Politecnico di Torino

POLITECNICO DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale (LM-31)

Tesi di Laurea Magistrale

Analisi dell'impatto della cybersecurity nelle imprese private italiane

Relatore:
Prof.ssa Laura Abrardi

Candidato:
Edoardo Temporale

Anno accademico 2023/2024

Abstract

Nell'attuale scenario di trasformazione digitale, la cybersecurity riveste un ruolo fondamentale per garantire la sicurezza delle informazioni sensibili e la continuità delle operazioni aziendali, preservandole da attacchi informatici sempre più sofisticati. L'incremento della digitalizzazione, sia nell'economia che nella società, se da un lato rappresenta un grande passo avanti verso l'innovazione, dall'altro espone imprese e istituzioni a rischi crescenti. Le minacce spaziano da frodi online e ricatti informatici a veri e propri attacchi di stampo terroristico, con un impatto potenzialmente devastante su settori strategici. La crescente dipendenza delle aziende dai servizi digitali e dalle piattaforme software rende il tessuto economico sempre più vulnerabile. Le reti digitali, che coinvolgono una vasta gamma di attori, dalle amministrazioni pubbliche alle imprese private fino agli enti statali, sono ormai altamente interconnesse. Questa interconnessione, pur offrendo enormi vantaggi in termini di efficienza e innovazione, comporta anche un ampliamento del perimetro di rischio. Infatti, un attacco a una singola parte della rete può propagarsi rapidamente, mettendo in pericolo l'intero ecosistema digitale. Di conseguenza, diventa imperativo per le aziende e gli enti pubblici adottare strategie di difesa informatica robuste e agire con tempestività per prevenire e contrastare tali minacce. Un'azione proattiva, basata su tecnologie avanzate e su una costante vigilanza, è essenziale per limitare i danni e garantire che il processo di digitalizzazione, pur con le sue sfide, continui a rappresentare un volano di crescita e sviluppo sostenibile.

Questo elaborato si propone di analizzare in modo approfondito il livello di sicurezza informatica nelle imprese italiane. Nel primo capitolo viene esaminata la nascita della cybersecurity, evidenziandone le tappe fondamentali nell'evoluzione e delineando le prospettive future del settore. Questo consente di comprendere non solo come si sia sviluppata la sicurezza informatica nel corso del tempo, ma anche quali direzioni potrà prendere in futuro. Il secondo capitolo si concentra sullo studio delle principali tipologie di crimini informatici, con un'analisi approfondita di quelli più diffusi. Si esaminano i metodi utilizzati dai criminali e le motivazioni alla base di questi attacchi, al fine di comprendere meglio le dinamiche e i rischi legati al cybercrime. Nel terzo capitolo si analizzano le riforme e i provvedimenti adottati a livello europeo e italiano nel corso degli anni, mirati a contrastare le problematiche legate alla sicurezza informatica. Viene tracciato un quadro delle politiche e delle normative sviluppate per proteggere le imprese e le istituzioni da minacce sempre più complesse. Il quarto capitolo dello studio si basa sull'analisi di un dataset fornito da Istat, che valuta il livello di sicurezza informatica nelle imprese italiane con più di 10 dipendenti. I dati sono ricavati da un questionario annuale che indaga il grado di digitalizzazione delle aziende italiane, con un focus sugli indicatori principali che determinano la loro sicurezza informatica. Questo consente di osservare le variazioni di questi indicatori nel tempo e di confrontarle con l'incidenza dei vari tipi di attacchi informatici subiti dalle aziende italiane. L'analisi si conclude con una valutazione dell'evoluzione delle imprese che hanno deciso di sottoscrivere una polizza assicurativa contro attacchi di natura digitale, evidenziando i cambiamenti avvenuti nel corso del tempo e le risposte delle aziende italiane a questo crescente bisogno di protezione.

Indice

Figure

Capitolo 1: Storia della Cyber Security

1.1 Origini della Cyber Security

Il National Institute of Standards and Technology (NIST) ha definito il termine cybersecurity come "*The ability to protect or defend the use of cyberspace from cyber attacks*"[1], dove il cyberspazio è un "*A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*". [2]

La cybersecurity si concentra sugli aspetti relativi alla sicurezza delle informazioni, enfatizzando la resilienza, la robustezza e la capacità reattiva delle tecnologie per affrontare gli attacchi informatici. Gli ambiti di applicazione della sicurezza informatica sono molteplici, comprendendo sia il business che il mobile computing. Le principali categorie di sicurezza informatica includono [3]:

- **Network security**: Protezione delle reti informatiche contro attacchi e malware.
- **Cloud security**: Protezione delle risorse e i servizi basati sul cloud, comprese le applicazioni, i dati e l'infrastruttura.
- **Critical infrastructure security**: Soluzioni di cybersecurity utilizzate per proteggere le reti, le applicazioni, i sistemi e le risorse digitali da cui dipendono le organizzazioni di infrastrutture critiche.
- **Data security**: Gestione e protezione degli asset di dati, compresa la gestione delle autorizzazioni di accesso.
- **Endpoint security**: Protezione di devices e dati che vi sono contenuti.
- **IoT security**: Minimizzazione del rischio che gli oggetti utilizzati da questo settore possono portare all'organizzazione.
- **Application security:** Protezione da accessi non autorizzati e dall'uso non consentito di applicazioni.

La nascita della cybersecurity come campo disciplinare si colloca nel contesto di un mondo sempre più dipendente dalle tecnologie informatiche, una dipendenza che ha aperto nuove frontiere sia in termini di opportunità che di vulnerabilità. Con l'aumento dell'uso di computer e reti per la gestione e lo scambio di dati sensibili, soprattutto in ambiti come quello militare e governativo inizialmente, si è reso evidente il bisogno di proteggere queste informazioni da minacce esterne, che potessero compromettere la sicurezza nazionale o causare danni ingenti.

La Guerra Fredda fu un periodo particolarmente critico, durante il quale la sicurezza delle informazioni divenne una priorità assoluta per gli Stati Uniti e i loro alleati, nonché per i paesi del blocco sovietico. Uno degli eventi che segnò un punto di svolta per la consapevolezza sulla sicurezza informatica fu la creazione di ARPANET nel 1969, il predecessore di ciò che oggi conosciamo come Internet. ARPANET fu sviluppato dall'Advanced Research Projects Agency (ARPA) del Dipartimento della Difesa degli Stati Uniti e collegava università e laboratori di ricerca che lavoravano su progetti governativi. Questa rete nacque per facilitare la condivisione di informazioni e risorse, ma ben presto si presentarono i primi casi di vulnerabilità della sicurezza, esponendo la rete ad accessi non autorizzati. [4]

Questi primi tentativi di intrusione dimostrarono la necessità di sviluppare strategie per proteggere le reti e i dati. Le prime soluzioni prodotte furono la creazione di password e protocolli di autenticazione,

così come l'implementazione di software per monitorare e registrare le attività sulla rete, identificando e rispondendo agli accessi sospetti o non autorizzati.

Il motivo fondamentale che spingeva la nascita della cybersecurity era dunque la protezione delle informazioni sensibili e delle infrastrutture critiche. Con la crescente complessità delle tecnologie e l'espansione delle reti, anche i metodi di attacco divennero più sofisticati, rendendo evidente che la semplice protezione fisica non era più sufficiente. Era necessaria una nuova disciplina che potesse evolvere rapidamente per tenere il passo con le mutevoli tecniche di attacco e le strategie di difesa.

Fu durante gli anni '80 e '90 che la disciplina iniziò a strutturarsi più formalmente, in risposta a una serie di famosi incidenti di sicurezza che evidenziarono la fragilità delle infrastrutture informatiche esistenti. Questi eventi portarono alla creazione di protocolli di sicurezza più robusti e all'introduzione di leggi e regolamenti specifici per la protezione dei dati.

Il concetto di "cybersecurity" si è evoluto per includere non solo la protezione contro gli accessi non autorizzati, ma anche la prevenzione contro virus, worm e altri tipi di malware che possono danneggiare o rubare dati. Inoltre, con l'avvento di Internet e la sua rapida espansione durante gli anni '90, la cybersecurity è diventata una preoccupazione globale, rendendo necessaria una cooperazione internazionale per affrontare minacce che si potrebbero originare da qualsiasi parte del mondo.

Con il nuovo millennio, la questione della cybersecurity ha assunto nuove dimensioni con la proliferazione di dispositivi connessi, l'aumento delle transazioni online e la digitalizzazione di servizi in settori critici come la finanza, la sanità e l'energia. Questo ha portato all'elaborazione di normative più stringenti e alla nascita di industrie dedicate alla sicurezza informatica, spingendo le organizzazioni a considerare la cybersecurity non più come un optional, ma come una componente fondamentale della loro strategia operativa.

