} + I)^2} - 2H$$

Funzione dei consumatori

Come per l'hacker anche per i consumatori sono state adottate le stesse ipotesi e parametri utilizzati nel modello con indipendenza, la sua funzione di utilità rimane sostanzialmente invariata, con il livello di sicurezza considerato della singola azienda i, la funzione di utilità del consumatore diventa:

$$U_C = U_0 + \log(1 + I_i) - L\frac{\mathrm{H}}{1 + \mathrm{H} + I_i} \cdot a\frac{X}{N} - CI_i$$

Sempre considerando la simmetria la FOC del consumatore è:

$$\frac{\partial U_C}{\partial I} = \frac{1}{1 + \mathrm{I}_i} + \mathrm{L}\frac{aX}{N} \cdot \frac{H}{(1 + \mathrm{H} + \mathrm{I}_i)^2} - C$$

EQUILIBRIO OTTIMO A SISTEMA

Per determinare l'equilibrio ottimo dell'investimento in cybersicurezza data la presenza del parametro K che dipende dal livello di investimenti in sicurezza I e non permette una soluzione chiusa, negli studi condotti da Fedele e Roner è stato analizzato il caso di duopolio e di simmetria degli investimenti I. Le loro conclusioni e analisi possono essere utilizzate anche per il nostro modello, offrendo un quadro di riferimento utile per comprendere le dinamiche dell'equilibrio ottimale in presenza degli ulteriori attori hacker e consumatore.

Nel contesto di un duopolio, per modello di Fedele e Roner la scelta che l'azienda deve compiere è descritta dalla seguente funzione:

$$max_{I_i \geq 0} R_M(I_i, I_j) - I_i = \frac{X}{2} - \frac{X}{2} \cdot \frac{1}{1+I_i} + [1 - \frac{1}{1+I_i}] \cdot \frac{1}{I_j + 1} \frac{X}{2} - I_i$$

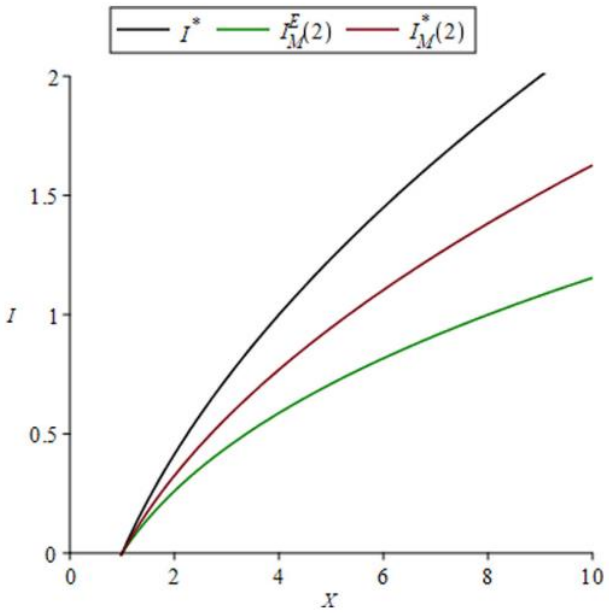
Dalla risoluzione del problema si ricava il livello di investimento associato all'equilibrio di Nash simmetrico:

$I_M^*(2) = \frac{X+6Y^2}{6H} - 1$ con Y che indica una funzione esplicita del ricavo, $Y = \sqrt[3]{\sqrt{\frac{X^2(27-2X)}{432}} + \frac{X}{4}}$.

L'equilibrio $I_M^*(2)$ trovato viene poi confrontato sia con l'investimento socialmente ottimale per N=2, indicato come $I_M^{\mathrm{E}}(2)$. Quest'ultimo rappresenta il livello di investimento scelto da un pianificatore sociale per massimizzare il profitto complessivo delle due imprese. A tal fine, consideriamo la risoluzione del seguente problema:

$max_{I_i \geq 0} 2 \times R_M(I_i, I_j) - I_i = 2\left[\frac{X}{2} - \frac{X}{2} \cdot \frac{1}{1+I} + [1 - \frac{1}{1+I}] \cdot \frac{1}{I+1} \frac{X}{2} - I_i\right]$ da cui si ricava $I_M^{\mathrm{E}}(2) = \sqrt[3]{X} - 1$, inoltre E $I_M^*(2)$ viene anche confrontato con l'investimento ottimo in caso di monopolio dato da:

$max_{I \geq 0}\{R(I) - I\} = X - \frac{1}{1+I} aX - I$ la cui soluzione ottima è $I^* = \sqrt{aX} - 1$.



(Figura 29- Andamento investimenti in cybersicurezza con interdipendenze di mercato)

(Fonte - Dangerous games: A literature review on cybersecurity investments)

Dall'analisi dei grafici di $I_M^*(2)$ (curva rossa), I^* (curva nera) con a=1, e $I_M^{\mathrm{E}}(2)$ (curva verde), mettendoli in relazione con il valore di X si può notare che entrambi gli investimenti ottimi I^* ed $I_M^*(2)$ sono superiori al livello socialmente ottimo $I_M^{\mathrm{E}}(2)$ per X>1, questo sovrainvestimento è il risultato di un'esternalità negativa legata agli spillover di mercato. Se un'impresa decide di aumentare l'investimento I_i per migliorare la propria sicurezza, il miglioramento diretto del proprio profitto ovvero il beneficio marginale privato, risulta maggiore rispetto al beneficio marginale sociale ossia il vantaggio combinato per entrambe le imprese i e j. Questo perché l'impresa i non considera gli impatti negativi che il suo investimento esercita sulla probabilità dell'azienda j rivale di sottrarle la quota di mercato.

Dal grafico si può anche notare anche che l'investimento ottimo in caso di duopolio risulta sempre inferiore a quello di monopolio per ogni X>1, gli spillover delle interdipendenze di mercato determinano un effetto analogo a quelle strutturali, ma attraverso un meccanismo differente, non legato al free riding. In un mercato monopolistico, un'azienda che aumenta il proprio investimento in sicurezza informatica riduce il rischio di subire un attacco, assicurandosi così l'intero ricavo di mercato X, mentre in un mercato duopolistico, lo stesso incremento nell'investimento risulta meno efficace, perché l'azienda i può ottenere l'intero profitto del settore solo nel caso in cui il concorrente j venga colpito da un cyberattacco, ma, questa probabilità non è mai pari a 1 quando I_j>0, rendendo quindi l'investimento meno vantaggioso rispetto al caso monopolistico.

Nel caso di oligopolio, con il numero di imprese N≥ 2 la soluzione ottima è monotonicamente decrescente all'aumentare di N, questo andamento è dovuto dagli spillover di mercato che rendono l'investimento in cybersicurezza meno efficace quando il numero di imprese cresce. Infatti, ciascuna impresa i=1,…,N può ottenere l'intero profitto di mercato X solo se tutti i rivali subiscono un cyberattacco andato a buon fine, e la probabilità che ciò accada si riduce all'aumentare di N, rendendo meno conveniente investire in cybersicurezza.

All'aumentare del numero di concorrenti, l'efficacia marginale degli investimenti delle imprese tende a diminuire, l'effetto negativo degli spillover di mercato sull'investimento di equilibrio, osservato nel caso del duopolio, si manifesta in modo progressivo anche in contesti oligopolistici.

In questo scenario, una possibile soluzione per ridurre le esternalità negative potrebbe essere l'introduzione di un'imposta proporzionale agli investimenti in cybersicurezza favorendo una riduzione del sovrainvestimento, tuttavia, come nel caso delle interdipendenze strutturali, sarebbe necessario che le autorità dispongano delle informazioni dettagliate sull'impatto di ogni investimento sulla probabilità di violazione della sicurezza, così da poter internalizzare in modo adeguato l'esternalità negativa generata dagli spillover di mercato.

Per verificare se questi risultati si possono applicare anche al modello di mercato completo dei tre attori impresa-hacker-consumatore, come fatto da Fedele e Roner è stato analizzato il mercato in caso di duopolio e simmetria degli investimenti, le funzioni di utilità dei diversi attori si modificano:

$$\begin{cases} U_I = \dfrac{X}{2} - \dfrac{XH^2}{2(1+H+I)^2} - \dfrac{1}{2}I^2 \\ U_H = \dfrac{X}{2} \cdot \dfrac{H}{1+\mathrm{H}+I} - H^2 \\ U_C = U_0 + \log(1+I) - L\dfrac{\mathrm{H}}{1+\mathrm{H}+I} \cdot \dfrac{X}{2} - CI \end{cases}$$

Derivando le funzioni di utilità per ottenere le condizioni del primo ordine il sistema risultante è:

$$\begin{cases} \dfrac{XH^2}{(1+H+I)^3} - I = 0 \\ \dfrac{X}{2} \cdot \dfrac{1+I}{(1+H+I)^2} - 2H = 0 \\ \dfrac{1}{1+I} - L\dfrac{\mathrm{H}}{(1+H+I)^2} \cdot \dfrac{X}{2} - C = 0 \end{cases}$$

E risolvendo il sistema per I e H per trovare l'equilibrio di Nash risulta:

$$\begin{cases} I^*_{duo} = \dfrac{1+2L{H^*_{duo}}^2}{C} - 1 \\ 4{H^*_{duo}}^3 = (\dfrac{1+2L{H^*_{duo}}^2}{C} - 1) \cdot \dfrac{1+2L{H^*_{duo}}^2}{C}(H^* + \dfrac{1+2L{H^*_{duo}}^2}{C}) \end{cases}$$

Le soluzioni I^*_{duo}, H^*_{duo} si possono confrontare con le soluzioni trovate precedentemente in caso di monopolio:

$$\begin{cases} I^*_{mono} = \dfrac{C - L + \sqrt{(L+C)^2 - 4L}}{2L} \\ H^*_{mono} = \sqrt{\dfrac{I^*(I^*+1)}{2}} \end{cases}$$

Risulta che per i valori dei parametri C>L, l'impresa monopolistica sceglie un livello ottimale di investimento in cybersicurezza più elevato rispetto a quello che si osserva in un mercato duopolistico $I^*_{mono} > I^*_{duo}$ e di conseguenza anche $H^*_{mono} > H^*_{duo}$. L'introduzione dello sforzo strategico dell'hacker e l'impatto sul consumatore non alterano il principio di base in presenza di interdipendenze di mercato, l'investimento in sicurezza è meno efficace in contesti competitivi, per via degli spillover che riducono il beneficio marginale privato. Pertanto, anche nel modello a tre versanti le conclusioni rimangono coerenti, l'impresa monopolistica tende a investire di più rispetto a quella che opera in un mercato concorrenziale, confermando la validità e l'applicabilità dei risultati di Fedele e Roner anche in scenari di mercato più complessi.

L'analisi congiunta delle interdipendenze strutturali e di mercato nel contesto della cybersicurezza rappresenta un campo di ricerca ancora in fase iniziale, principalmente a causa della complessità dei modelli richiesti per catturare in modo accurato le interazioni, ma, il tema sta diventando sempre più centrale nell'economia digitale, poiché le aziende sono sempre più interconnesse nel mercato globale e attraverso strutture informatiche condivise, rendendo essenziale comprendere come queste interdipendenze influenzino le decisioni di investimento in sicurezza.
Un ulteriore aspetto ancora poco esplorato è la determinazione empirica della probabilità di subire una violazione della sicurezza. Attualmente, non esistono modelli consolidati che ne descrivano in modo preciso la forma funzionale, nonostante le funzioni di probabilità di attacco siano un elemento chiave per determinare l'investimento ottimale in sicurezza, senza una stima empirica affidabile di questi parametri, il rischio è che le imprese sovra o sotto-investano, con conseguenze negative sia a livello individuale che sistemico. Quindi, una migliore comprensione della distribuzione e dei fattori determinanti della probabilità di attacco è fondamentale per sviluppare strategie di difesa più efficaci e per supportare eventuali interventi normativi volti a migliorare la resilienza complessiva del sistema economico.

4. Analisi dati ISTAT

Questa sezione si concentrerà sull'analisi dei dati riguardanti la digitalizzazione e la sicurezza informatica in Italia. In modo da poter confrontare la realtà alle teorie economiche e ai modelli matematici trattati precedentemente.

Gli investimenti riguardanti la cybersecurity da parte delle imprese nel territorio italiano sono spesso limitati e non sempre disponibili, ed è uno degli aspetti più critici di questa analisi. Concetti come gli investimenti ottimali derivanti dai modelli avrebbero bisogno dei dati specifici, che non sono a disposizione per tutte le categorie esaminate.

Tramite le statistiche fornite dall'ISTAT (Istituto nazionale di statistica), sono disponibili informazioni sulle strategie di difesa più impiegate, il livello di protezione e gli attacchi informatici riscontrati dalle aziende italiane nei vari settori economici.

I diversi ambiti economici sono organizzati in base alla classificazione ATECO del 2025, entrata in vigore il primo gennaio 2025 e che sarà adottata operativamente dal 1° aprile dello stesso anno. I settori economici sono divisi in sezione e divisioni. Questa classificazione permette di analizzare lo sviluppo della sicurezza e degli attacchi informatici nei vari settori dell'economia italiana.

A seguire è riportato un elenco dettagliato dei settori considerati nel dataset, con i relativi codici ATECO:

Sezione	**Divisione**
C Attività Manifatturiere	[13] industrie tessili e dell'abbigliamento [17] industria dei prodotti in legno e carta [19] fabbricazione di coke e di prodotti derivanti dalla raffinazione del petrolio [25] metallurgia e fabbricazione di prodotti in metallo [26] computer e prodotti di elettronica e ottica [27] fabbricazione di apparecchiature elettriche ed apparecchiature per uso domestico non elettriche [30] fabbricazione di mezzi di trasporto [33] riparazione e installazione di macchine e apparecchiature
D Fornitura di Energia elettrica	[35] fornitura di energia elettrica, gas e vapore
F Costruzioni	
G Commercio all'ingrosso e al dettaglio	[47] commercio al dettaglio [47.2] industrie alimentari, delle bevande e del tabacco
H Trasporto e magazzinaggio	[53] attività postali e attività di corriere
I Attività dei servizi di alloggio e di ristorazione	[55] servizi di alloggio [56] attività dei servizi di ristorazione
J Attività editoriali, trasmissioni radiofoniche e produzione e distribuzione di contenuti	[58] attività editoriali [59] attività di produzione cinematografica, di video e di programmi televisivi

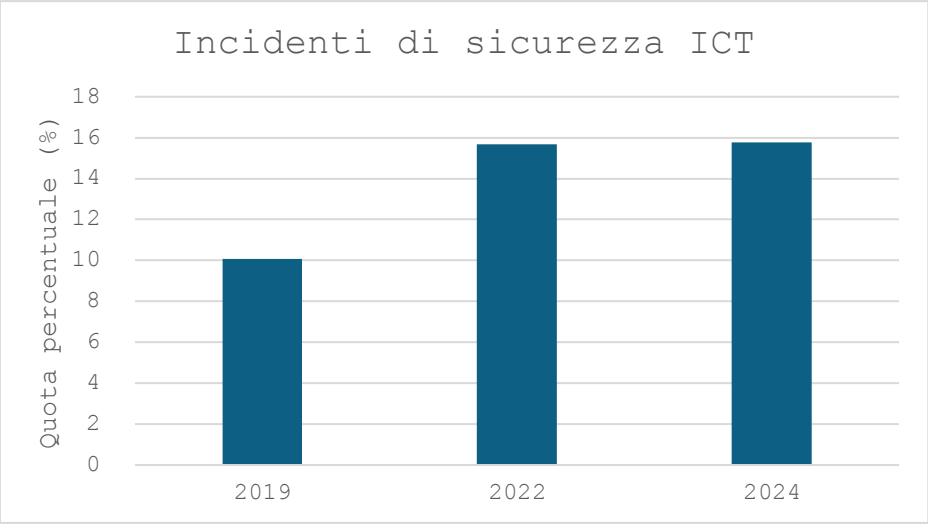
K Settore ICT	[61] telecomunicazioni [62] informatica ed altri servizi d'informazione [63.92] Altre attività dei servizi di informazione
M attività immobiliari	[68] attività immobiliari
N Attività professionali, scientifiche e tecniche	
O Attività amministrative e di servizi di supporto	[79] attività dei servizi delle agenzie di viaggio e dei tour operator

(Tabella 6- Codici ATECO 2025 dei settori presi in esame)

4.1 Incidenti di sicurezza ICT

Gli indicatori legati alla sicurezza informatica per i codici ATECO elencati precedentemente sono disponibili in forma aggregata per le aziende con almeno 10 dipendenti. I dati raccolti non differenziano le imprese in base alla loro dimensione specifica, ma considerano un insieme composto da aziende con un numero minimo di 10 lavoratori. Analisi e considerazioni sulla dimensione aziendale verranno svolte in un paragrafo successivo. Il periodo preso in considerazione è stato tra il 2019 e il 2024.