La cybersecurity oggi non si occupa solo di difendere le infrastrutture IT esistenti, ma anche di prevedere e mitigare i rischi associati all'innovazione tecnologica continua. Questo include lo sviluppo di intelligenza artificiale per la previsione di attacchi, l'analisi comportamentale per rilevare attività sospette e l'impiego di blockchain per garantire l'integrità e la tracciabilità delle informazioni. In questo modo, la cybersecurity continua a evolversi in risposta alle sfide poste da un panorama tecnologico che cambia rapidamente, cercando di anticipare le minacce future piuttosto che limitarsi a reagire a quelle presenti.

1.2 Milestone nella Storia della Cyber Security

Negli anni '70, l'espansione delle reti informatiche rese evidente la necessità di sviluppare protocolli di sicurezza per garantire una comunicazione sicura tra i computer. Due delle innovazioni chiave di questo periodo furono l'adozione del protocollo TCP/IP e la creazione del primo standard di crittografia dei dati.

Il TCP/IP (Transmission Control Protocol/Internet Protocol) è il protocollo di comunicazione fondamentale che consente ai computer di collegarsi e comunicare su Internet. Questo protocollo definisce le regole per il trasferimento dei dati tra dispositivi su reti diverse, permettendo la creazione di una rete di reti che costituisce l'Internet moderna. Fu sviluppato dall'ARPA come parte del progetto ARPANET e Vinton Cerf e Robert Kahn, spesso chiamati i "padri di Internet", furono i principali artefici di

questo protocollo. La loro idea rivoluzionaria fu di creare un metodo per collegare reti diverse in modo che potessero comunicare come un'unica rete unificata.

Questo protocollo è formato da due principali strutture. La prima è il TCP, che garantisce che i dati trasferiti tra due dispositivi siano suddivisi in pacchetti, inviati, ricevuti e riassemblati correttamente nella sequenza originale ma anche della gestione degli errori e del controllo del flusso. La seconda è l'IP e si occupa dell'indirizzamento e dell'instradamento dei pacchetti di dati. Ogni dispositivo collegato a Internet riceve un indirizzo IP univoco, che permette ai pacchetti di dati di raggiungere la destinazione corretta.
Nel 1983, ARPANET adottò ufficialmente il TCP/IP come standard per la comunicazione, segnando un momento cruciale nella storia di Internet. Questa adozione permise l'interconnessione di reti diverse, accelerando l'espansione e l'evoluzione della rete globale. [5]

Un'altra pietra miliare nella sicurezza informatica fu l'introduzione del Data Encryption Standard (DES), sviluppato sempre in quegli anni e adottato come standard federale negli Stati Uniti nel 1977.

Il DES fu sviluppato dalla IBM e successivamente adottato dal National Institute of Standards and Technology (NIST). Questo standard di crittografia a chiave simmetrica fu progettato per proteggere informazioni sensibili attraverso la crittografia dei dati, rendendoli illeggibili a chiunque non avesse la chiave corretta per decrittarli. Alla base del suo funzionamento c'è l'utilizzo di una chiave a 56 bit per cifrare e decifrare i dati. Nonostante la sua complessità e iniziale robustezza, con l'avanzare della tecnologia e la maggiore potenza di calcolo, la lunghezza della chiave di DES fu considerata vulnerabile agli attacchi di forza bruta. Questo portò, alla fine, allo sviluppo di standard di crittografia più avanzati, come l'Advanced Encryption Standard (AES). [6]

I protocolli di sicurezza come TCP/IP e DES hanno svolto un ruolo fondamentale nel garantire la sicurezza e l'affidabilità delle comunicazioni su Internet. Hanno stabilito le basi per lo sviluppo di tecnologie di sicurezza più avanzate e hanno contribuito a creare un ambiente in cui le informazioni potessero essere trasmesse e archiviate in modo sicuro.

Negli anni '80, il panorama delle minacce informatiche cominciò a prendere forma con la comparsa dei primi virus informatici e con la crescente attenzione verso la sicurezza informatica. Questo decennio segnò l'inizio di una corsa agli armamenti tra criminali informatici e professionisti della sicurezza.

Uno dei primi e più famosi virus fu il Creeper, creato da Bob Thomas nel 1971, che poteva spostarsi tra i computer connessi ad ARPANET, lasciando il messaggio "I'm the creeper, catch me if you can". Questo virus non era dannoso, ma il suo esperimento fu il precursore di una serie di eventi che hanno portato alla realtà informatica dei nostri giorni. In risposta a Creeper, un altro membro del team (Ray Tomlinson, l'inventore dell'e-mail) creò un programma in grado di individuare ed eliminare il virus, il Reaper, e rappresentò il primo esempio di antivirus. [7]

Durante gli anni '80, gli attacchi informatici cominciarono a guadagnare visibilità nei media, con giornali e telegiornali che riportavano incidenti significativi contro grandi istituzioni come AT&T e CSS. Nel 1983, il fenomeno degli hacker entrò nella cultura popolare attraverso il film "WarGames – Giochi di Guerra", che narrava la storia di un giovane hacker capace di accedere ai sistemi di controllo delle armi nucleari.

Sebbene molte rappresentazioni degli hacker e dei criminali informatici fossero imprecise ed esagerate, esse contribuirono a familiarizzare il pubblico con l'idea dell'informatica. Con l'emergere di Internet,

anche se ancora agli inizi del suo sviluppo, le persone iniziarono a comprendere sia i benefici che i rischi associati a questa nuova tecnologia.

Un caso particolare che attirò l'attenzione pubblica fu quello del virus Vienna, un malware autoreplicante capace di corrompere i file dei dispositivi infetti. Nonostante esistessero molte minacce simili all'epoca, Vienna divenne noto non tanto per i danni causati, ma per il modo in cui venne neutralizzato. Il ricercatore tedesco Bernd Fix scoprì che il suo dispositivo era stato infettato da questo virus ed in risposta, sviluppò un antivirus capace di rilevarlo e rimuoverlo, segnando uno dei primi esempi di antivirus moderno.

Gli anni '90 furono segnati dalla diffusione di Internet e dall'esplosione delle minacce informatiche. L'apertura di Internet al pubblico trasformò il modo in cui le persone comunicavano e lavoravano, ma creò anche nuove opportunità per i criminali informatici. L'introduzione di servizi di posta elettronica come Hotmail rese la comunicazione più facile, ma anche più vulnerabile agli attacchi. Con l'aumento dell'accesso pubblico alla rete, la cybersecurity dovette adattarsi rapidamente per proteggere una base di utenti sempre più vasta e diversificata. Un esempio noto è quello del virus Melissa, creato dal programmatore David Smith e considerato uno dei virus a più alta diffusione di sempre e che ha causato danni per 1,3 miliardi di euro. Melissa è un virus scritto in linguaggio macro VBA, tipico dei sistemi Office, e viene distribuito come allegato tramite email. Quando l'allegato viene aperto, il codice viene eseguito, infettando tutti i file del sistema. Il successo di questo virus è attribuibile alla sua straordinaria capacità di propagazione: una volta infettato il sistema, Melissa genera una lista dei primi 50 contatti presenti nella rubrica e si auto-invia a questi contatti.

Con l'aumento delle minacce, la necessità di proteggere le reti aziendali portò all'introduzione dei primi firewall. Questi dispositivi o software controllavano il traffico di rete in entrata e in uscita per prevenire accessi non autorizzati. Allo stesso tempo, gli antivirus evolsero per rilevare e rimuovere una gamma sempre più ampia di malware. Nel 1991, Symantec rilasciò la prima versione di Norton AntiVirus, che divenne un punto di riferimento nel mercato degli antivirus.

Negli anni 2000, la cybersecurity è passata dall'essere una preoccupazione tecnica di nicchia, ad una priorità globale, venendo sempre più integrata nelle strategie di sicurezza nazionale e aziendale. L'inizio del millennio è stato segnato da un aumento significativo delle minacce informatiche, in parallelo con la crescente dipendenza da Internet e dalle tecnologie digitali.

Uno degli eventi più emblematici di questo periodo è stato l'attacco del worm "ILOVEYOU" nel 2000, che ha infettato milioni di computer in tutto il mondo in poche ore, causando danni economici per oltre 5 miliardi di dollari. Questo incidente ha evidenziato la vulnerabilità delle infrastrutture informatiche globali e la necessità di migliorare le pratiche di sicurezza informatica [8].

Con il crescente utilizzo di Internet e la proliferazione delle reti aziendali, è emersa l'esigenza di standard di sicurezza più rigorosi. La promulgazione della Direttiva sulla protezione dei dati dell'Unione Europea nel 1995 e del Gramm-Leach-Bliley Act (GLBA) negli Stati Uniti nel 1999 ha segnato l'inizio di un'epoca in cui la protezione dei dati personali e finanziari è diventata materia di interesse legale con la creazione di specifiche normative. Queste normative hanno imposto alle aziende requisiti stringenti per la protezione delle informazioni sensibili e la segnalazione delle violazioni di sicurezza.

Nel 2001, gli attacchi terroristici dell'11 settembre hanno catalizzato un ulteriore cambiamento nella percezione della cybersecurity, che è diventata una componente essenziale della sicurezza nazionale. La

legislazione come il PATRIOT Act negli Stati Uniti ha ampliato i poteri delle agenzie governative per monitorare e prevenire le minacce informatiche, riflettendo una crescente integrazione tra sicurezza informatica e sicurezza fisica.

Con l'avvento del cloud computing negli anni 2010, la cybersecurity ha dovuto adattarsi a nuove sfide. Le aziende hanno iniziato a migrare i loro dati e applicazioni su piattaforme cloud, beneficiando di scalabilità e flessibilità, ma esponendosi anche a nuovi vettori di attacco. In risposta, sono stati sviluppati nuovi protocolli di sicurezza e standard di protezione, come il NIST Cybersecurity Framework, introdotto nel 2014, che fornisce linee guida dettagliate per la gestione del rischio informatico.

L'introduzione del Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea nel 2018 ha rappresentato un ulteriore passo avanti nella protezione dei dati personali. Questo regolamento ha imposto sanzioni severe per le violazioni dei dati e ha stabilito diritti chiari per gli individui riguardo alle loro informazioni personali, spingendo le aziende a migliorare significativamente le loro pratiche di cybersecurity.

1.3 Le nuove frontiere e le prospettive future

Negli ultimi anni, la diffusione del lavoro remoto a causa della pandemia di COVID-19 ha aumentato la superficie di attacco per i cybercriminali. Le aziende hanno dovuto affrontare nuove sfide legate alla sicurezza delle connessioni remote e alla protezione dei dati aziendali su dispositivi personali. In risposta a questi pericoli intervengono modelli come la Zero Trust Security che, come riporta Cloudflare "*richiede una rigorosa verifica dell'identità per ogni persona e dispositivo che cerca di accedere alle risorse di una rete privata, indipendentemente dal fatto che si trovi all'interno o all'esterno del perimetro della rete*" [8].

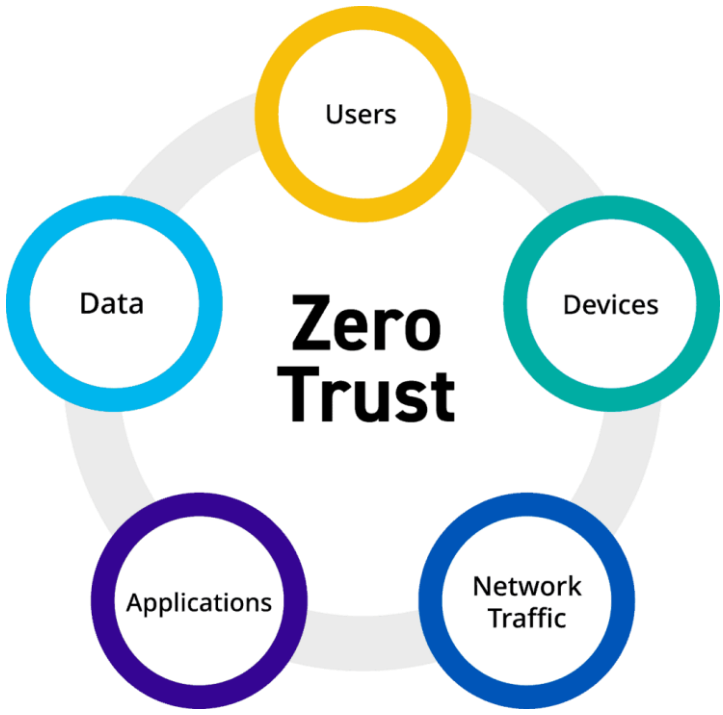

Figura 1. Zero Trust Security Model

Invece di dare per scontato che tutto ciò che si trova dietro il firewall aziendale sia sicuro, i principi Zero Trust rafforzano la sicurezza di un'organizzazione eliminando una difesa perimetrale e concentrandosi su

un'autenticazione rigorosa in ogni punto di accesso. Un modello di sicurezza Zero Trust garantisce che nessun dispositivo, utente, sistema o carico di lavoro sia affidabile per impostazione predefinita, indipendentemente dal luogo in cui opera.

Parallelamente, sempre più utilizzati sono i servizi di VPN (Virtual Private Network) e sempre un maggior numero di utenti su internet ne fanno uso. Infatti, come le telecamere di sorveglianza e gli allarmi proteggono le abitazioni, le VPN sono diventate strumenti fondamentali per salvaguardare la privacy e la sicurezza in rete. Una VPN crea un tunnel criptato tra il dispositivo dell'utente (come un computer, uno smartphone o un tablet) e un server remoto gestito dal fornitore di VPN. Questo tunnel nasconde l'indirizzo IP dell'utente, rendendo le sue attività online anonime e proteggendole da possibili intercettazioni o monitoraggi da parte di terze parti.

Le principali utilità sono:

- **Protezione della privacy:** l'indirizzo IP di un utente viene mascherato, impedendo ad utenti terzi di monitorare la sua attività online.
- **Sicurezza nell'uso del Wi-Fi:** i Wi-Fi pubblici, presenti spesso in luoghi come hotel o aeroporti, sono soggetti a frequenti attacchi informatici. L'utilizzo di una VPN rende la connessione sicura in questo tipo di scenari.
- **Accesso a contenuti limitati:** le VPN possono bypassare le restrizioni di un utente legate alla sua area geografica, come ad esempio servizi di streaming e notizie, ma anche sorpassare censure imposte dalle stesse organizzazioni nazionali.

Il mercato delle VPN ha una valenza globale e con un bacino di utenti pari a quello degli utilizzatori di piattaforme browser per la navigazione su internet. È infatti di facile utilizzo e che non richiede particolari nozioni di informatica o di cybersicurezza per poterlo sfruttare.

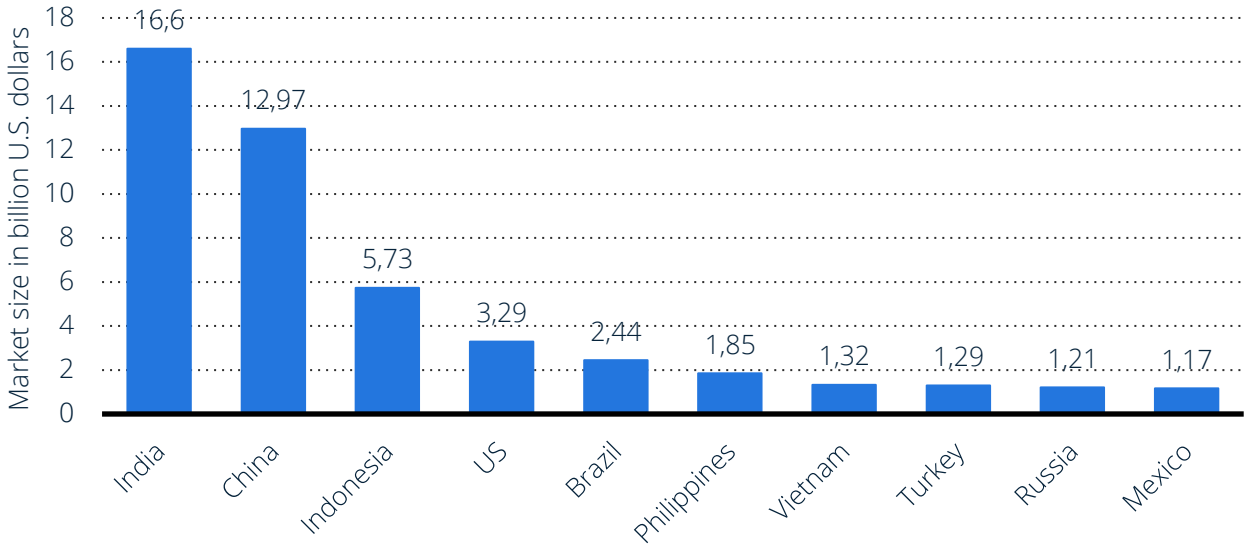

Figura 2. Virtual private network (VPN) market worldwide in 2023, by country (in billion U.S. dollars) [10]

Il grafico mostrato evidenzia come India e Cina emergano come i maggiori contribuenti in questo settore. L'India si posiziona al vertice con una spesa totale nel 2023 di 16,6 miliardi di dollari, seguita subito dalla Cina con 12,97 miliardi di dollari. Gli Stati Uniti si posizionano solamente al terzo posto e

con una spesa totale decisamente inferiore alle due precedenti. Una assenza cruciale è quella dei paesi europei.

In conclusione, le VPN sono uno strumento necessario per grandi aziende, riescono infatti a proteggere la connessione dei propri dipendenti da attacchi esterni, proteggendo informazioni sensibili che, se rubate e diffuse, potrebbero mettere a rischio il vantaggio competitivo costruito all'interno dell'azienda. Sono tuttavia anche uno strumento alla portata del singolo consumatore.