Il grafico sottostante illustra la percentuale annuale di tutte le attività economiche che hanno subito almeno un attacco informatico. Gli incidenti inclusi nel rapporto ISTAT sono indisponibilità servizi ICT, distruzione o corruzione di dati e divulgazione di dati riservati.



(Grafico 8– incidenza degli incidenti di sicurezza ICT dal 2019 al 2024)

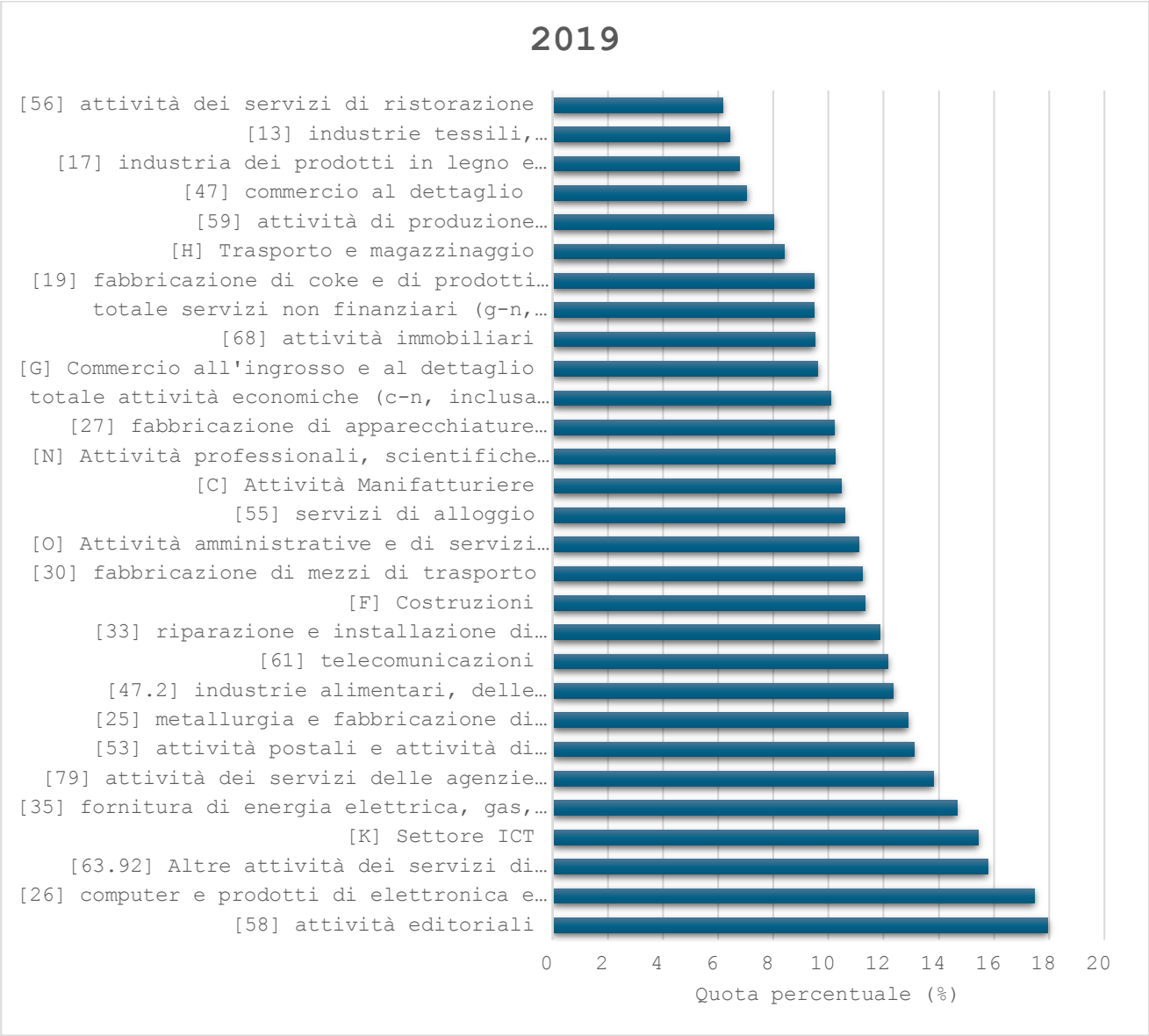
Esaminando il grafico, è possibile osservare che la quota degli attacchi informatici è significativamente aumentata, partendo da circa il 10% del 2019 per poi stabilizzarsi tra il 2022 e il 2024 con un'incidenza rispettiva del 15,7% e 15,8%. L'aumento riscontrato dopo il 2019, come accennato nei capitoli precedenti, può essere associato alla pandemia di Covid-19, con una digitalizzazione rapida e forzata che ha esposto le imprese a maggiori minacce. L'incidenza quasi

identica tra gli anni 2022 e 2024 può riflettere ad un adattamento delle aziende alle nuove tecnologie adottate negli anni, con l'utilizzo di queste ultime è aumentata la comprensione e consapevolezza, introducendo misure di sicurezza più adatte.
Gli attacchi sembrano essersi stabilizzati, ma le imprese devono proseguire nel migliorare le proprie strategie di difesa, per poter affrontare un contesto di minacce in continua evoluzione.

4.2 Analisi per settore

Dopo aver esaminato il campione complessivo delle imprese che hanno subito degli attacchi informatici, verrà approfondito quali settori siano stati più colpiti nei periodi 2019, 2022 e 2024. Questo consente di comprendere meglio la distribuzione delle minacce in relazione alle diverse

attività economiche e di analizzare le strategie adottate dai vari settori per affrontare le sfide della cybersicurezza.



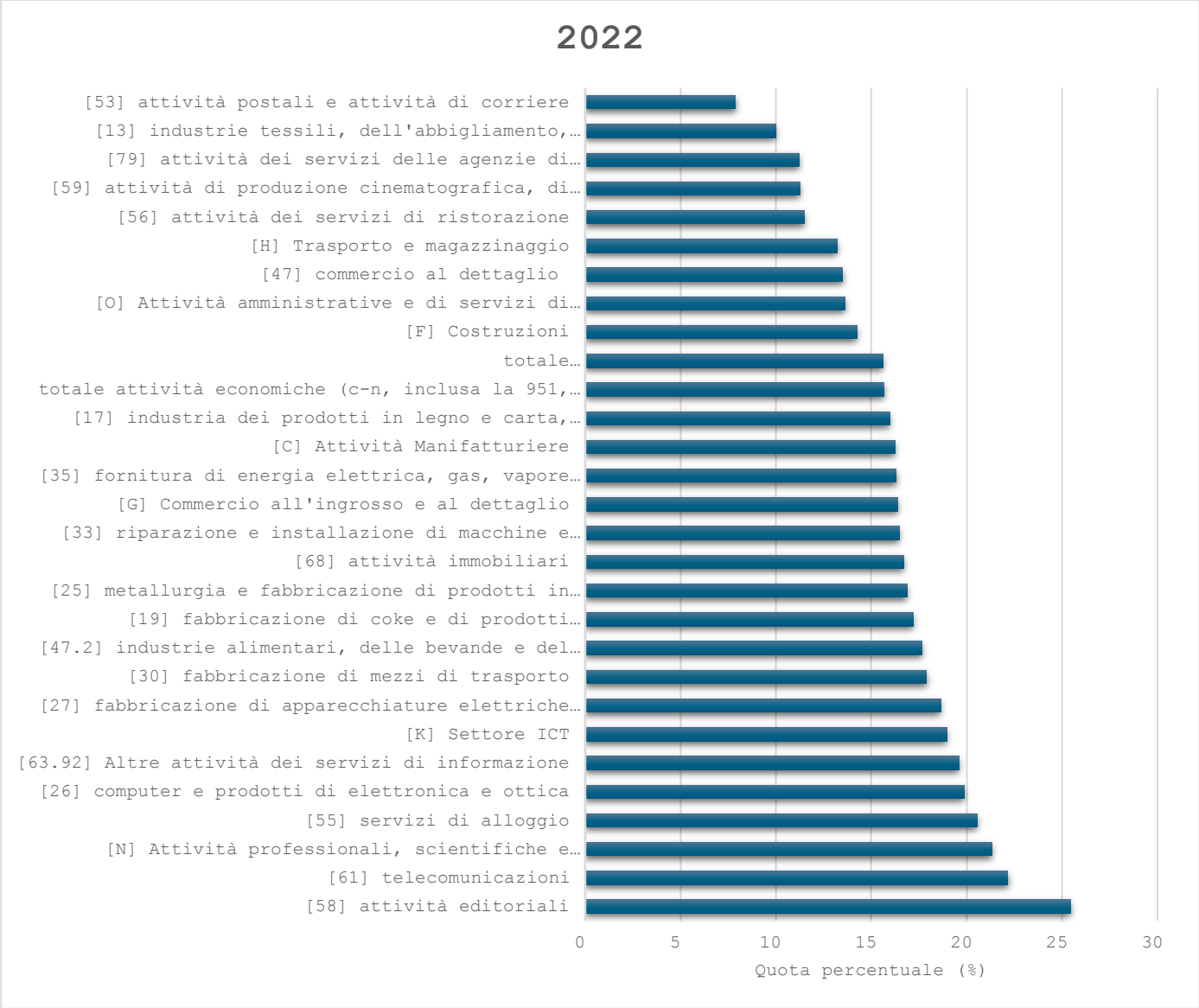
(Grafico 9– settori più colpiti nel 2019)

Durante il 2019 i settori più colpiti sono stati:

- [58] attività editoriali: 18%
- [26] computer e prodotti di elettronica e ottica: 17,5%
- [63.92] Altre attività dei servizi di informazione: 15,8%
- [K] Settore ICT: 15,4%
- [35] fornitura di energia: 14,7%

I settori più colpiti dagli attacchi informatici in Italia evidenziano una forte esposizione delle attività legate all'informazione, le attività editoriali occupano la prima posizione, probabilmente a causa della gestione di notizie sensibili come contenuti esclusivi e informazioni riservate. Il comparto della

produzione di computer segue vicino in seconda posizione, un dato che riflette l'importanza strategica di queste aziende. Le altre attività dei servizi di informazione e l'intero settore ICT confermano come il mondo digitale sia particolarmente vulnerabile, in quanto gestisce una grande quantità di dati e infrastrutture critiche.

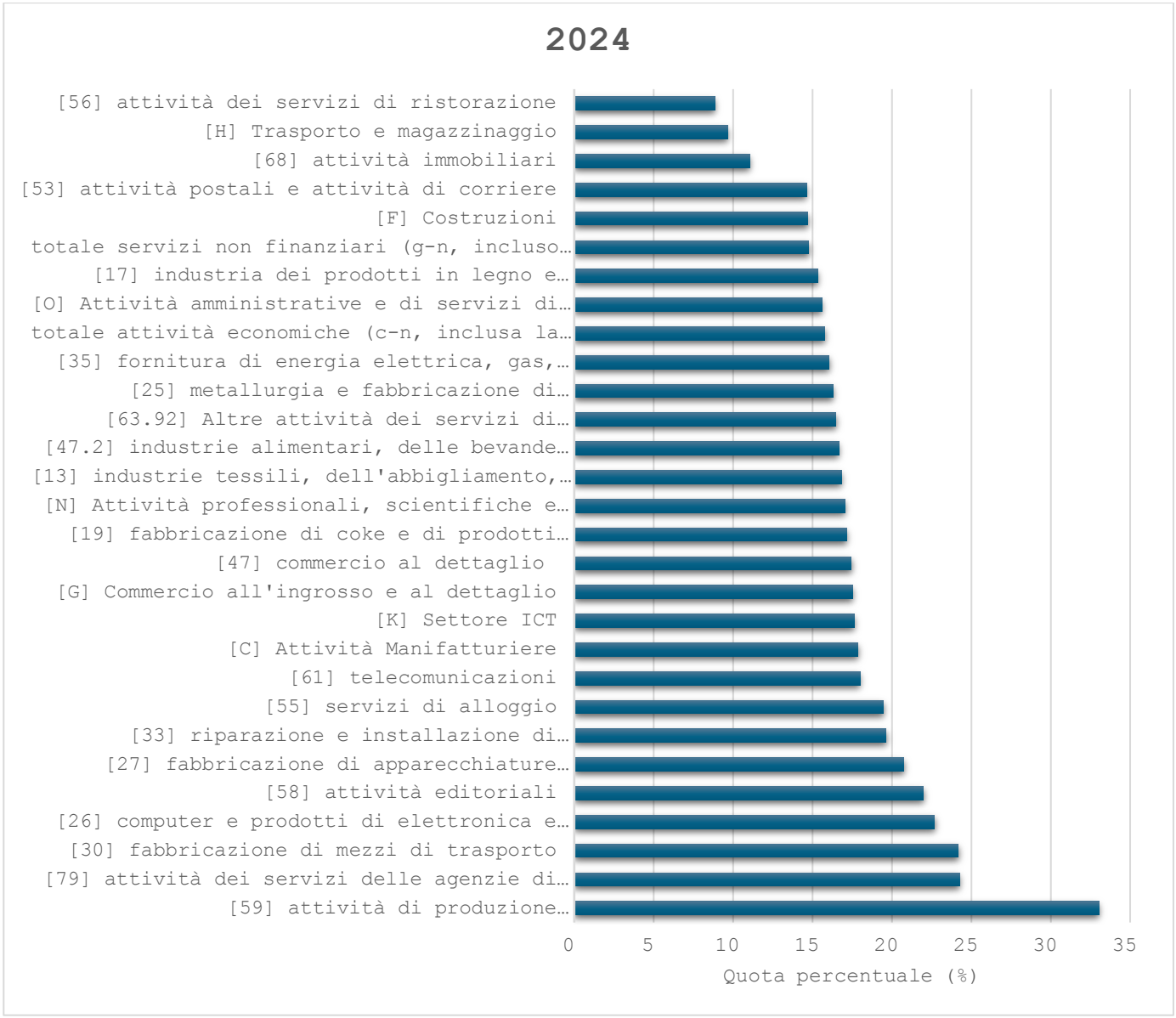


(Grafico 10- settori più colpiti nel 2022)

Durante il 2022 i settori più colpiti sono stati:

- [58] attività editoriali: 25,4%
- [61] telecomunicazioni: 22,2%
- [N] Attività professionali, scientifiche e tecniche: 21,3%
- [55] servizi di alloggio: 20,6%
- [26] computer e prodotti di elettronica e ottica: 19,9%

Le attività editoriali continuano ad essere le più vulnerabili, aumentando di 7,4 punti percentuali, l'Italia come descritto precedentemente è particolarmente vulnerabile agli attacchi di tipo Hacktivism e di disinformazione, che rendono le infrastrutture mediatiche bersagli prioritari. Le telecomunicazioni**,** che nel 2019 non figuravano tra i settori più colpiti, emergono come uno dei bersagli principali. La crescente dipendenza da infrastrutture digitali e la diffusione di connessioni veloci potrebbero aver reso il settore un obiettivo primario per minacce mirate alla compromissione delle reti e delle comunicazioni. Un altro dato interessante è la forte presenza delle attività professionali, scientifiche e tecniche un settore che anche esso nel campione precedente non rientrava tra i più colpiti. Questo aumento potrebbe riflettere l'interesse crescente verso il furto di proprietà intellettuale e dati sensibili aziendali.