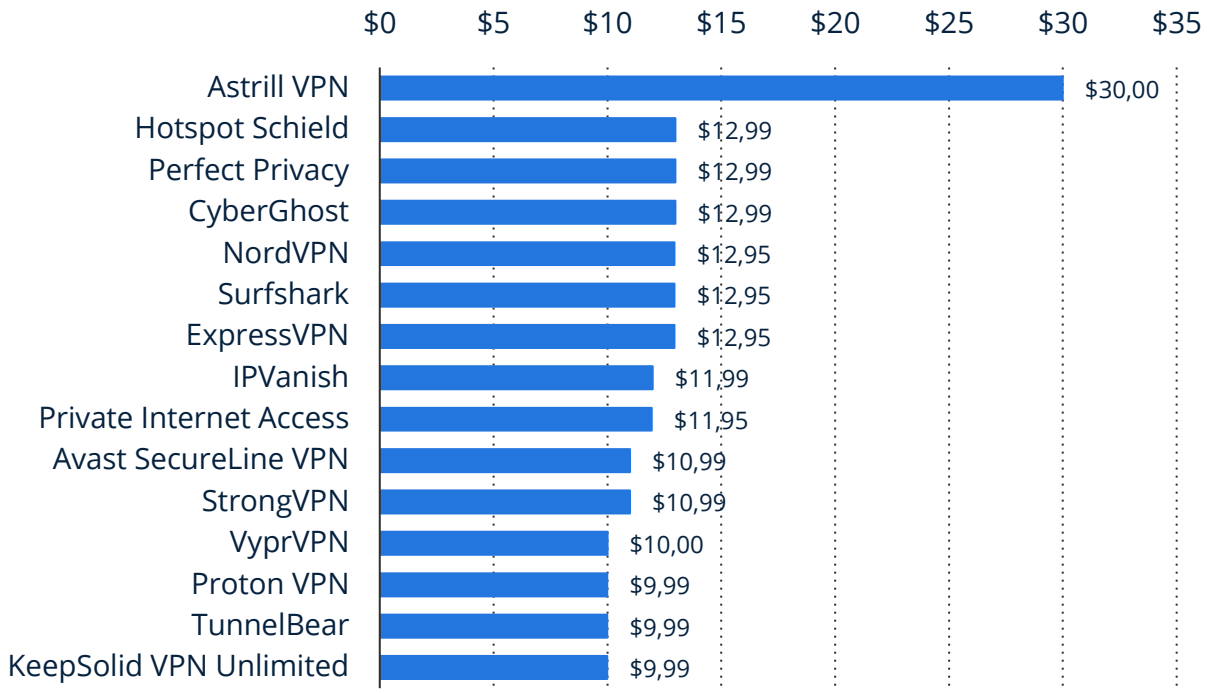

Figura 3. Average monthly price for virtual private networks in 2023 [11]

Il grafico in figura, ricavato da un sondaggio di Security.org, mostra il prezzo medio in dollari per un abbonamento mensile ad un servizio di VPN. Esclusa Astrill VPN, che offre un servizio a più ampio spettro e con maggiori funzioni rispetto ad i suoi competitor, il prezzo base si assesta tra i 10$ ed i 13$, in linea con un abbonamento ad un servizio di streaming online. Risulta quindi chiaro che per un utente finale che abbia la necessità o l'interesse all'uso di questo servizio, la spesa possa essere sostenuta con relativa facilità.

Capitolo 2: I crimini del mondo digitale

2.1 Il Cyber crime

Ad accompagnarsi alla sempre più diffusa pratica di implementare sistemi di cyber sicurezza, il cyber crime si è affermato come una minaccia significativa che attraversa le barriere nazionali e settoriali. La criminalità informatica comprende una vasta gamma di atti illeciti che si svolgono nel cyberspazio, un ambiente in cui la comunicazione avviene tramite reti di computer e altri dispositivi elettronici.

Il cyber crime può essere definito come "qualsiasi reato penale che è commesso o facilitato attraverso l'uso delle capacità di comunicazione di computer e sistemi informatici" [16]. Questa definizione cattura l'essenza delle attività criminali che sfruttano le tecnologie digitali, sia per commettere reati tradizionali in modi nuovi sia per perpetrare nuovi tipi di crimini che sono possibili solo con l'uso della tecnologia.

Inoltre, il cyber crime si distingue per la sua capacità di superare le barriere fisiche e giurisdizionali, complicando così gli sforzi di applicazione della legge e di prevenzione del crimine. Originariamente limitato a semplici frodi e furti di dati, il cyber crime ha ora ampliato il suo ambito ad attacchi sofisticati come il ransomware, gli attacchi ai sistemi critici infrastrutturali e le campagne di disinformazione su larga scala. Questo aspetto è particolarmente problematico poiché, come sottolineato in alcune analisi, la determinazione della giurisdizione e l'applicabilità delle leggi possono diventare sfide significative a causa della natura transnazionale e spesso anonima del cyber crime. [17]

Tracciare i cyber criminali rappresenta una delle sfide più complesse nell'ambito della sicurezza informatica. A differenza della criminalità tradizionale, dove le azioni illecite sono spesso visibili e le loro tracce fisiche, i criminali informatici operano in un ambiente dove possono facilmente nascondere la propria identità e la propria posizione geografica. Utilizzano una varietà di tecniche sofisticate per mascherare le loro tracce digitali, come l'uso di VPN, server proxy, e la navigazione tramite la rete Tor, che rende quasi impossibile ricondurre a loro le attività illecite.

Questo livello di anonimato rende il cyberspazio un terreno particolarmente fertile per i criminali, poiché diminuisce significativamente le loro inibizioni. Sapendo di essere difficilmente tracciabili, i cyber criminali si sentono più liberi di esplorare e commettere atti illegali senza il timore immediato di essere scoperti o identificati. La difficoltà di tracciare i cyber criminali, molti dei quali utilizzano tecniche avanzate per mascherare la loro identità e ubicazione, pone sfide uniche che non sono presenti nella criminalità tradizionale. Questo anonimato può diminuire le inibizioni degli aggressori, rendendo il cyber spazio un ambiente particolarmente attrattivo per commettere reati senza un rischio percepito immediato di cattura o identificazione.

Inoltre, la natura globale di Internet permette ai criminali di operare da qualsiasi luogo nel mondo, spesso in paesi con leggi meno severe sulla cybercriminalità o con risorse limitate per farla rispettare. Questo li mette al sicuro non solo dalla giurisdizione in cui avviene il crimine ma anche da quelle che potrebbero avere leggi più severe.

In sintesi, l'attrattiva del cyber crimine risiede nella combinazione di elevato anonimato, basso rischio di cattura, e potenziali rendimenti elevati, che insieme creano un ambiente che i criminali trovano irresistibilmente vantaggioso. Questo spiega il continuo aumento degli attacchi cyber nonostante i crescenti sforzi per migliorare la cyber sicurezza a livello globale.

L'impatto del cyber crime sulla società è vasto e multidimensionale, influenzando profondamente sia il settore privato che quello pubblico. Ogni anno, le perdite economiche globali attribuibili a questa forma di criminalità si contano in miliardi di dollari, ma l'impatto va ben oltre il danno finanziario immediato.

Nei settori privati, le aziende di tutte le dimensioni affrontano costi significativi non solo per il recupero diretto dei dati e la riparazione dei sistemi, ma anche per l'aggiornamento delle infrastrutture di sicurezza, la formazione del personale per prevenire futuri attacchi e, in molti casi, per sanzioni legali e compensazioni in seguito a violazioni dei dati. Questi costi possono risultare proibitivi, specialmente per le piccole e medie imprese, e possono portare alla chiusura di aziende altrimenti redditizie.

Sul fronte del settore pubblico, il cyber crime incide sulla sicurezza nazionale e sulla pubblica amministrazione. Gli attacchi contro infrastrutture critiche, come reti elettriche, sistemi di trasporto e reti sanitarie, possono avere conseguenze devastanti sulla vita quotidiana e sulla sicurezza dei cittadini. Inoltre, il furto di informazioni sensibili dal settore pubblico, come dati personali o segreti di stato, mina la fiducia nelle istituzioni governative.

A livello individuale, il cyber crime erode la fiducia dei consumatori nelle transazioni online. Il timore di furto di identità e di frodi finanziarie può dissuadere le persone dall'utilizzare servizi digitali per fare acquisti o per operazioni bancarie, limitando così la crescita dell'economia digitale. Questo sentimento di sfiducia può estendersi a Internet in generale, rallentando l'adozione di tecnologie potenzialmente rivoluzionarie e modificando il comportamento online degli utenti.