(Grafico 11- settori più colpiti nel 2024)

Durante il 2024 i settori più colpiti sono stati:

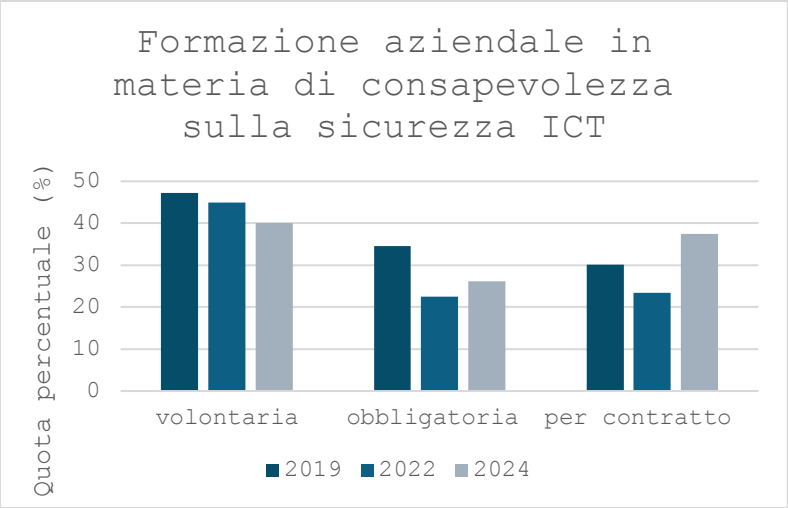
- [59] attività di produzione cinematografica, di video e di programmi televisivi: 33%
- [79] attività dei servizi delle agenzie di viaggio e dei tour operator: 24,3%
- [30] fabbricazione di mezzi di trasporto: 24,2%
- [26] computer e prodotti di elettronica e ottica: 22,7%
- [58] attività editoriali: 22%

Per la prima volta c'è stato un cambiamento nella testa della classifica con il settore cinematografico e televisivo che registra il valore più alto. Questo dato potrebbe evidenziare l'interesse da parte dei cybercriminali nel colpire l'industria dei contenuti digitali, a causa della crescente diffusione delle piattaforme di streaming e del valore della pirateria. Anche le attività dei servizi di agenzie di viaggio debuttano tra le vittime più colpite, una delle motivazioni potrebbe essere l'utilizzo sempre maggiore di applicazioni e piattaforme online che hanno aumentato l'esposizione di questa categoria. Le attività editoriali e il comparto computer ed elettronica sono gli unici settori sempre presenti nella top 5, segnalando una minaccia costante e il bisogno di adottare maggiori misure di sicurezza.

4.2.1 Strategie di difesa

Con gli attacchi informatici in aumento e in continua evoluzione le imprese non rimangono passive di fronte a questi pericoli, ma adottano tecniche sempre più avanzate per proteggere i propri sistemi e dati sensibili. La cybersecurity non si limita a rispondere alle minacce, ma richiede un approccio preventivo che integri sia soluzioni di protezione delle proprie infrastrutture che la formazione dei dipendenti per una migliore preparazione contro i criminali informatici.

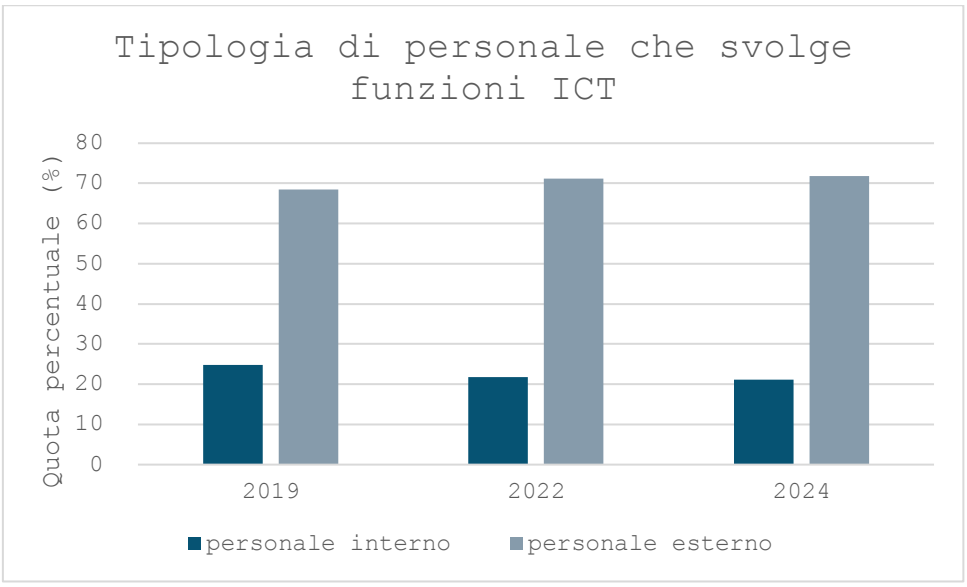
Nel dataset è presente l'incidenza percentuale delle imprese che rendono consapevoli i propri dipendenti dei loro obblighi in materia di sicurezza ICT, divisa mediante la diversa erogazione dei corsi di formazione, su base volontaria, obbligatoria e da contratto. I dati analizzati riguardano il totale delle attività economiche.



(Grafico 12– tipologia di formazione in materia di sicurezza ICT)

La consapevolezza volontaria dei dipendenti riguardo alla sicurezza ICT è la più diffusa in tutti gli anni considerati, ma con un trend in diminuzione, rispetto a quella obbligatoria e per contratto che dopo un calo nel 2022 sono aumentate nel periodo successivo, specialmente per contratto, grazie anche a normative più stringenti imposte per la sicurezza dei dati.

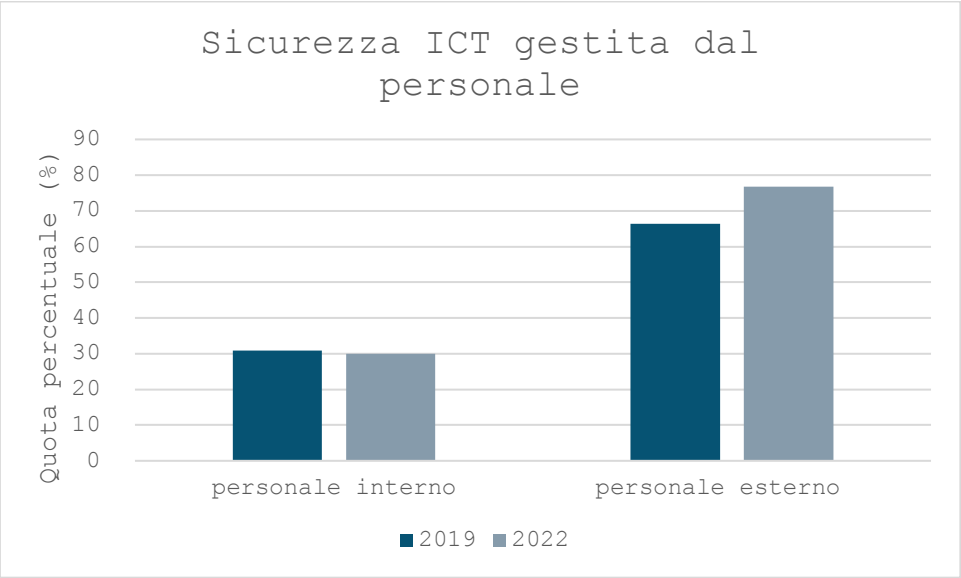
Non tutto il personale aziendale ha accesso ai sistemi informatici, le aziende gestiscono le proprie funzioni ICT in modo diverso, nel grafico sottostante è possibile osservare l'andamento generale.



(Grafico 13– Tipologia di personale che svolge funzioni ICT)

Si nota chiaramente che il controllo delle funzioni ICT è affidata prevalentemente al personale esterno, lo sviluppo di sistemi informatici sempre più sofisticati e complicati da gestire ha reso conveniente per molte aziende italiane affidarsi a competenze specializzate esterne.

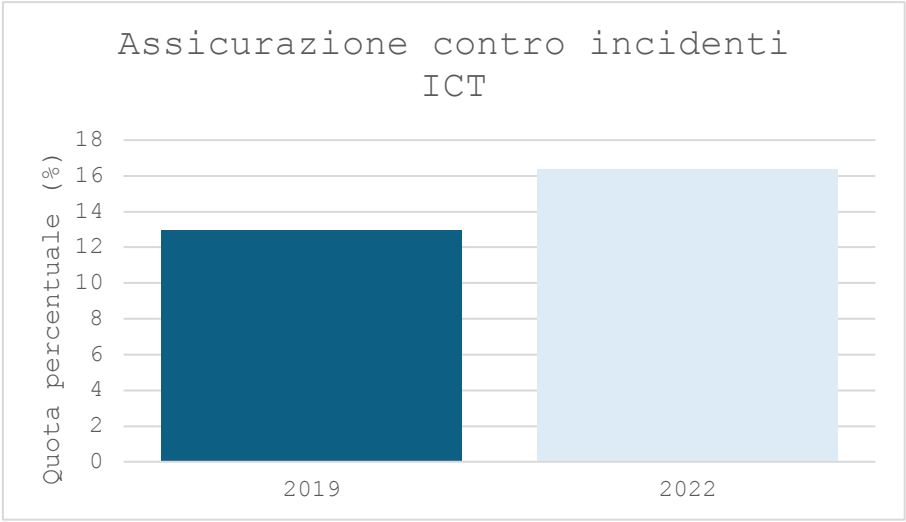
Per i periodi 2019 e 2022 sono anche disponibili le incidenze percentuali sulla gestione della sicurezza ICT interna o esterna e la sottoscrizione di assicurazioni sulla cybersicurezza.



(Grafico 14– tipologia di personale che gestisce la sicurezza ICT)

In Italia, le aziende, come per la gestione delle funzioni ICT, tendono maggiormente ad affidarsi a personale esterno per la sicurezza ICT, questo potrebbe evidenziare le crescenti sfide nel mantenere protetto un sistema autonomamente, preferendo affidarsi a esperti esterni, specializzati nel settore di sicurezza informatica in grado di affrontare in maniera migliore le crescenti complessità delle minacce informatiche. Tuttavia, il mancato rafforzamento del personale interno potrebbe rappresentare un rischio in termini di dipendenza da fornitori esterni e di continuità operativa in caso di emergenze.

Con i rischi riguardanti la sicurezza informatica in continua crescita, una possibile soluzione è la sottoscrizione di una polizza assicurativa, in grado di coprire eventuali danni.

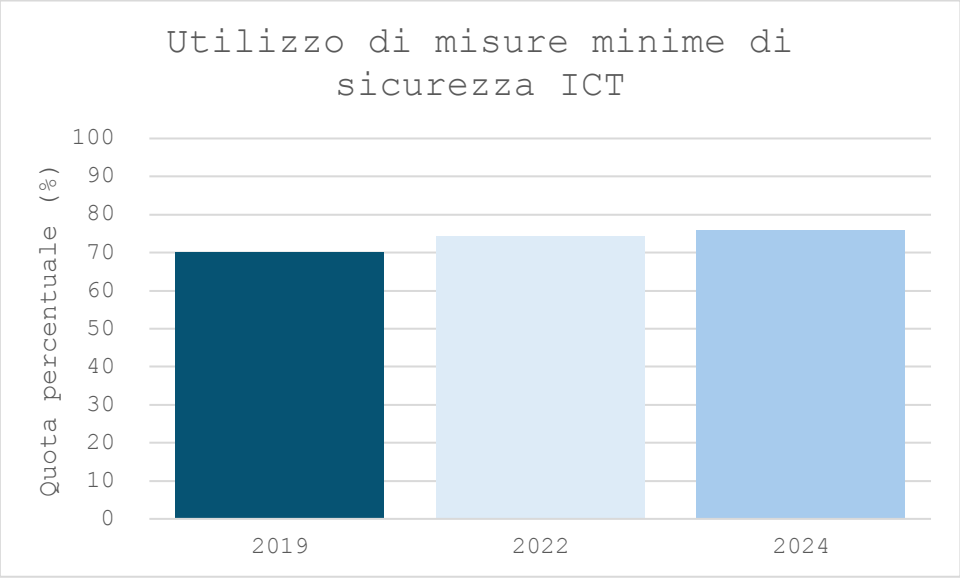


(Grafico 15– Quota aziende con assicurazione sulla sicurezza ICT)

Le aziende che scelgono di tutelarsi attraverso assicurazioni contro incidenti ICT sono in aumento, nel 2019 erano il 13% per arrivare al 16,4% del 2022. Questo potrebbe rappresentare una maggiore consapevolezza del pericolo rappresentato dagli cyberattacchi, soprattutto dopo la massiccia digitalizzazione avvenuta nel 2020. Le imprese scelgono maggiormente soluzioni assicurative per limitare possibili danni economici derivanti da incidenti informatici.

4.2.2 Misure di sicurezza

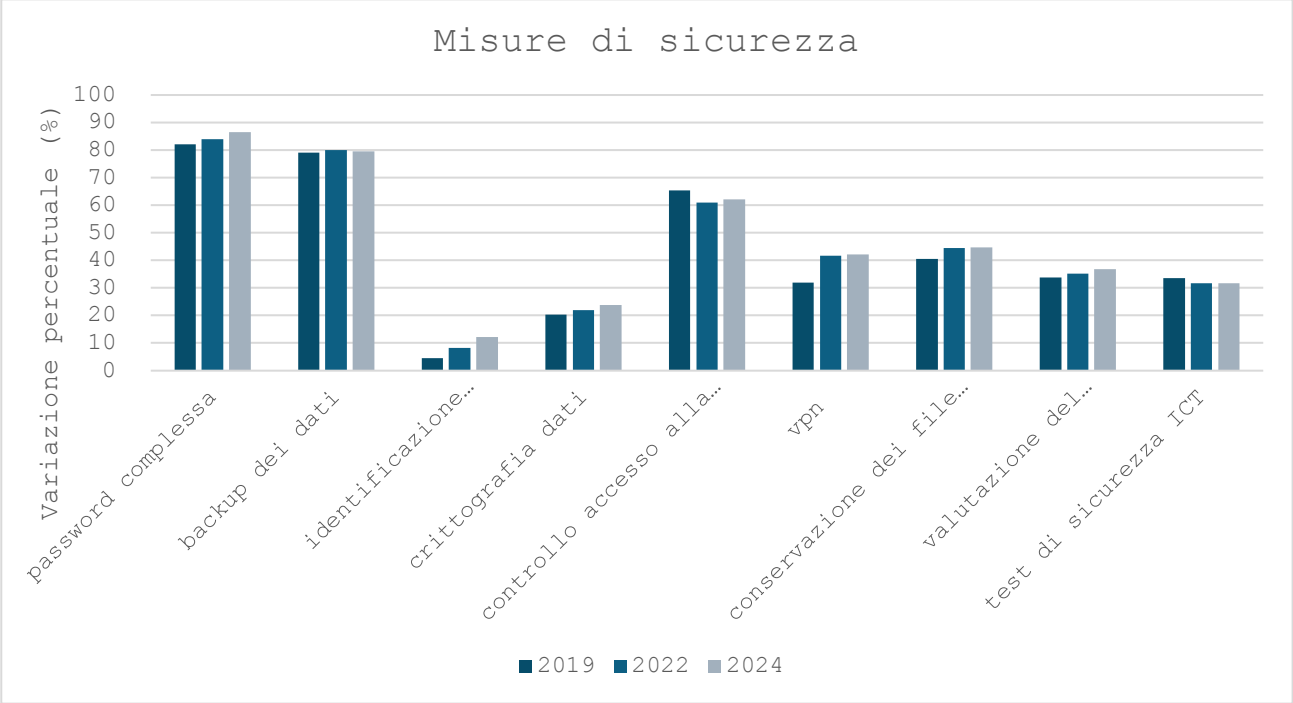
Oltre alla formazione del personale e l'acquisto di assicurazioni per limitare l'impatto degli attacchi informatici le imprese hanno implementato diversi sistemi di sicurezza. Nel grafico sotto stante si può vedere l'incidenza percentuale delle aziende che hanno adottato misure minime di sicurezza, intese come utilizzo di password complesse, l'aggiornamento software e backup dei dati.