Infine, l'impatto sulla stabilità economica globale è significativo. I mercati finanziari possono subire turbolenze a seguito di attacchi informatici su larga scala, influenzando investimenti e risparmi a livello mondiale. Gli attacchi mirati possono alterare il commercio e l'economia internazionale, creando uno stato di incertezza che impatta le decisioni di investimento e le politiche economiche nazionali.

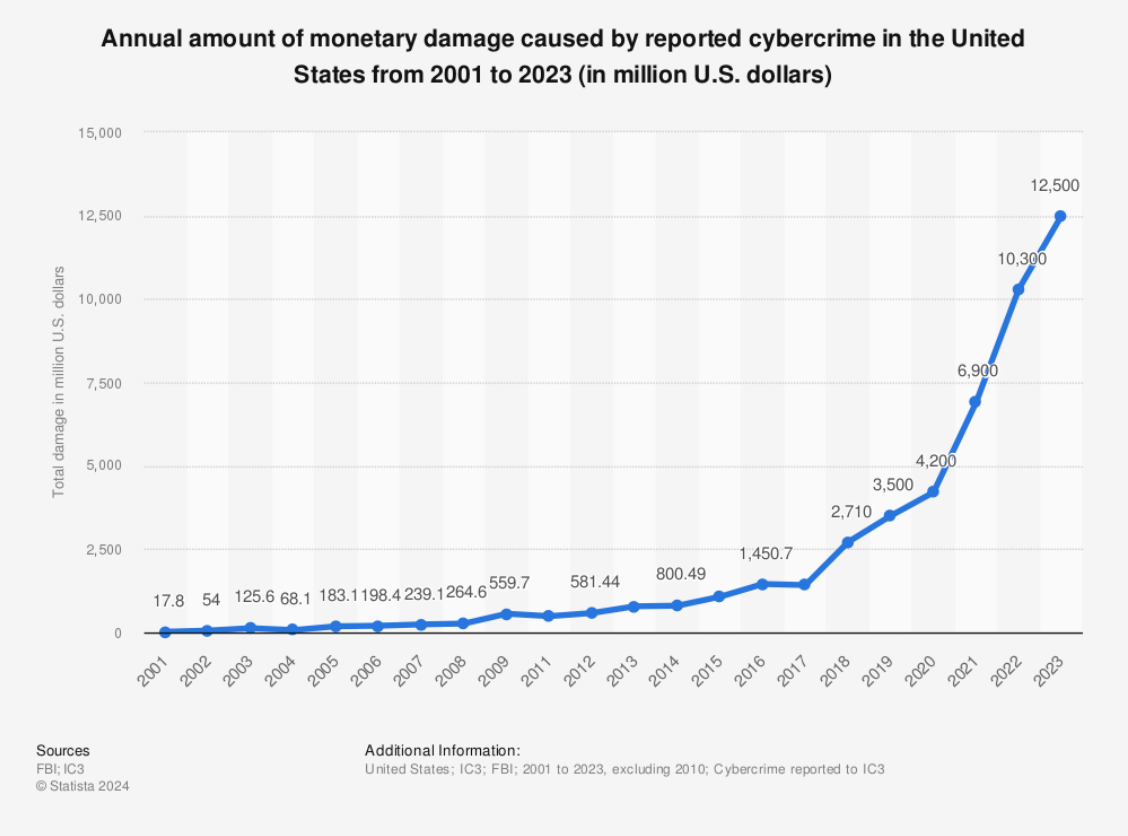

Figura 4. Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023 (in million U.S. dollars) [14]

Nel recente rapporto sul cyber crime negli Stati Uniti, elaborato dal Federal Bureau of Investigation (FBI) e dall'Internet Crime Complaint Center (IC3), emerge una situazione allarmante. Nel 2023, i danni monetari causati da crimini informatici hanno raggiunto il picco storico di 12,5 miliardi di dollari, segnando un aumento del 21% rispetto all'anno precedente. L'incremento non solo evidenzia le gravi perdite economiche, ma sottolinea anche l'ampio impatto psicologico sui cittadini, esacerbando sentimenti di vulnerabilità e impotenza di fronte a minacce sempre più sofisticate.

Il rapporto dettaglia come il cyber crime influenzi vari segmenti della popolazione, con particolare attenzione agli anziani, che si rivelano particolarmente esposti. I dati del 2023 mostrano che gli individui oltre i 60 anni hanno presentato 101,068 reclami, con perdite economiche che ammontano a 3,4 miliardi di dollari, rappresentando quasi il 27% del totale delle perdite segnalate all'IC3. Questo gruppo è dunque il più colpito, sia in termini di numero di reclami sia per l'entità delle perdite economiche.

Le categorie più giovani, sebbene registrino un numero minore di perdite economiche, continuano a subire significativi attacchi informatici. I giovani sotto i 20 anni hanno segnalato 18,174 reclami con perdite totali di 40,7 milioni di dollari, mentre i giovani adulti tra i 20 e i 29 anni hanno riportato 62,410 reclami con perdite di 360,7 milioni di dollari. Questi dati evidenziano una preoccupazione crescente per la sicurezza digitale tra i giovani e suggeriscono la necessità di strategie preventive adatte a questa fascia d'età.

Infine, il gruppo di età compresa tra i 30 e i 49 anni, attivo nel mondo del lavoro e spesso bersaglio di frodi legate a investimenti o compromissioni di email aziendali, ha segnalato un alto numero di reclami. I trentenni hanno registrato 88,138 reclami con perdite di 1,2 miliardi di dollari e i quarantenni hanno presentato 84,052 reclami con perdite ancora maggiori, pari a 1,5 miliardi di dollari. Questi dati confermano che il cyber crime rappresenta una minaccia trasversale che richiede un impegno collettivo per il contrasto efficace.

Queste statistiche sottolineano la diversità dell'impatto dei crimini informatici tra le varie fasce d'età e l'importanza di adottare approcci di prevenzione e protezione che tengano conto delle specifiche vulnerabilità associate a ciascun gruppo d'età.

Tra le tipologie di crimine più costose segnalate, spiccano le frodi sugli investimenti, con perdite che hanno raggiunto i 4,57 miliardi di dollari, rappresentando l'aumento maggiore rispetto all'anno precedente. Questo tipo di frode include varie truffe finanziarie che promettono grandi ritorni con rischi minimi, sfruttando la fiducia e l'avidità delle vittime.

Un altro crimine notevolmente dannoso è il Business Email Compromise (BEC), una sottocategoria del Phishing, che ha visto perdite per quasi 2,95 miliardi di dollari. Queste truffe si verificano quando i criminali riescono a inserirsi nelle comunicazioni aziendali, spesso tramite tecniche di ingegneria sociale o hacking, per deviare pagamenti o informazioni riservate.

Le truffe legate al supporto tecnico, che sfruttano la scarsa conoscenza tecnica delle vittime, hanno portato a perdite di circa 924 milioni di dollari. Similmente, le frodi legate a ransomware hanno continuato a essere una minaccia costosa, con perdite segnalate per circa 59,6 milioni di dollari, evidenziando un aumento sia nel numero di reclami che nell'entità delle perdite rispetto all'anno precedente.

Le violazioni dei dati personali hanno causato danni per 744 milioni di dollari, mostrando quanto possa essere costosa la perdita o il furto di informazioni sensibili. Inoltre, i crimini legati all'usurpazione d'identità hanno avuto un impatto notevole, con perdite stimate in oltre 126 milioni di dollari.

Questi numeri illustrano non solo la diversità dei crimini informatici ma anche il profondo impatto economico che possono avere su individui e aziende. La consapevolezza e le misure preventive sono essenziali per proteggersi da queste minacce sempre più sofisticate.

2.2 Phishing

Tra i crimini più diffusi si distingue il phishing, una tecnica di truffa apparentemente semplice ma paradossalmente una delle più pericolose. Quando realizzato con successo, il phishing può causare ingenti perdite economiche, dimostrandosi una minaccia significativa nell'ambito della sicurezza informatica.

Il phishing è una tecnica di frode online che mira a carpire informazioni sensibili come credenziali di accesso, dettagli delle carte di credito e altre informazioni personali. Gli aggressori spesso si avvalgono di email che sembrano provenire da fonti legittime, come banche o aziende conosciute, per indurre le vittime a fornire dati personali su siti web falsificati che imitano quelli reali. Questi siti sono creati con grande attenzione ai dettagli per ingannare le vittime affinché credano di essere sul sito web corretto.

Le tecniche di phishing sono diverse e riflettono la creatività e l'ingegnosità dei criminali informatici. Tra le più comuni troviamo il phishing tramite email, una delle strategie più diffuse, dove gli aggressori inviano messaggi che sembrano provenire da enti legittimi per indurre le vittime a rivelare informazioni sensibili. Queste email possono contenere link a siti web fraudolenti che imitano quelli reali o allegati infetti che, una volta aperti, possono scaricare malware sul computer della vittima. Una tecnica più raffinata è lo spear phishing, mirato specificamente a individui o organizzazioni con l'intento di ottenere accesso a dati di particolare valore. Questo metodo si distingue per il livello di personalizzazione dell'attacco, spesso basato su ricerche approfondite sulle potenziali vittime per renderlo quanto più credibile possibile.