(Grafico 16– misure minime di sicurezza ICT)

L’utilizzo di misure minime di sicurezza negli anni è aumentato, partendo dal 70% del 2019 fino ad arrivare al 76% del 2024, nonostante la tendenza sia positiva e la percentuale relativamente alta, rimane comunque un fattore negativo, che essendo misure di sicurezza minime quasi la totalità delle aziende dovrebbe adottarle.

Per osservare l’andamento delle specifiche misure di sicurezza più utilizzate dalle imprese italiane si può utilizzare il grafico sottostante.

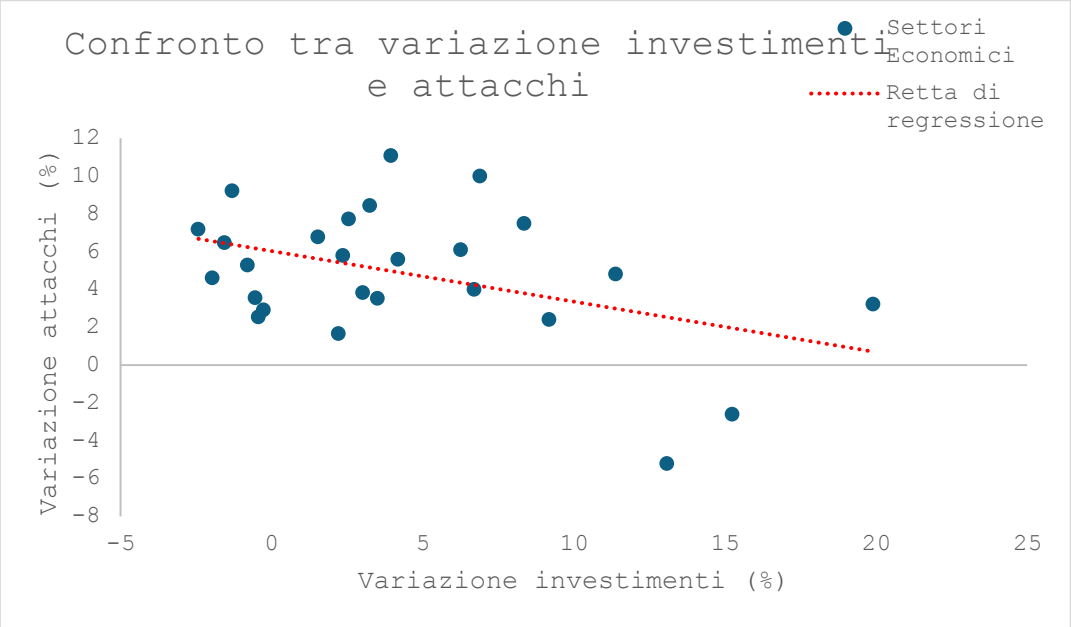


(Grafico 17– variazione delle singole misure di sicurezza)

Nel complesso la maggior parte delle tecniche di sicurezza ha registrato una crescita nel tempo. L'uso di password complesse e il backup dei dati, procedure che fanno parte delle misure minime di sicurezza, si mantengono costantemente elevate essendo ormai pratiche standard. L'identificazione biometrica ha l'incidenza più bassa, nonostante la maggior affidabilità rispetto alle password tradizionali presenta maggiori costi di implementazione, la sua quota percentuale è comunque quasi triplicata nel periodo considerato. Anche la crittografia dei dati, fattore molto importante per contrastare il furto delle informazioni non è largamente utilizzata, sebbene sia in crescita. La VPN, con la diffusione dello smart working è diventata fondamentale per garantire connessioni sicure alle reti aziendali, subendo infatti un sensibile aumento dopo la pandemia del 2020.
In generale, si nota un rafforzamento delle politiche di sicurezza informatica, con un'adozione sempre più diffusa di tecniche di sicurezza e un'evoluzione verso strumenti più avanzati.

4.2.3 Efficacia degli investimenti in cybersicurezza

Per valutare l'efficacia delle strategie di difesa adottate dalle imprese è necessario confrontare i dati relativi agli investimenti in sicurezza informatica e l'andamento degli attacchi per i vari settori economici durante i periodi considerati, partendo dal 2022-2019.

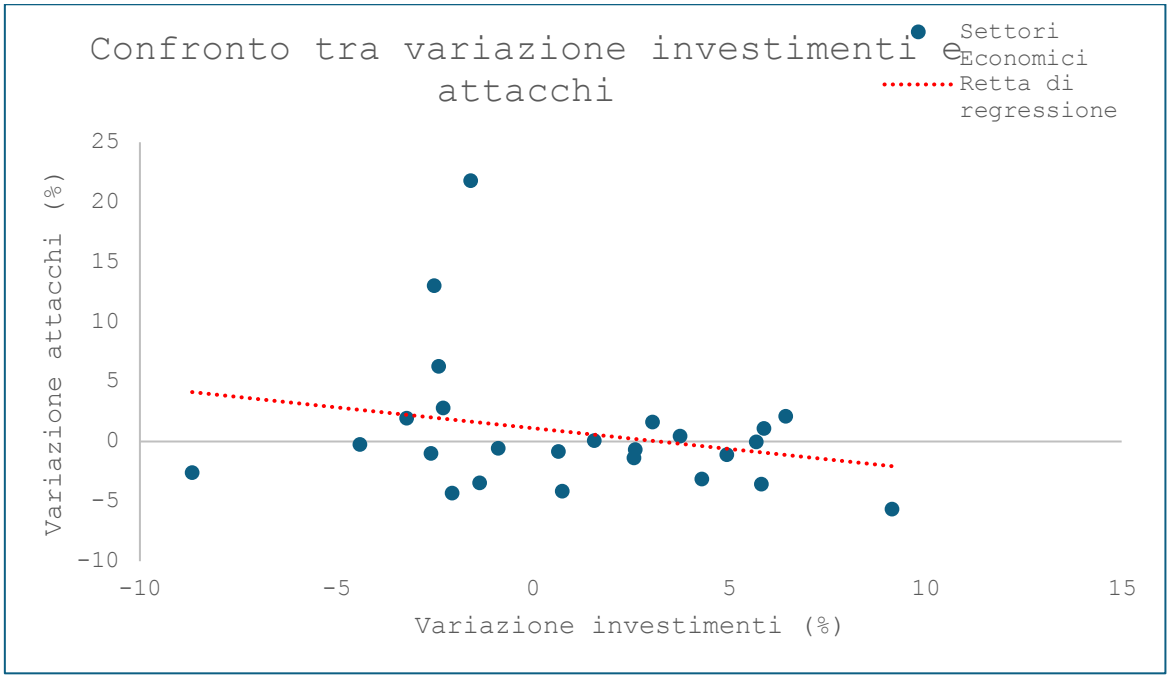


(Grafico 18 – confronto tra variazione investimenti e attacchi informatici 2022-2019)

Durante il periodo 2022-2019 viene evidenziata una relazione inversa tra l'aumento degli investimenti e la variazione degli attacchi. La tendenza generale degli attacchi informatici è stata in aumento per tutte le categorie, ma i settori che hanno utilizzato maggiori risorse aumentando le misure di sicurezza hanno riscontrato una crescita minore degli attacchi, in confronto ai settori con investimenti inferiori. La retta di regressione conferma questo andamento, con un p-value del valore

di 0.029, risulta un legame statisticamente significativo. Questo indica che aumentare le risorse destinate alla sicurezza informatica ha contribuito a contenere la crescita degli attacchi.

Il confronto tra variazione di investimenti e attacchi informatici per il periodo 2024-2022 risulta.



(Grafico 19 – confronto tra variazione investimenti e attacchi informatici 2024-2022)

La relazione inversa tra un aumento della sicurezza e la variazione degli attacchi informatici risulta ancora sempre presente. Rispetto al periodo precedente (2022-2019), non c'è stato un incremento significativo degli attacchi, come precedentemente visto dall'incidenza degli incidenti ICT sul totale delle attività economiche, tra il 2022-2019 l'incremento era stato poco più di 5 punti percentuali, mentre tra il 2024 e il 2022 di solamente 0,1 punti percentuali. Questo andamento può essere associato alle soluzioni sulla sicurezza adottate dalle imprese che hanno permesso di ridurre i rischi, dopo l'implementazione rapida e massiccia di sistemi informatici per gestire la crisi sanitaria della pandemia di COVID-19, spesso non supportata da misure di sicurezza adeguate. Il consolidamento

delle strategie di difesa negli anni ha quindi portato ad un incremento minore degli attacchi informatici riusciti, portando diversi settori economici a ridurre le risorse impiegate sulla sicurezza. La minaccia dei cybercriminali resta comunque significativa, le difese attuali non eliminano i rischi di nuove vulnerabilità future date da attacchi più sofisticati. Diventa determinante quindi, continuare a rafforzare le strategie di difesa, garantendo aggiornamenti adeguati all'evoluzione delle minacce informatiche.

4.3 Confronto tra le dimensioni aziendali

L'esposizione e gli impatti degli attacchi informatici dipendono da molte variabili, tra queste la dimensione aziendale gioca un ruolo importante. Le imprese più grandi, grazie a maggiori risorse a disposizione possono implementare difese più sofisticate, ma allo stesso tempo offrendo guadagni superiori per gli attaccanti risultano bersagli privilegiati. Analizzare il legame tra la grandezza aziendale e la frequenza degli attacchi subiti permette di comprendere meglio le criticità di ciascun segmento. Per la suddivisione aziendale in base alla dimensione del personale, nel dataset sono presenti quattro classi di grandezza:

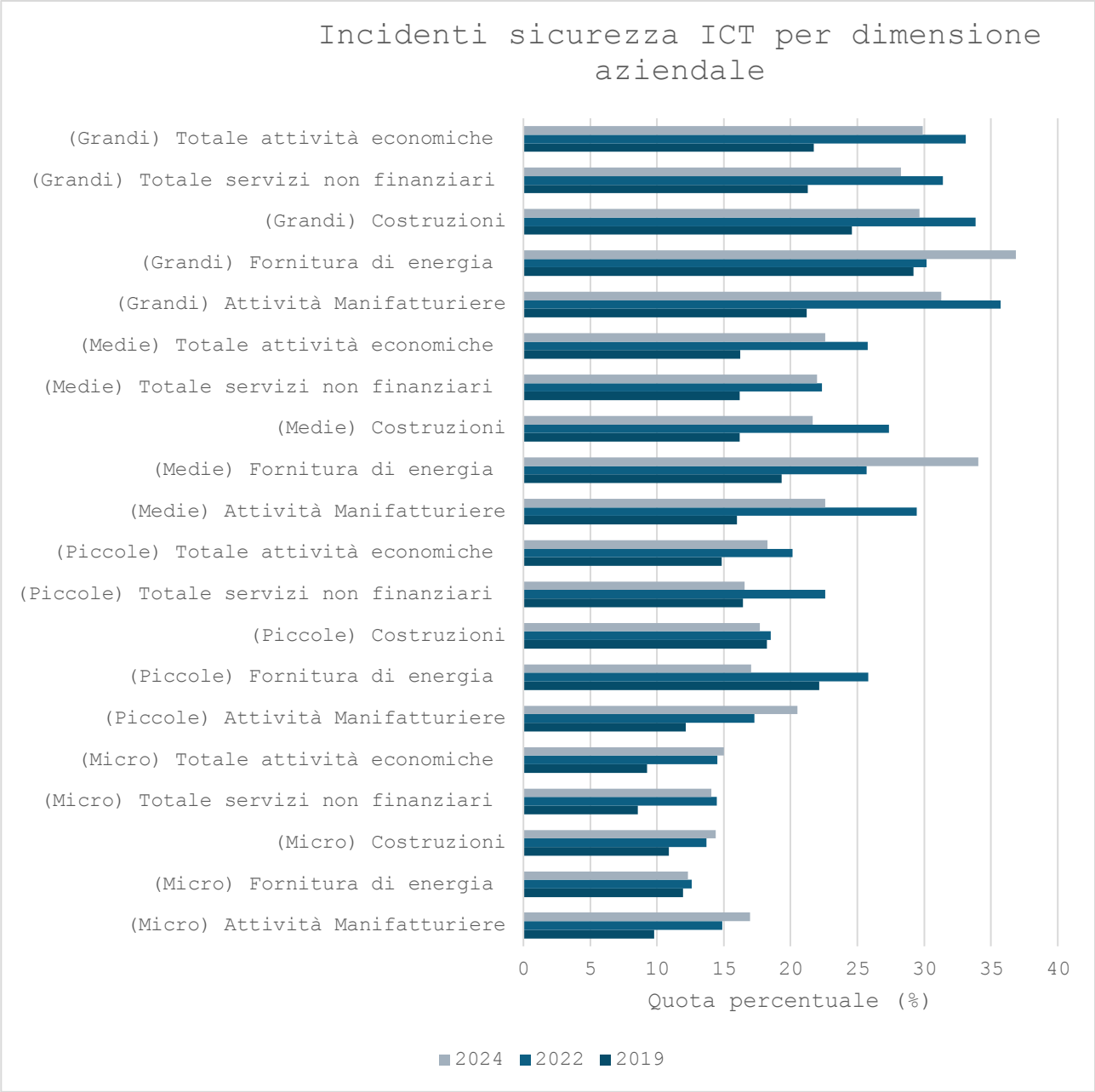
- **Micro imprese**: con un organico che varia tra 10 e 49 dipendenti.
- **Piccole imprese**: con un organico che varia tra 50 e 99 dipendenti.
- **Medie imprese**: con un organico che varia tra 100 e 249 dipendenti.
- **Grandi imprese**: con un organico di oltre 250 dipendenti.

Il dataset suddiviso in base alla dimensione aziendale non fornisce un livello di dettaglio equivalente ai dati aggregati delle aziende con 10 o più lavoratori, le informazioni presenti riguardano solamente i sottostanti settori:

- Attività Manifatturiere
- Fornitura di energia
- Costruzioni
- Totale servizi non finanziari
- Totale attività economiche

4.3.1 Frequenza incidenti digitali per dimensione aziendale

L'analisi della frequenza degli incidenti di cybersecurity in base al numero di dipendenti può essere fatta considerando i trend presenti nel grafico successivo.



(Grafico 20- Incidenti sicurezza ICT per dimensione aziendale e settore)

Le grandi imprese, come era prevedibile, risultano quelle più colpite in tutti i settori considerati, una gestione di enormi quantità di dati e le difficoltà nel controllare sistemi più complessi, le rendono maggiormente esposte rappresentano obiettivi più redditizi per i cybercriminali. Per le aziende medie e piccole l'incidenza degli attacchi si riduce tra le prime e le seconde, con entrambe che presentano le forniture di energia come settore più colpito. Le microimprese sono le meno esposte, ma con un aumento costante nel tempo, minori risorse da dedicare alle difese informatiche potrebbero aver attirato sempre più attenzioni da parte dei cybercriminali.

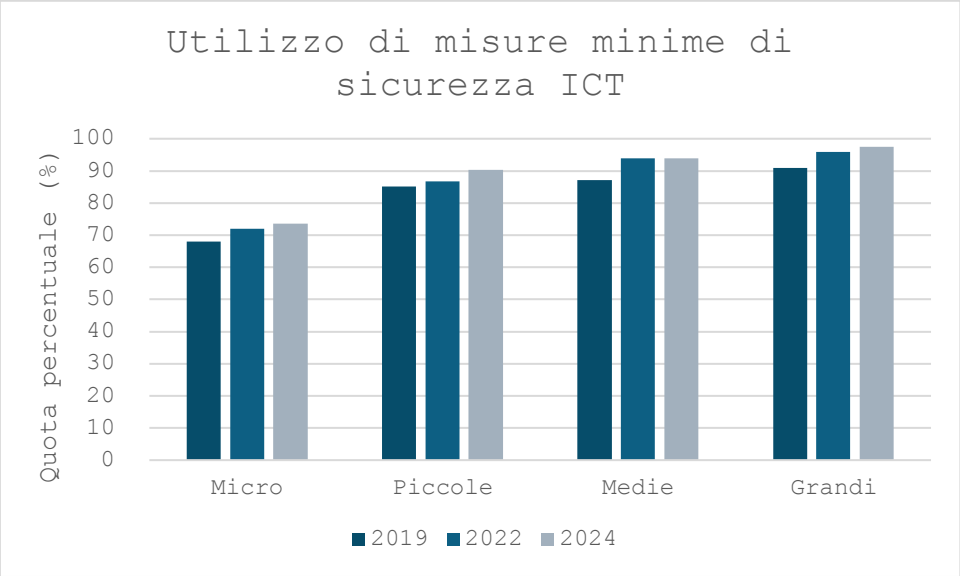
Nel complesso le tendenze mostrate sono comparabili con quelle osservate precedentemente per i dati aggregati, ma la dimensione influisce significativamente sull'incidenza delle aggressioni. Nonostante

la quota generale sia inferiore, anche le aziende con minor numero di personale dovrebbero prestare attenzione alla cybersicurezza, con gli attacchi in continua crescita negli anni.

4.3.2 Strategie di difesa per dimensione aziendale

Misure di sicurezza per dimensione aziendale

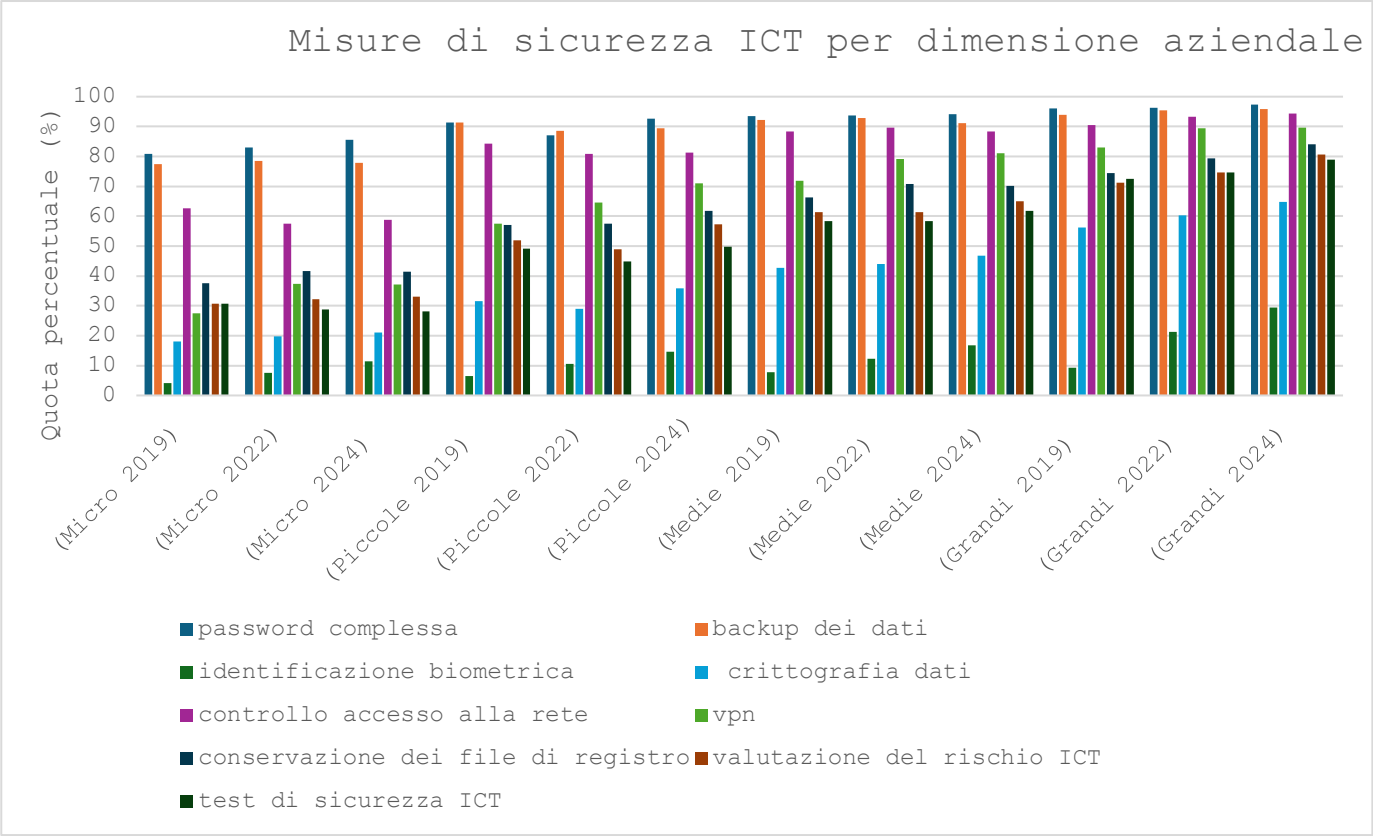
Come per il campione aggregato anche per la divisione in base alla dimensione aziendale sono presenti i dati sulle misure di sicurezza adottate dalle imprese.



(Grafico 21- misure minime di sicurezza in base alla dimensione aziendale)

La tendenza rispecchia pienamente in campione generale aggregato, in quasi praticamente tutti i periodi considerati le misure di sicurezza minime sono adottate dal 70% delle imprese, con una crescita costante nel tempo. Le microimprese, che spesso devono gestire una mole di dati inferiore rispetto ad aziende con un maggior numero di personale, hanno una percezione del pericolo minore e questo le può portare a non adottare sempre misure minime di sicurezza. Per le altre classi di grandezza invece la sicurezza è considerata un argomento rilevante, con una media generale che supera il 90% di adozione.

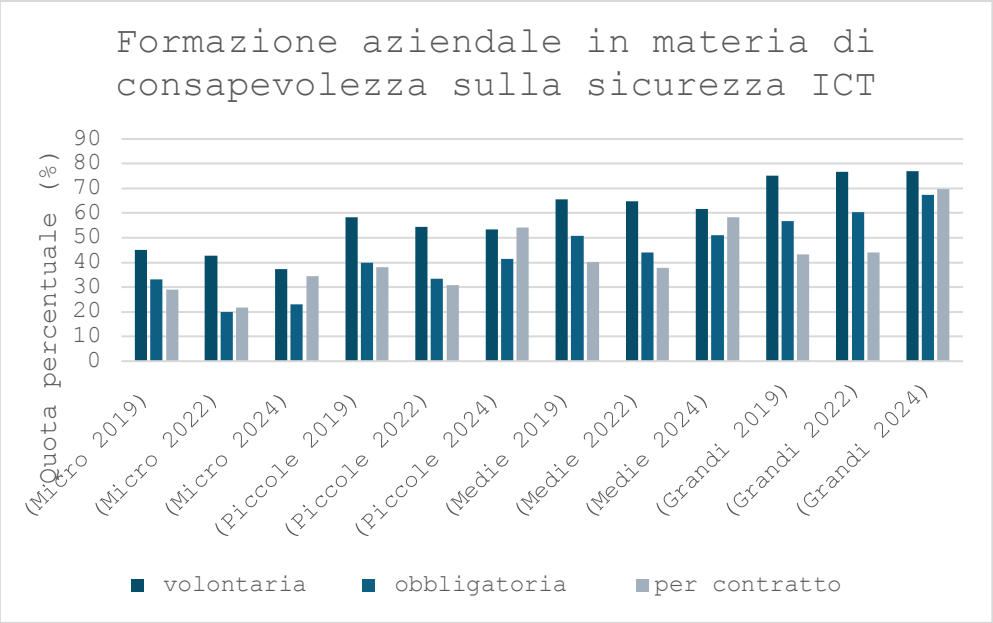
Nel dettaglio delle misure di sicurezza più utilizzate si può subito notare un andamento crescente dalle microimprese alle grandi per tutte le tipologie di sistemi di sicurezza.



(Grafico 22- misure di sicurezza adottate in base alla dimensione aziendale)

Come per i casi precedenti anche sulle singole contromisure le grandi imprese presentano livelli più elevati di incidenza. Tra le specifiche misure di sicurezza, l'utilizzo di password complesse è ampiamente adottato per tutte le classi di grandezza, anche grazie alla sua semplicità di implementazione ed efficacia. Il backup dei dati, tra le misure minime di sicurezza come per le password, non varia sensibilmente tra le diverse categorie, essendo fondamentale per avere un rapido ripristino in caso di incidenti. La crittografia dei dati e la VPN risentono fortemente della dimensione aziendale, con grandi volumi di informazioni da gestire la cifratura di esse consente di avere una protezione anche in caso di furto dei dati. Mentre con un grande organico distribuito in più sedi o la possibilità di lavorare in smart working, più comune nelle imprese grandi, una VPN consente l'accesso sicuro alle reti aziendali a tutti i dipendenti.

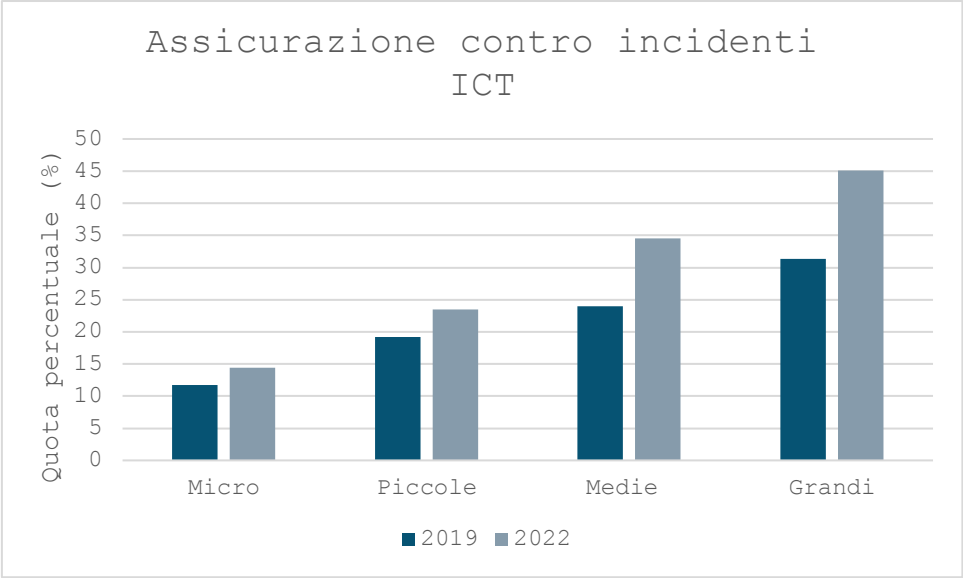
La formazione dei dipendenti in materia di sicurezza informatica è fondamentale tanto quanto l'utilizzo delle migliori difese, esistono diversi attacchi di ingegneria sociale che sfruttano l'errore umano per poter entrare dentro i sistemi.



(Grafico 23- Formazione in materia di consapevolezza sulla sicurezza ICT per dimensione aziendale)

La tendenza è sempre crescente in base al numero di dipendenti, le aziende con una maggiore dimensione del personale sono maggiormente a rischio che un errore umano possa creare una breccia nella sicurezza informatica, per cui hanno un interesse superiore a formare i propri dipendenti. Dal lato opposto le microimprese, con una dimensione aziendale piccola, non è detto che tutti i dipendenti abbiano l'accesso a risorse IT, richiedendo meno persone per gestire i sistemi informatici risulta meno necessario formare l'intero organico. In generale le tendenze corrispondono al campione aggregato, la formazione volontaria diminuisce nel tempo con un aumento di quella obbligatoria e per contratto.

Come per il campione complessivo, l'incidenza percentuale delle imprese che sottoscrivono assicurazioni sulla cybersecurity sono disponibili solo per i periodi 2019 e 2022.



(Grafico 24– stipula di polizze assicurative per dimensione aziendale)

Le aziende più grandi solo le più propense a sottoscrivere polizza assicurative, la loro esposizione maggiore agli attacchi cyber le rende più consapevoli dei rischi e rende conveniente avere un'assicurazione per coprire eventuali danni. Le microimprese invece, tendono a risparmiare da questo punto di vista, risorse minori disponibili e una frequenza di attacchi subiti più bassa potrebbero essere tra le motivazioni principali. Con l'aumentare delle aggressioni informatiche il numero di polizze assicurative è aumentato nel tempo, con un mondo sempre più interconnesso i rischi derivanti dai cybercriminali sono in continuo aumento e con essi aumenta anche la consapevolezza di tutelarsi dai possibili danni.

In conclusione, la grandezza delle imprese incide in modo significativo sia sul rischio di essere colpiti da incidenti sulla sicurezza ICT sia sulla capacità di adottare misure di protezione adeguate. Le aziende più grandi, a causa dei loro asset di valore e alla maggiore visibilità, rappresentano obiettivi di alto interesse per i cybercriminali, ma allo stesso tempo possono permettersi più facilmente di implementare strumenti di sicurezza sofisticati rispetto alle piccole e medie imprese.

4.4 Analisi dati interdipendenza strutturale e di mercato

Utilizzando i modelli discussi precedentemente, nei prossimi paragrafi verranno analizzati i dati reali, e saranno confrontati con le aspettative date dalle teorie economiche sull'influenza delle interdipendenze.

Nel dataset ISTAT sono presenti diversi parametri per provare a categorizzare i settori economici in base alle loro interdipendenze. Il periodo preso in considerazione è stato il 2024, e i dati sono stati analizzati per il campione aggregato, imprese con 10 o più dipendenti. I parametri utilizzati per la categorizzazione sono:

Commercio elettronico, riguardo l'incidenza percentuale delle vendite online via web e/o sistemi di tipo EDI (Electronic Data Interchange).

Vendite online, riguardo l'incidenza percentuale delle vendite online rispetto al totale.

Cloud computing, riguardo l'incidenza percentuale delle imprese che acquistano servizi di cloud computing.

Indicatori DESI (Digital Economy and Society Index), in merito alla quota percentuale delle imprese che hanno realizzato vendite su piattaforme digitali online per valori uguali o superiori all'1% del fatturato complessivo.