Gli attacchi possono anche essere camuffati da richieste urgenti o allarmanti, progettate per spingere la vittima a reagire impulsivamente. Ad esempio, potrebbero essere informati di un problema non esistente con il loro conto bancario o di un pacchetto bloccato che richiede la conferma dei dettagli personali per essere consegnato. Queste tecniche sfruttano la tendenza umana alla fiducia e alla risposta emotiva, rendendo il phishing una delle minacce più insidiose nel panorama della sicurezza informatica. La consapevolezza e la formazione continua sono essenziali per aiutare gli individui e le organizzazioni a riconoscere e prevenire questi attacchi.

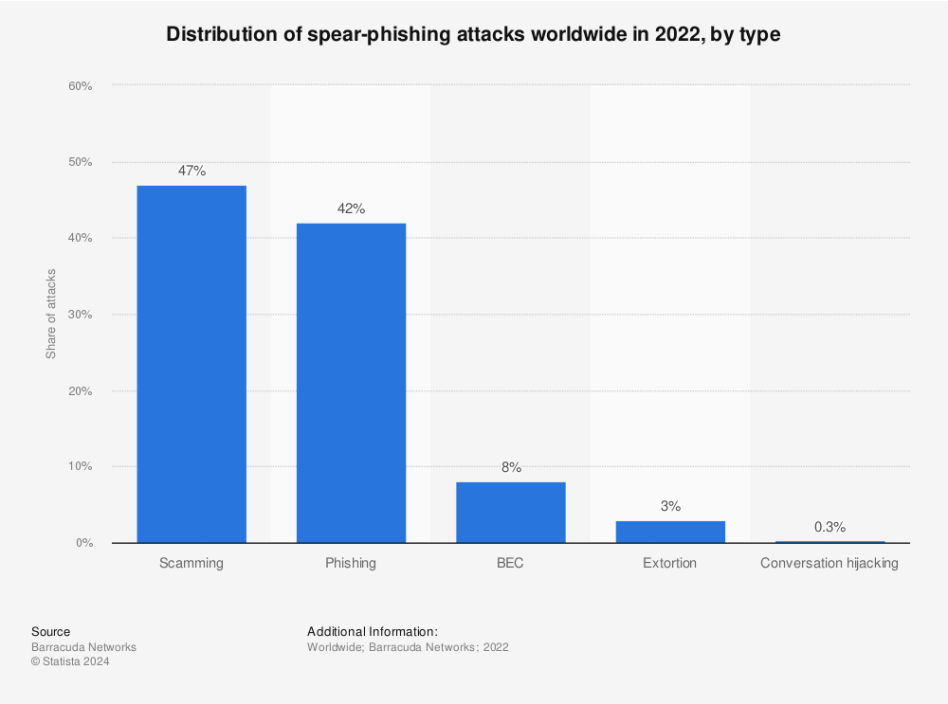

Figura 5. Distribution of spear-phishing attacks worldwide in 2022, by type [15]

Nel rapporto del 2023 sui trend del spear-phishing, pubblicato da Barracuda Networks, società di consulenza informatica e servizi IT, e condotto analizzando oltre 50 miliardi di email distribuite su 3.5 milioni di caselle di posta elettronica, è emerso che oltre 30 milioni di queste fossero mail con scopo di spear phishing.

Il 47% delle e-mail contraffatte analizzate è rappresentato dallo “Scamming”, un tipo di attacco di progettato per catturare informazioni private e sensibili, come conti bancari e carte di credito. Gli aggressori inducono le vittime a rivelare le informazioni e poi le usano per frodarle, rubare la loro identità o entrambe le cose. Gli attacchi vengono eseguiti utilizzando una serie di espedienti, come vincite alla lotteria, pacchi non reclamati, falsi annunci di lavoro, richieste di donazioni e altre tattiche.

Al secondo posto si trova il cosiddetto “Brand impersonating”, progettato per impersonare aziende note e applicazioni aziendali comunemente utilizzate, e rappresenta il 42% di tutti gli attacchi. Si tratta di uno dei tipi di attacchi più diffusi perché sono ben progettati come punto di ingresso per raccogliere le credenziali ed eseguire l'acquisizione di un account. Gli attacchi di impersonificazione dei marchi sono tipicamente utilizzati per rubare le informazioni di accesso agli account e normalmente vengono sfruttati i nomi di grandi e ben note imprese come Microsoft, DHL, WeTransfer ed altri.

Nonostante impattino solamente per l’8% del totale, le BEC causano miliardi di dollari di perdite per le aziende che ricadono in questa truffa. I truffatori impersonano un dipendente, un partner, un fornitore o un'altra persona fidata in un'e-mail, richiedendo un bonifico bancario o informazioni di identificazione personale ai dipendenti del reparto finanziario o ad altre persone con accesso a informazioni sensibili. Questi attacchi altamente mirati sono particolarmente difficili da individuare perché raramente includono un URL o un allegato dannoso.

Le estorsioni rappresentano il 3% del numero totale di attacchi di phishing mirati. La maggior parte degli attacchi è costituita da minacce via e-mail di tipo sextortion. I criminali informatici affermano di essere in possesso di video compromettenti, immagini o altri contenuti sensibili o imbarazzanti presumibilmente registrati dal computer della vittima. Minacciano di condividerli con tutti i loro contatti

e-mail a meno che non venga pagato un riscatto. Le richieste variano in genere da poche centinaia a qualche migliaio di dollari e devono essere pagate in bitcoin, difficili da rintracciare.

Per le 0,3% del totale incide il “Conversation hijacking”, noto anche come vendor impersonation, che può essere devastante. In questi attacchi elaborati i criminali informatici si inseriscono in conversazioni aziendali esistenti o ne avviano di nuove sulla base di informazioni raccolte da account e-mail compromessi o da altre fonti. Il dirottamento delle conversazioni fa tipicamente parte di un attacco di tipo account-takeover. Gli aggressori utilizzano attacchi di phishing per rubare le credenziali di accesso e compromettere gli account aziendali. Leggono le e-mail e monitorano l'account compromesso per comprendere le operazioni aziendali e conoscere gli affari in corso, le procedure di pagamento e altri dettagli. I criminali sfruttano queste informazioni, comprese le conversazioni interne ed esterne tra dipendenti, partner e clienti, per creare messaggi convincenti, inviarli da domini impersonati e indurre le vittime a versare denaro o aggiornare le informazioni di pagamento. [16]

Nonostante le mail Phishing costituiscano meno dello 0.1% del totale delle mail ricevute in una casella di posta, comportano un grosso impatto in termini di perdite economiche per chi cade nella trappola. È stimato che una organizzazione riceva in media 5 email di spear-phishing ogni giorno e che il click-rate degli utenti sia di circa l’11%. Riportato su base annuale risulta quindi in circa 200 email che vengono aperte ed in cui gli utenti cliccano su un ipotetico link al loro interno. Certamente non tutti questi 200 reindirizzamenti comportano la riuscita della truffa ma anche solo un successo può comportare un grosso esborso monetario per l’azienda.

Infatti, secondo il Cost Data Breach Report 2023 [17] condotto da IBM, il costo medio di una violazione di sistemi informatici a livello globale si assesta sui 4.5 milioni di dollari, in crescita del 15% in 3 anni.

Risulta chiaro che gli autori di reati di phishing variano notevolmente per sofisticazione e motivazioni, spaziando da criminali individuali a gruppi di cybercriminali organizzati, i quali operano in reti ben strutturate, spesso con collegamenti a organizzazioni criminali più ampie, e possono orchestrare campagne di phishing su larga scala per rubare dati di grande valore da aziende o enti governativi.

In alcuni casi, gli attacchi di phishing possono essere condotti da attori sponsorizzati dallo stato, utilizzando questa tecnica come strumento di cyber spionaggio per acquisire segreti commerciali o informazioni governative sensibili. Questi attacchi possono avere motivazioni politiche o economiche e sono spesso parte di operazioni di intelligence più ampie.

Infine, esistono situazioni in cui aziende o concorrenti non etici possono ricorrere al phishing per ottenere vantaggi competitivi illegali, cercando di accedere a informazioni riservate o di danneggiare la reputazione di un rivale. Questo sottolinea l'importanza di una vigilanza costante e di misure di sicurezza robuste per proteggere le informazioni sensibili contro una vasta gamma di minacce.

Non è quindi un caso che il 51% delle organizzazioni intenda aumentare gli investimenti in sicurezza, spesso a seguito di una violazione, con strumenti di rilevamento e risposta alle minacce, ma anche e soprattutto con la formazione dei propri dipendenti.