Tecnologie per l'organizzazione interna, di filiera e internet delle cose, riguardo l'incidenza percentuale delle aziende che condividono dati in rete con fornitori e clienti.

Numero di imprese e fatturato totale dei diversi settori economici

Interdipendenza strutturale

L'interdipendenza strutturale tra le imprese nel contesto digitale si manifesta quando più aziende utilizzano infrastrutture informatiche comuni, rendendosi reciprocamente vulnerabili agli stessi rischi e benefici.

I principali parametri utilizzati per generare il punteggio sono stati il commercio elettronico, vendite via web o altri sistemi, indicatori DESI che possono essere considerati parametri di dipendenza da infrastrutture informatiche comuni, poiché le imprese che operano online si appoggiano a server e piattaforme condivise. Anche l'utilizzo di cloud computing e la condivisione dei dati in rete con fornitori e clienti sono parametri di interdipendenza strutturale, aumentano l'efficienza del sistema e degli investimenti in sicurezza, ma allo stesso tempo possono anche amplificare i rischi di compromissione, poiché una vulnerabilità in un nodo della rete può propagarsi rapidamente a tutti gli altri soggetti coinvolti.

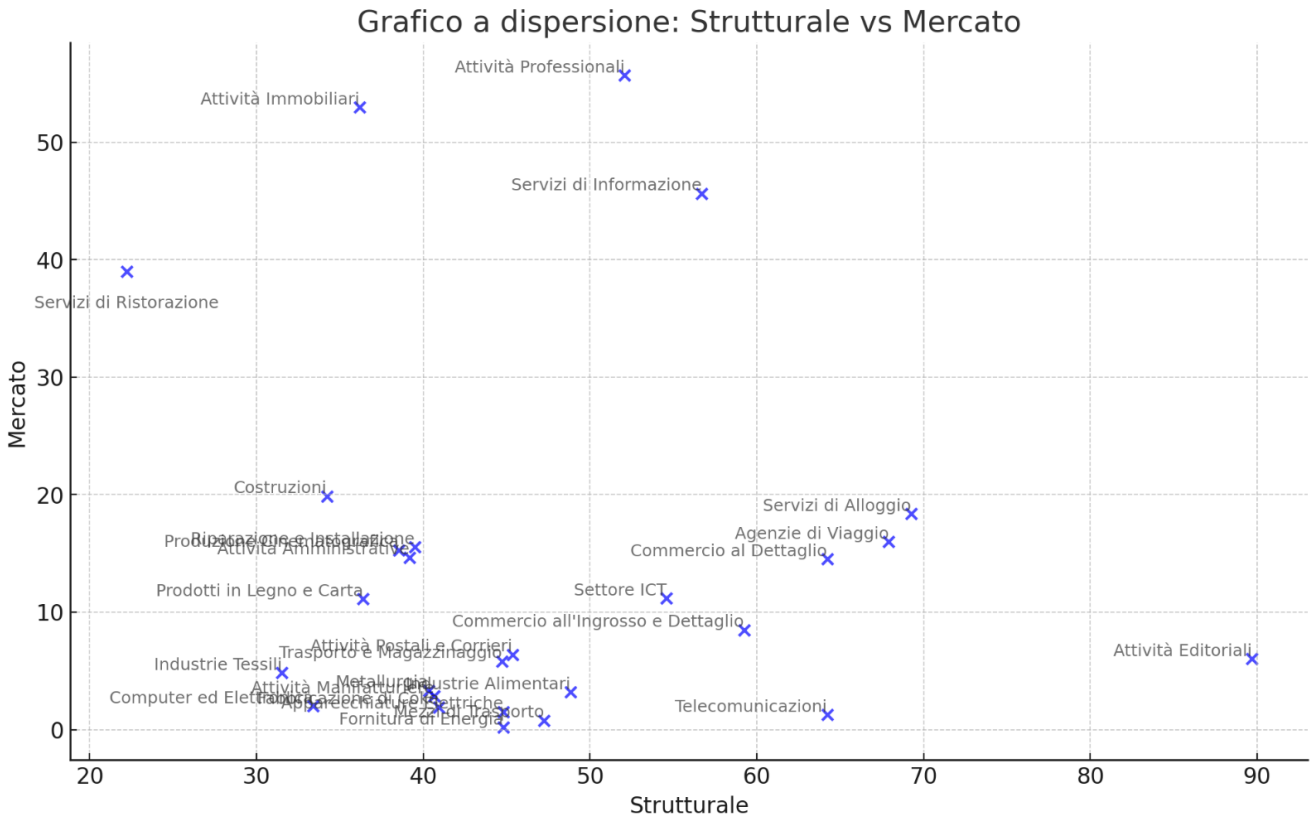
Interdipendenza di mercato

Le interdipendenze di mercato riguardano le relazioni competitive tra imprese che operano nello stesso settore economico senza necessariamente condividere infrastrutture digitali, ma che sono legate dalle dinamiche concorrenziali del mercato in cui competono. In questo contesto, il grado di

interdipendenza tra le imprese è determinato dalla struttura del mercato e dal livello di competizione presente all'interno del settore. Per quantificare questa interdipendenza e avere grado approssimato di concentrazione di mercato, è stato utilizzato il rapporto tra il numero totale di imprese di un determinato settore e il fatturato totale generato nello stesso settore. Questo parametro offre una misura indicativa della distribuzione del fatturato tra le imprese e della frammentazione del mercato, permettendo di valutare, anche se in maniera approssimata, il livello di competitività e l'impatto strategico delle decisioni di un'impresa sui suoi concorrenti.

Un valore elevato di questo rapporto indica un settore caratterizzato da un alto numero di imprese rispetto al fatturato complessivo, suggerendo un mercato frammentato e competitivo, al contrario valori bassi del rapporto indicano un mercato più concentrato, dove poche imprese detengono la maggior parte del fatturato totale.

Tramite questi parametri è stata calcolata una media pesata per assegnare il valore dei vari settori economici nelle due classi di interdipendenza e creato un grafico a dispersione.



(Grafico 25– grafico a dispersione confronto tra interdipendenza strutturale e di mercato)

Il grafico mostra il rapporto tra interdipendenza tecnica e di mercato dei settori economici presenti nel dataset. Attività dei servizi di ristorazione, immobiliare e le costruzioni rispettano le aspettative, essendo servizi non interconnessi tra di loro in maniera significativa e sono settori competitivi con molte aziende presenti nel territorio anche a poca distanza le une dalle altre.

La posizione elevata di interdipendenza strutturale dei servizi di alloggio potrebbe essere dovuta all'utilizzo sempre più diffuso delle piattaforme online da parte dei consumatori, i locatori devono affidarsi a questi servizi per poter ottenere visibilità, concorrendo con tutti gli host presenti sulla rete.

Le attività professionali, scientifiche e tecniche sono il secondo settore per numero di imprese, e risultano avere il valore più elevato di interdipendenze di mercato, mentre per quelle strutturali, le attività editoriali occupano il primo posto, una delle motivazioni potrebbe essere il progressivo abbandono del formato fisico in favore di quello digitale, sfruttando piattaforme e infrastrutture condivise per la distribuzione dei contenuti.

La disposizione generale, con alcune limitazioni, risulta coerente con le dinamiche tipiche dei vari settori economici presenti e con la teoria di base utilizzata.

4.4.1 Analisi comparativa dati reali e classificazione teorica

Dal grafico a dispersione creato precedentemente, si può provare a organizzare i settori economici in quattro classi in base alle loro interconnessioni. La dispersione dei dati presenti nel grafico evidenzia un raggruppamento nel basso centro, rendendo difficile la suddivisione equilibrata nelle quattro classi, per questo motivo sono stati presi come riferimento i settori più significativi. La classificazione adottata è riportata di seguito:

Interdipendenza bassa di mercato e bassa strutturale

Industrie tessili e dell'abbigliamento, Computer e prodotti di elettronica e ottica, ed fabbricazione di coke e di prodotti derivanti dalla raffinazione del petrolio sono i principali settori che possono essere inclusi in questa categoria. Riguardato mercati che tendono ad essere composti non da troppi competitors, con una concorrenza limitata dovuta anche ad un elevato capital-intensive iniziale e in diversi casi prodotti specifici che non permettono una facile sostituzione dei fornitori e produttori. In questi settori, anche in un comparto tecnologico come quello dei computer e prodotti di elettronica, ma che riguardano la produzione hardware e non software, la produzione e la distribuzione rimangono spesso ancora legate a filiere tradizionali con un uso limitato di infrastrutture IT condivise.

Interdipendenza bassa di mercato alta strutturale

I settori delle telecomunicazioni, attività editoriali e agenzie di viaggio e tour operator si appoggiano principalmente a strutture digitali comuni. Attività editoriali e agenzie di viaggio utilizzano le infrastrutture condivise per la distribuzione e prenotazione dei servizi, mentre le telecomunicazioni condividono spesso le medesime infrastrutture di rete. Il mercato delle telecomunicazioni, inoltre, tende a essere concentrato in pochi grandi operatori, spesso oligopoli regolamentati, limitando la competizione diretta, come anche le attività editoriali che possono godere di un pubblico fidelizzato che riduce la concorrenza.

Interdipendenza bassa strutturale e alta di mercato

Le attività dei servizi di ristorazione, immobiliari e il settore delle costruzioni principalmente tendono ad utilizzare sistemi informatici con una bassa condivisione a livello settoriale, ma più su misura aziendale per la gestione dei progetti e delle operazioni, sono inoltre tutti settori altamente competitivi, con svariate aziende presenti nel territorio e che offrono servizi non troppo differenziati che non comportano elevati costi di switching al consumatore.

Interdipendenza alta strutturale e alta di mercato

Altre attività dei servizi di informazione e le attività professionali, scientifiche e tecniche presentano valori elevati di entrambe le interdipendenze, questi settori fanno largo uso di infrastrutture IT comuni

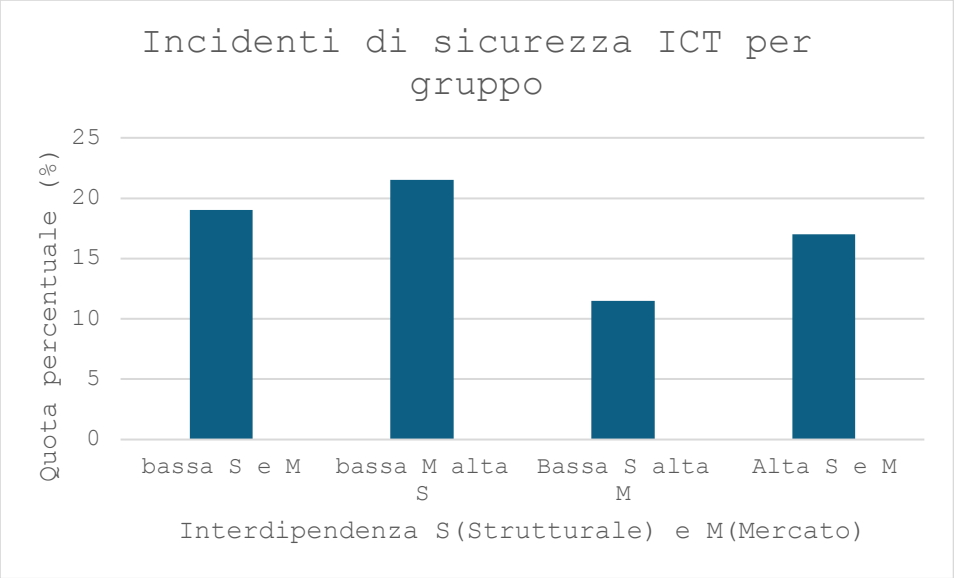
per la distribuzione e gestione dei dati, ed eventuali collaborazioni. Entrambi i settori riguardano mercati competitivi, con aziende che offrono servizi simili facilitando il passaggio dei consumatori tra i diversi concorrenti rendendo il settore sensibile alle dinamiche di prezzo, qualità e innovazione.

Comparazione parametri dei gruppi

Utilizzando i settori economici individuati per le diverse categorie create è stata determinata la media per ogni gruppo degli attacchi subiti e il livello delle risorse utilizzate nella difesa, in modo da poterne confrontare l'andamento ed osservare se vengono rispettate le aspettative della teoria,
con i settori aventi un elevata interdipendenza strutturale ma bassa di mercato che dovrebbero mostrare elevati investimenti in cybersicurezza generali, dovuti alla maggior efficienza delle risorse destinate alla difesa in comune, rispetto a quelli con caratteristiche opposte.
Sempre secondo quanto evidenziato dalla letteratura, per i settori con interdipendenze basse strutturali e alte di mercato dovrebbero essere presenti minori incentivi dovuti agli spillover di mercato, che riducono le possibilità di acquisire le quote di ricavo dei rivali all'aumentare dell'interdipendenza.

4.4.2 Incidenti di sicurezza ICT

Come già effettuato per i parametri in aggregato e divisi in base alla dimensione del personale aziendale, verranno analizzati i dati relativi agli attacchi informatici contro i diversi gruppi.



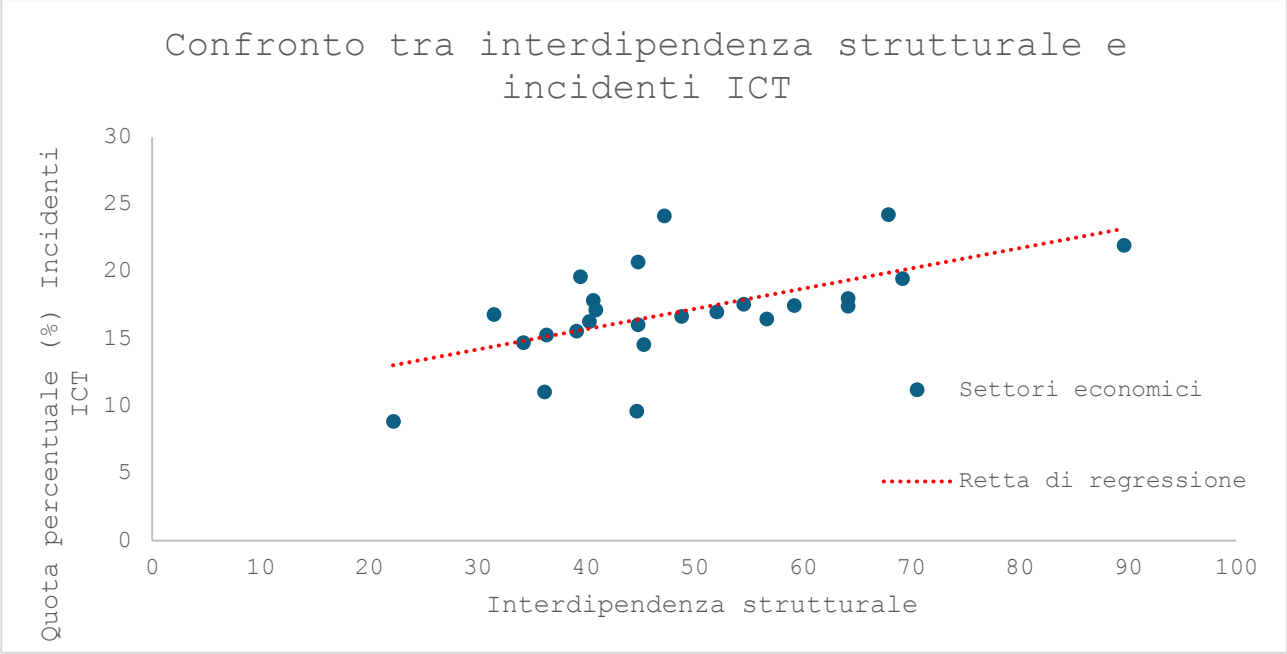
(Grafico 26– confronto incidenza attacchi per gruppo di interdipendenza)

Analizzando il grafico si può osservare il gruppo più colpito risulta essere quello con alta interdipendenza strutturale e bassa di mercato, la diffusa presenza di strutture IT condivise e una bassa frammentazione del mercato risultano essere degli incentivi favorevoli per i criminali informatici,

con la compromissione di un nodo comune che permette poi di estendere l'attacco anche al resto della rete. Invece, elevati valori di interdipendenza di mercato, settori altamente competitivi in cui il fatturato totale viene distribuito su più imprese rende i benefici di un'intrusione informatica minori, a causa della più bassa possibilità di guadagno per intrusione, in relazione a un mercato poco competitivo e oligopolistico, con il gruppo con bassa interdipendenza strutturale e alta di mercato che risulta essere vittima del minor numero di attacchi.