La formazione è un primo passo cruciale, insegnare ai dipendenti a riconoscere le email sospette e ad evitare di cliccare su link non verificati può ridurre significativamente il rischio di cadere vittima di phishing. È importante che i dipendenti siano consapevoli delle tattiche comuni usate dai phisher, come l'uso di linguaggio urgente, indirizzi email sospetti e richieste di informazioni personali o sensibili.

L'adozione di software anti-phishing è un altro strato essenziale di protezione. Questi strumenti possono identificare e bloccare email sospette, siti web fraudolenti e tentativi di login da fonti non autorizzate. Molti di questi sistemi includono filtri anti-spam che aiutano a segregare o eliminare email potenzialmente pericolose prima che raggiungano gli utenti.

Le tecnologie di cifratura end-to-end proteggono i dati trasmessi, rendendo più difficile per gli attaccanti intercettare informazioni sensibili. Utilizzare autenticazione a più fattori (MFA) è una pratica di sicurezza che aggiunge un ulteriore livello di verifica, riducendo il rischio che le credenziali rubate vengano utilizzate per accedere a sistemi sensibili.

Questi approcci multidimensionali non solo rafforzano la sicurezza delle informazioni aziendali ma aiutano anche a costruire una cultura di consapevolezza della sicurezza che può proteggere l'organizzazione dagli attacchi di phishing e altre minacce informatiche.

2.3 Ransomware

Nel contesto attuale dell'informatica e della sicurezza dei dati, una delle minacce più pervasive e dannose è rappresentata dai ransomware. Questi software maligni, che letteralmente significano "software di riscatto", rappresentano un tipo di attacco informatico estremamente sofisticato e insidioso, il cui scopo è criptare o sequestrare i dati digitali di un'entità – che può essere un utente individuale o un'intera organizzazione – per poi richiedere un pagamento in cambio della chiave di decrittazione.

Il Federal Bureau of Investigation statunitense, meglio noto come FBI, definisce i ransomware come: “a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim’s data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim’s data or to release it to the public” in un documento redatto nel 2021 per informare su questa pratica e spiegare quali sono le modalità per contrastarla. [18]

Il fenomeno dei ransomware non è solo un semplice problema di sicurezza informatica, ma una vera e propria crisi che colpisce trasversalmente tutti i settori della società moderna. Dalle infrastrutture critiche come ospedali, scuole e governi fino alle aziende private e agli utenti domestici, nessuno è immune. Il modus operandi di questi attacchi spesso inizia con tecniche come il phishing, attraverso cui il malware viene inoculato nei sistemi. È possibile scaricare inconsapevolmente un ransomware su un computer aprendo un allegato di posta elettronica, facendo clic su un annuncio pubblicitario, seguendo un link o persino visitando un sito Web incorporato nel malware. Una volta caricato sul computer, il codice blocca l'accesso al computer stesso o ai dati e ai file memorizzati. Le versioni più minacciose possono criptare file e cartelle su unità locali, unità collegate e persino computer collegati in rete.

Nella maggior parte dei casi, non ci si accorge che il computer è stato infettato. Di solito lo si scopre quando non si riesce più ad accedere ai propri dati o si vedono messaggi sul computer che informano dell'attacco e richiedono il pagamento di un riscatto. La capacità di questi malintenzionati di sfruttare le vulnerabilità esistenti nelle reti informatiche mostra quanto sia critico per le organizzazioni investire in misure di sicurezza robuste e in formazione continua per i loro dipendenti.

Tra le organizzazioni che hanno subito un attacco ransomware, il 71% ha affermato di aver pagato almeno una parte del riscatto richiesto, nonostante il 72% abbia identificato l'incidente in tempi brevi, spesso in pochi minuti. Anche se quasi tutti gli intervistati possedevano un'assicurazione informatica, questa non ha coperto completamente i costi o il ripristino dei dati. Infatti, solo il 35% delle vittime di ransomware è riuscito a recuperare tutti i dati persi a seguito dell'attacco. Tuttavia, non tutte le notizie sono negative. Nonostante l'incertezza economica, quasi tutti i leader intervistati (91%) prevedono di aumentare il budget per la sicurezza nell'anno successivo, puntando a investire in tecnologie e servizi che rafforzino ulteriormente la protezione delle loro reti da potenziali attacchi ransomware. [19]

La priorità principale per i responsabili della sicurezza è l'adozione di tecnologie avanzate come l'intelligenza artificiale (AI) e l'apprendimento automatico (ML), che migliorano il rilevamento tempestivo delle minacce. Queste sono seguite dall'implementazione di sistemi di monitoraggio centralizzati per accelerare la risposta agli attacchi. In particolare, la sicurezza degli Internet-of-Things (IoT) e i firewall di nuova generazione (NGFW) sono al top delle priorità di investimento, con una crescente attenzione anche verso le soluzioni di rilevamento e risposta degli endpoint (EDR) e i secure email gateway (SEG). Ciò è particolarmente rilevante considerando che le email di phishing sono il metodo principale utilizzato dai criminali del ransomware per infiltrarsi nelle reti.

È importante notare che, sebbene molti leader della sicurezza ritengano che l'acquisto del miglior prodotto per un dato progetto possa garantire la migliore postura di sicurezza, i risultati dell'indagine di quest'anno suggeriscono che le organizzazioni con un approccio focalizzato su prodotti specifici tendono ad essere più vulnerabili agli attacchi ransomware. Tuttavia, la tecnologia rappresenta solo una parte della soluzione. L'indagine ha evidenziato che quattro delle cinque principali sfide nella prevenzione del ransomware sono correlate a persone e processi. Con il continuo sviluppo del ransomware e la sofisticazione crescente dei metodi di attacco, è cruciale che i responsabili della sicurezza investano ora nelle tecnologie, nelle persone e nei processi adeguati a prevenire futuri incidenti ransomware.

l ransomware soni noti da decenni, tuttavia recentemente si è assistito ad un'escalation nell'uso di versioni di questo malware sempre più sofisticate e complesse. Questo incremento è dovuto in gran parte alla popolarità delle operazioni Ransomware-as-a-Service (RaaS), che hanno semplificato la diffusione di questi attacchi anche tra criminali non esperti di tecnologia. Con il crescere di questa minaccia, la preoccupazione tra i leader aziendali di tutto il mondo è in aumento.

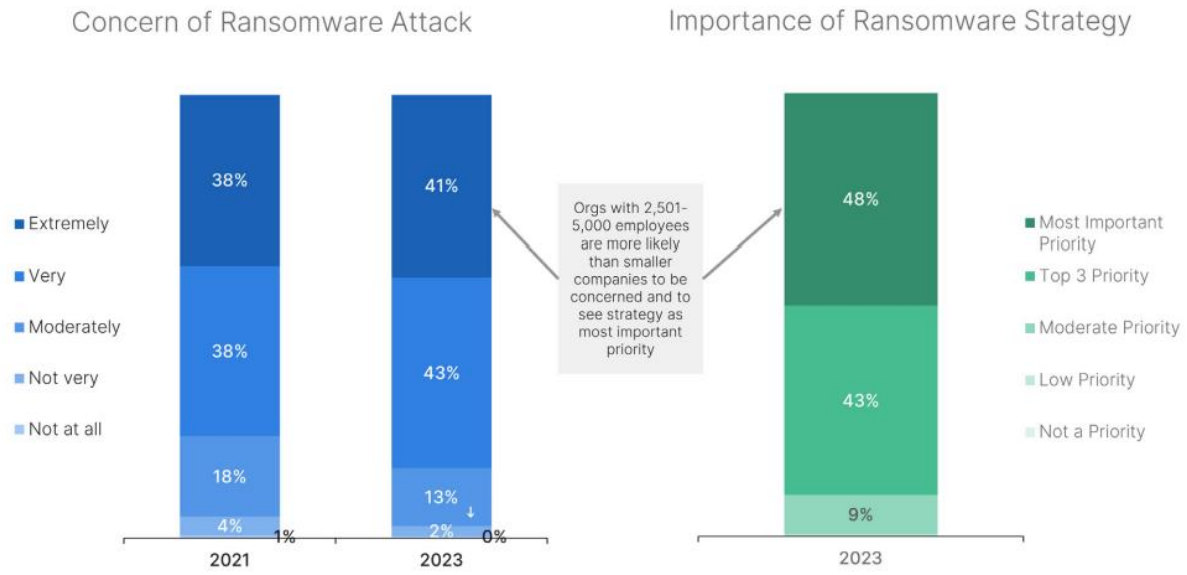

Figura 6. Sondaggio Fortinet: Preoccupazione in riferimento ad attacchi ransomware [19]

Secondo un sondaggio di Fortinet, azienda leader nello sviluppo software e sicurezza informatica, posto a 569 responsabili di cybersecurity provenienti da organizzazioni di tutti i tipi nel mondo, “more than 80% of respondents say they are “very” or “extremely” concerned about the threat of ransomware”. Tuttavia, oltre il 90% degli intervistati ha dichiarato che l'adozione di una strategia contro il ransomware è la più importante o una delle tre principali priorità del proprio team. E l'88% include l'assicurazione informatica come parte della propria strategia di preparazione. [19]