4.4.3 Confronto tra interdipendenza e incidenti ICT

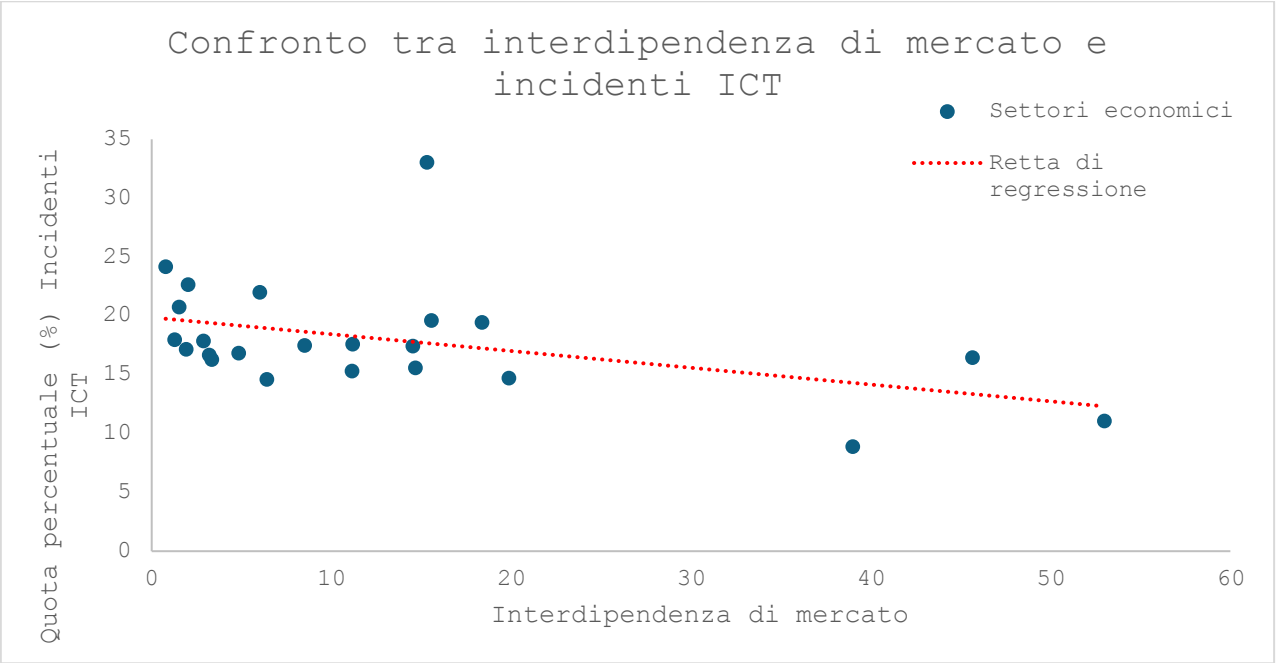
Nei paragrafi precedenti è stata osservata l'efficacia degli investimenti in sicurezza informatica in relazione agli attacchi subiti. Per confrontare l'incidenza degli attacchi con il livello di interdipendenza delle aziende dei settori economici presenti nel dataset, sono stati costruiti i seguenti grafici.



(Grafico 27– confronto tra attacchi informatici e interdipendenza strutturale per settore economico)

La retta di regressione dimostra in modo statisticamente significativo (p-value= 0.0018), che all'incrementare dell'interdipendenza strutturale dei settori economici e la conseguente esposizione nel mondo digitale, crescono anche gli incidenti ICT.

Una maggior dipendenza da piattaforme digitali condivise, con la possibilità dei cybercriminali di propagare l'attacco lungo la rete, aumentando il potenziale ritorno, risulta essere un obiettivo più attraente per gli hacker.



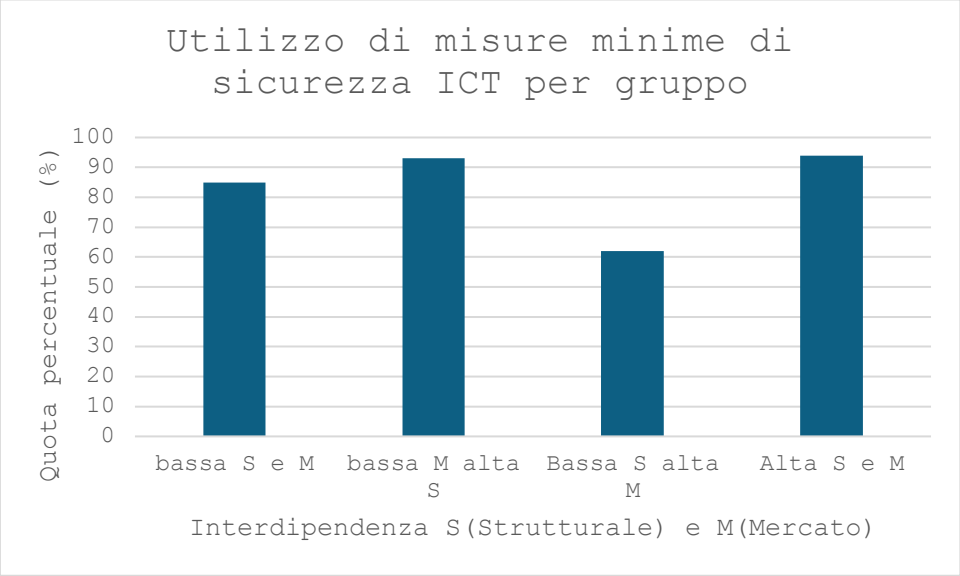
(Grafico 28 - confronto tra attacchi informatici e interdipendenza di mercato per settore economico)

Per gli attacchi e le interdipendenze di mercato, sempre con una retta di regressione statisticamente significativa (p-value=0,048), risulta un risultato opposto, all'aumentare della competitività e quindi della dispersione dei ricavi del settore ad un maggior numero di imprese, gli incentivi dei criminali informatici diminuiscono. La possibilità di ottenere minori ritorni economici da un attacco, e spesso rimanendo violazioni isolate senza potersi propagare ad altre aziende interconnesse, riducono gli incentivi degli attaccanti e i rischi delle imprese.

4.4.4 Misure di sicurezza per gruppo

Nel dataset non sono presenti valori monetari degli investimenti in cybersicurezza dei diversi settori, spesso sono dati che le imprese non rendono di pubblico dominio, per provare a confrontare le aspettative dei modelli teorici, come livello di investimenti in sicurezza informatica è stata utilizzata la quota percentuale di adozione delle difese minime di cybersicurezza che possono rappresentare una misura approssimata di un livello di risorse destinate alla sicurezza informatica.

Analizzando le misure minime di sicurezza adottate dai diversi gruppi di interdipendenza si può osservare se il comportamento delle aziende rimane coerente.



(Grafico 29– misure di sicurezza minime adottate per gruppo di interdipendenza)

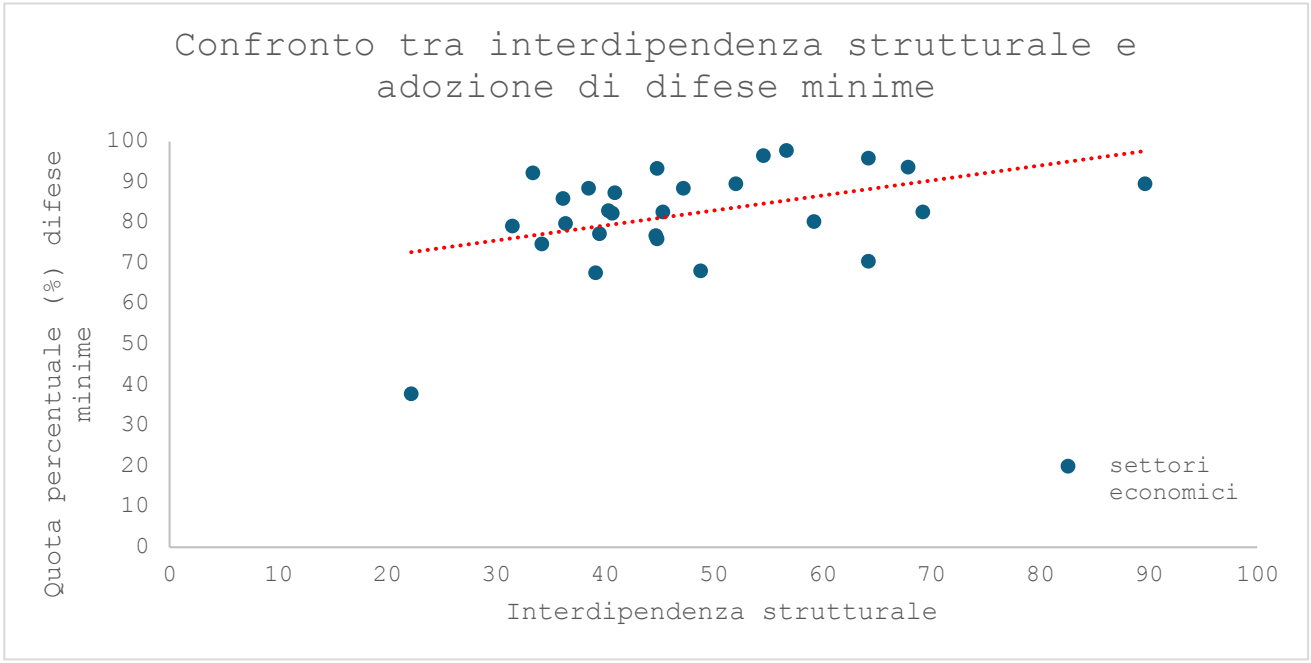
I gruppi che subiscono il numero più elevato di incidenti ICT sono anche quelli che adottano in modo più esteso le misure minime di sicurezza. La consapevolezza di una maggior esposizione ai rischi è fondamentale per investire in modo corretto nelle strategie di difesa e gestire le minacce informatiche. Come adozione di difese minime, i settori con entrambe le interdipendenze elevate risultano avere la quota percentuale più alta fra i gruppi, anche se praticamente quasi a pari merito con bassa M e alta S, che ha registrano i maggiori attacchi subiti.

In mancanza dei dati specifici sugli investimenti in cybersicurezza delle singole imprese non si possono fare confronti dettagliati con la letteratura, in particolare per il fenomeno del free riding ed il conseguente sotto investimento, che nell'analisi dei dati reali, in presenza di elevate interdipendenze strutturali non sembra causare gravi problemi generali di deficit degli investimenti con valori di oltre il 90% delle imprese che adottano le misure di protezione minime per entrambi i gruppi con alta interdipendenza strutturale.

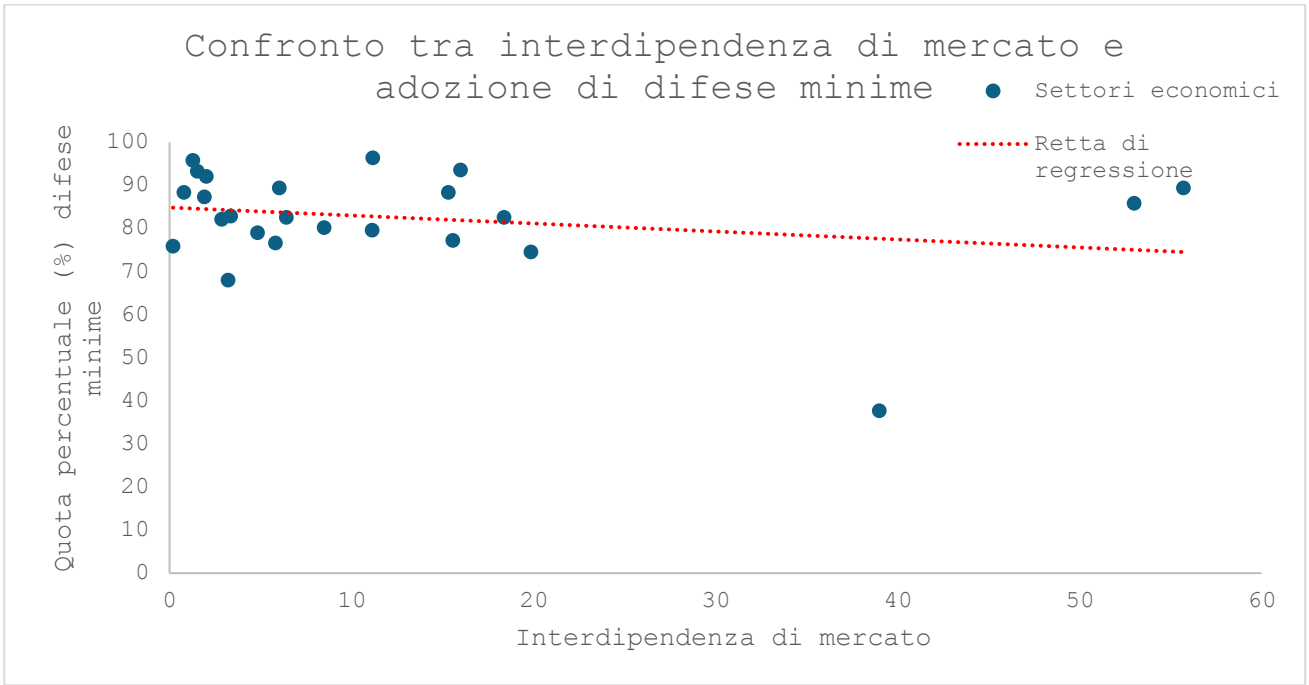
Gli investimenti in sicurezza per elevati valori di interdipendenze di mercato sono in parte coerenti con la frequenza degli attacchi, che diminuiscono all'aumentare degli spillover di mercato, in valore assoluto rimangono comunque insufficienti, con poco più del 60% delle imprese che investe risorse per adottare le misure minime di sicurezza, il minor numero di risorse da proteggere in un mercato frammentato e il relativo budget di cybersicurezza inferiore potrebbero essere tra i principali motivi di questo scenario. Le minori risorse destinate alle difese per il gruppo bassa S e alta M sono anche riconducibili alla natura intrinseca dei settori appartenenti a questa categoria, le attività della

ristorazione, immobiliari e le costruzioni, si basano prevalentemente su asset fisici e infrastrutture materiali, mentre l'aspetto digitale rappresenta solo una parte marginale delle loro operazioni. In questi ambiti, la sicurezza informatica può essere percepita come meno prioritaria rispetto ad altri settori più digitalizzati, portando a un'allocazione inferiore di risorse nelle difese informatiche.

Questa relazione può essere ulteriormente verificata, confrontando i dati delle interdipendenze per tutti i settori economici presenti nel dataset con le risorse utilizzate per le difese.



(Grafico 30 - confronto tra adozione delle difese minime e interdipendenza strutturale per settore economico)



(Grafico 31- confronto tra adozione delle difese minime e interdipendenza di mercato per settore economico)

Anche in questo caso per il primo grafico la correlazione è statisticamente significativa (p-value= 0.023), con il progressivo aumento dell'interdipendenza strutturale dei settori economici crescono anche gli investimenti destinati all'adozione delle misure minime di sicurezza. Per le interdipendenze di mercato invece, la relazione risulta essere debolmente negativa all'aumentare degli spillover di mercato.

Dai dati emerge come le aziende che possiedono un'alta interdipendenza strutturale sono le più esposte a minacce cyber e per questo motivo implementano sistemi di difesa migliori, rispetto alle imprese meno dipendenti da piattaforme digitali condivise. La consapevolezza dei rischi informatici dei vari settori diventa quindi fondamentale, non solo a livello aziendale ma anche istituzionale, per promuovere politiche efficaci ed incentivagli gli investimenti sulla sicurezza.

In conclusione, delle relazioni tra i dati reali e la letteratura sono in parte presenti, partendo dalle interdipendenze di mercato, le teorie sul modello si basavano sulle ipotesi che l'intero ricavo del settore X veniva diviso in parti uguali dalle N imprese presenti, ed in caso di violazione l'azienda perdeva interamente la sua quota. Questa semplificazione non trova pieno riscontro nella realtà dove i ricavi non sono distribuiti equamente, ma soprattutto un'impresa rischia di perdete interamente la sua quota di mercato solo in caso di violazioni estremamente gravi, riducendo quindi in parte gli incentivi che permettevano di acquisire i ricavi dei rivali. Il calo dei benefici per le imprese ad investire nelle difese con l'aumento degli spillover di mercato presente nella letteratura è evidenziato dai dati reali con una relazione debolmente negativa tra l'investimento in sicurezza e l'aumentare delle interdipendenze di mercato, ma, essendo questo effetto relativamente debole, occorrerebbero dati più precisi per analizzare e confermare in modo robusto questa dinamica, attualmente non disponibili.

La maggior dispersione delle risorse economiche del settore su più imprese si dimostra invece significativa nel ridurre gli incentivi dei criminali informatici ad attaccare, come previsto dalla teoria, ma rimane di primaria rilevanza, anche con elevate interdipendenze di mercato, la considerazione della specificità di ogni settore economico, che presenta differenti gradi di esposizione digitale, i quali incidono significativamente sia sulla vulnerabilità agli attacchi sia sugli incentivi a implementare misure difensive adeguate.

Nella letteratura delle interdipendenze strutturali invece, un loro aumento migliorava le difese delle reti condivise data la maggior efficacia degli investimenti comuni, questo fenomeno viene osservato anche nei dati reali, con un incremento delle difese adottate all'aumentare dell'interdipendenza strutturale. Il fenomeno del free riding, in assenza di dati dettagliati sugli investimenti in cybersicurezza di ciascuna impresa, non può essere analizzato, nonostante le difese complessive del sistema non risultino compromesse, non è possibile stabilire se ciò derivi da un contributo uniforme di tutte le aziende o se da una partecipazione limitata di alcune.

In contrasto con quanto visto nel modello teorico risulta invece una maggior propensione degli hacker ad attaccare imprese con la crescita degli spillover tecnici. Nella realtà, gli individui spesso non sono neutrale al rischio, sebbene l'incremento delle difese teoricamente dovrebbe ridurre gli incentivi degli attaccanti, l'elevata esposizione digitale e la possibilità di compromettere una rete, estendendo l'attacco ad altre aziende collegate, fanno di questi settori un bersaglio privilegiato per i criminali informatici.

Questi risultati possono delineare un percorso per delle ricerche future più approfondite, che potranno indagare ulteriormente tali dinamiche in presenza di dataset più esaustivi riguardanti gli investimenti in sicurezza informatica.

Conclusioni

Le evidenze raccolte nel corso di questa tesi hanno permesso di comprendere in maniera approfondita come il rischio cibernetico stia assumendo un ruolo sempre più determinante a livello globale, l'evoluzione degli attacchi informatici, con le loro modalità sempre più sofisticate e pericolose, non rappresenta più un fenomeno circoscritto, ma una componente quasi inevitabile nel panorama digitale odierno.

L'espansione quasi esponenziale delle infrastrutture digitali avvenuta negli ultimi anni, in cui la pandemia di Covid-19 e il lockdown dovuto ad essa hanno contribuito enormemente, ha incrementato le vulnerabilità presenti, espandendo le superfici d'attacco a disposizione dei cybercriminali sottolinea la necessità di adottare strategie difensive adeguate, in grado di rispondere alle nuove sfide poste dalle minacce emergenti.

Un quadro normativo appropriato, sia sul piano nazionale che a livello europeo, riveste un'importanza cruciale, fornendo una base regolamentare per la protezione dei dati sensibili e per promuove standard di sicurezza condivisi, infatti, le singole direttive legislative, pur essendo indispensabili, non possono costituire l'unica strategia di difesa, la sicurezza informatica passa anche attraverso una formazione continua dei dipendenti e consumatori e l'adozione di soluzioni tecnologiche sempre più avanzate.

Dal punto di vista economico, il mercato della cybersecurity sta vivendo una crescita notevole, trainato dalla necessità di proteggere le imprese, le istituzioni e i consumatori da minacce che, se non contrastate, possono comportare gravi danni sia in termini finanziari che di reputazione.

L'applicazione di modelli economici, e della teoria dei giochi, ha contribuito a fornire una lettura delle dinamiche di investimento in sicurezza, evidenziando come la cooperazione e l'interdipendenza tra gli attori del settore siano elementi fondamentali per strutturare una risposta efficace e coordinata.

Come può accadere per qualsiasi forma di investimento, anche nel caso della sicurezza informatica possono verificarsi fallimenti di mercato, che si manifestano quando le decisioni nella spesa delle risorse non rispecchiano i costi e benefici effettivi per l'intera società.

I dati analizzati hanno inoltre rivelato una distribuzione non uniforme degli attacchi informatici tra i vari comparti industriali, alcuni settori risultano particolarmente esposti e vulnerabili, le motivazioni sono diverse, la maggior esposizione nel mondo digitale e la redditività di un attacco sono le cause principali, ma anche l'implementazione di difese inefficaci e risorse limitate nella sicurezza contribuiscono ad attirare le attenzioni dei criminali informatici.

In un'epoca in cui la digitalizzazione è presente in ogni aspetto della vita, sia sociale che economica, la resilienza informatica non può più essere relegata a un ruolo marginale, ma deve essere considerata una priorità strategica, solo attraverso un approccio coordinato, che sappia combinare strumenti tecnologici all'avanguardia, un supporto delle istituzioni tramite regolamentazioni e una formazione

diffusa sulla sicurezza, sarà possibile fronteggiare in modo adeguato le sfide poste dalla cybersicurezza del futuro.

Le conclusioni che emergono da questo studio, pertanto, invitano a considerare il rischio cibernetico come un elemento centrale nella definizione delle strategie di sviluppo e protezione delle organizzazioni. Le enormi possibilità che offre la digitalizzazione non devono essere oscurate dalle minacce, l'impegno nel rafforzare la resilienza informatica rappresenta non solo una risposta necessaria ai cybercriminali, ma anche un investimento strategico per la stabilità e la crescita futura della società nel suo complesso.

Referenze

ACN relazione annuale 2023. https://www.acn.gov.it/portale/relazione-annuale-2023

'ACN_strategia_nazionale_cyberspazio'. https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

'Annual-Dark-Web-Report-2024'. https://socradar.io/wp-content/uploads/2025/01/Annual-Dark-Web-Report-2024.pdf

Dati ISTAT. http://dati.istat.it/Index.aspx?QueryId=24864#

'WEF_Global_Cybersecurity_Outlook_2024'. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

'2024_Global-Cybersecurity-Index-E'. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Concetti chiave sulla cybersicurezza. https://www.bancaditalia.it/focus/cybersicurezza/faq-concetti-cyber/concetti-chiave/index.html#faq8761-4

Microsoft Digital Defense Report 2024. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Banca d'Italia cybersicurezza. https://www.bancaditalia.it/focus/cybersicurezza/index.html

'The 2024 Ransomware Threat Landscape White Paper'.https://www.symantec.broadcom.com/hubfs/Symantec_Ransomware_Threat_Landscape_2024.pdf

'INM Report 2024 Cost of a Data Breach'. https://www.ibm.com/reports/data-breach

'Report_Riepilogativo_Cert-AgID_2024'. https://cert-agid.gov.it/news/report-riepilogativo-sulle-tendenze-delle-campagne-malevole-analizzate-dal-cert-agid-nel-2024/#:~:text=I%20dati%20riepilogativi%20del%202024,Indicatori%20di%20Compromissione%20(IoC).&text=In%20totale%20sono%20state%20identificate%2069%20famiglie%20di%20malware.

Armstrong, M. (2006a) 'Competition in two-sided markets', The RAND Journal of Economics, 37(3), pp. 668–691. Available at: https://doi.org/10.1111/j.1756-2171.2006.tb00037.x.

Armstrong, M. (2006b) 'Competition in two-sided markets', The RAND Journal of Economics, 37(3), pp. 668–691. Available at: https://doi.org/10.1111/j.1756-2171.2006.tb00037.x.

August, T. and Tunca, T.I. (2011) 'Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments', Management Science, 57(5), pp. 934–959. Available at: https://doi.org/10.1287/mnsc.1100.1304.

Babajide Tolulope Familoni (2024) ‘CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS’, Computer Science & IT Research Journal, 5(3), pp. 703–724. Available at: https://doi.org/10.51594/csitrj.v5i3.930.

Babanina, V. et al. (2021) ‘Cybercrime: History of formation, current state and ways of counteraction’, Revista Amazonia Investiga, 10(38), pp. 113–122. Available at: https://doi.org/10.34069/AI/2021.38.02.10.

Baldoni, R. et al. (2015) Il Futuro della Cyber Security in Italia ‘Laboratorio Nazionale di Cybersecurity CINI - Consorzio Interuniversitario Nazionale per l’Informatica’.

Bay, M. (no date) ‘In search of an encompassing definition for the post-Snowden era’.

Bencivelli L., Mongardini M. (2024) ‘La sicurezza cibernetica delle imprese italiane: percezione dei rischi e pratiche di mitigazione’

Biancotti, C. (2017) ‘The Price of Cyber (In)Security: Evidence from the Italian Private Sector’, SSRN Electronic Journal [Preprint]. Available at: https://doi.org/10.2139/ssrn.3082195.

Carfora, M.F. and Orlando, A. (2024) ‘Application of the Gordon Loeb model to security investment metrics: a proposal’, Data Science in Finance and Economics, 4(4), pp. 601–614. Available at: https://doi.org/10.3934/DSFE.2024025.

Christopher, J.D. and Conway, T. (2024) ‘SANS 2024 State of ICS/OT Cybersecurity’.

Daniele D.C. (2024) Cybersicurezza e Digitalizzazione in Italia: Un'Analisi dei Modelli Economici e dei Dati Empirici.

European Union Agency for Cybersecurity. (2024) ENISA threat landscape 2024: July 2023 to June 2024. LU: Publications Office. Available at: https://data.europa.eu/doi/10.2824/0710888 (Accessed: 14 February 2025).

Ezhei, M. and Tork Ladani, B. (2020) ‘Interdependency Analysis in Security Investment against Strategic Attacks’, Information Systems Frontiers, 22(1), pp. 187–201. Available at: https://doi.org/10.1007/s10796-018-9845-8.

Fedele, A. and Roner, C. (2022) ‘Dangerous games: A literature review on cybersecurity investments’, Journal of Economic Surveys, 36(1), pp. 157–187. Available at: https://doi.org/10.1111/joes.12456.

Fedele, A., Tonin, M. and Valerio, M. (2024) 'Phishing attacks: An analysis of the victims' characteristics based on administrative data', Economics Letters, 237, p. 111663. Available at: https://doi.org/10.1016/j.econlet.2024.111663.

Fischer, E.A. (2016) 'Cybersecurity Issues and Challenges: In Brief'.

Garcia, A. and Horowitz, B. (2007) 'The potential for underinvestment in internet security: implications for regulatory policy', Journal of Regulatory Economics, 31(1), pp. 37–55. Available at: https://doi.org/10.1007/s11149-006-9011-y.

Giannelli M., Gatti A. (2024) Presupposti per la configurazione e la dichiarazione di guerra cibernetica.

Hausken, K. Returns to information security investment (2006) *Inf Syst Front* **8**, 338–349 (2006). https://doi.org/10.1007/s10796-006-9011-6 Katyal, N.K. (2003) 'Digital

Hui, Kai-Lung and Zhou, Jiali (2020) The Economics of Hacking.

Architecture as Crime Control', The Yale Law Journal, 112(8), p. 2261. Available at: https://doi.org/10.2307/3657476.

Lam, W.M.W. (2016) 'Attack-prevention and damage-control investments in cybersecurity', Information Economics and Policy, 37, pp. 42–51. Available at: https://doi.org/10.1016/j.infoecopol.2016.10.003.

Wang, S. (2017). Optimal Level and Allocation of Cybersecurity Spending.

Naldi, M. and Flamini, M. (2017) 'Calibration of the Gordon-Loeb Models for the Probability of Security Breaches', in 2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim). 2017 UKSim-AMSS 19th International Conference on Computer Modelling & Simulation (UKSim), Cambridge: IEEE, pp. 135–140. Available at: https://doi.org/10.1109/UKSim.2017.18.

Poufinas, T. and Vordonis, N. (2018) 'Pricing the Cost of Cybercrime—A Financial Protection Approach', iBusiness, 10(03), pp. 128–143. Available at: https://doi.org/10.4236/ib.2018.103008.

Nathan Alexander Sales (2013) 'REGULATING CYBER-SECURITY'

Seamans, R. and Zhu, F. (2013a) 'A Simple Model of a Three-Sided Market', SSRN Electronic Journal [Preprint]. Available at: https://doi.org/10.2139/ssrn.2341356.

Seamans, R. and Zhu, F. (2013b) 'A Simple Model of a Three-Sided Market', SSRN Electronic Journal [Preprint]. Available at: https://doi.org/10.2139/ssrn.2341356.

Stevenson, C.L. (2014) 'To choose a definition is to plead a cause.'

Temitayo Oluwaseun Abrahams et al. (2024) 'A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION', Computer Science & IT Research Journal, 5(1), pp. 1–25. Available at: https://doi.org/10.51594/csitrj.v5i1.699.

The global risks report 2024: insight report. 19th ed (2024). Geneva: World Economic Forum.

Appendice

K rappresenta il valore atteso del profitto generato dall'azienda i quando ha l'opportunità di assorbire la quota di ricavi dei rivali colpiti da violazioni della sicurezza, è formalizzato attraverso una distribuzione di probabilità di Poisson:

$$K = \sum_{A \subseteq F_k \setminus \{i\}} \frac{X}{N} \frac{|A|}{N - |A|} \prod_{j \in A} \left(\frac{1}{I_j + 1} \right) \prod_{z \in A^c} \left(1 - \frac{1}{I_z + 1} \right)$$

A rappresenta l'insieme delle imprese che subiscono un cyberattacco, A^C le imprese che non subiscono un cyberattacco, è il complementare di A, $|A|$ è il numero di imprese che incorrono in un cyberattacco ed F_k è l'insieme delle N-1 imprese (esclusa l'azienda i) presenti nel mercato.
K_a presenta le stesse assunzioni del parametro K, tenendo in più conto dello sforzo dell'hacker H e della quota dei profitti persa a ed acquisita dai criminali informatici in caso di attacco riuscito.

$$K_a = \sum_{A \subseteq F_k \setminus \{i\}} \frac{X(1-a)}{N} \frac{|A|}{N - |A|} \prod_{j \in A} \left(\frac{H}{I_j + H + 1} \right) \prod_{z \in A^c} \left(1 - \frac{H}{I_z + H + 1} \right)$$