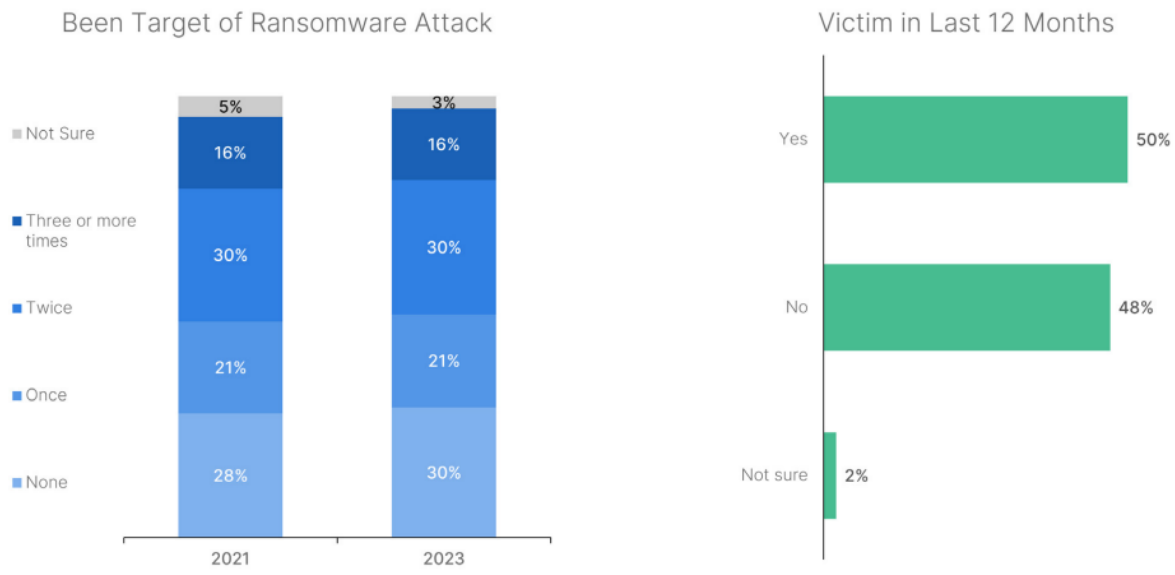

Figura 7. Sondaggio Fortinet: Incidenza di attacchi ransomware [19]

Sfortunatamente, esiste ancora una discrepanza significativa tra la percezione degli intervistati riguardo alla preparazione delle loro organizzazioni e la reale capacità di prevenire un incidente di ransomware. Metà delle aziende intervistate ha subito un attacco ransomware negli ultimi 12 mesi e il 46% è stato colpito da ransomware due o più volte. Tra le organizzazioni che hanno subito un attacco nel 2022, il phishing, ovvero l'inganno di individui o gruppi tramite email dannose, si conferma la tattica più frequente, impiegata nel 56% dei casi. Subito dopo si collocano l'uso di porte vulnerabili, con il 54%, e gli exploit di protocolli per desktop remoto, con il 51%. Considerando che più del 50% degli intervistati ha segnalato l'uso di molteplici metodi in un singolo attacco o in attacchi successivi, è evidente che gli autori di ransomware continuano a esplorare diverse vie di accesso per penetrare le difese organizzative.

La maggior parte degli intervistati il cui luogo di lavoro ha subito un attacco ransomware ha indicato che esiste una politica aziendale che prevede il pagamento del riscatto richiesto. È rilevante notare che, sebbene il 72% degli intervistati abbia identificato l'incidente entro poche ore, talvolta in minuti, oltre il 70% ha ammesso di aver pagato almeno in parte il riscatto richiesto dagli aggressori. Questo accade nonostante le raccomandazioni dell'FBI, secondo le quali pagare il riscatto contribuisce solo a perpetuare il problema e non assicura la restituzione dei dati.

È interessante osservare che le aziende appartenenti a certi settori tendono a pagare il riscatto più frequentemente rispetto ad altre. In particolare, le organizzazioni del settore manifatturiero risultano pagare più spesso il riscatto rispetto ad altri ambiti, con richieste economiche notevolmente più elevate: nel 25% dei casi di attacco in questo settore, il riscatto richiesto era pari o superiore a 1 milione di dollari. Questa propensione a pagare è comprensibile considerando gli alti costi associati ai tempi di inattività delle produzioni. Gli aggressori tendono a chiedere di più perché sanno che queste aziende sono disposte a pagare.

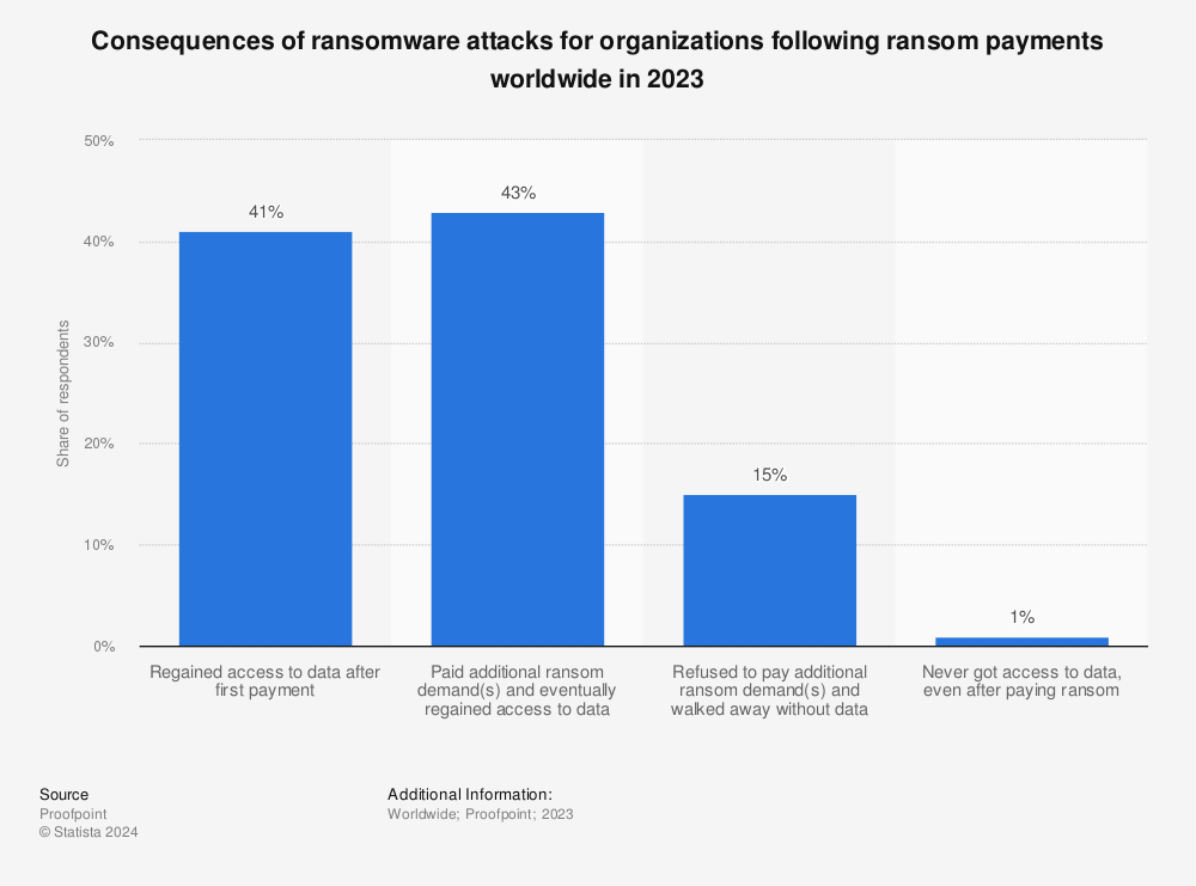

Figura 8. Consequences of ransomware attacks for organizations following ransom payments worldwide in 2023 [31]

Un sondaggio del 2023, prodotto da Proofpoint [31], società leader nel settore della cybersecurity, ha rivelato che dopo le infezioni da ransomware, circa il 41% delle organizzazioni intervistate ha riacquistato l'accesso ai dati dopo il pagamento del primo riscatto. In confronto, l'1% delle organizzazioni non ha mai ottenuto l'accesso ai dati, nemmeno dopo aver pagato un riscatto. Inoltre, quattro organizzazioni su dieci hanno dovuto pagare un ulteriore riscatto per riottenere l'accesso ai propri dati.

Tuttavia, accade che non pagando il riscatto si possa incorrere in costi decisamente più elevati di quelli che si incontrerebbero nell'assecondare le richieste dei malintenzionati. Sempre come riportato dall'FBI, ad una città statunitense, i cui sistemi erano stati infettati da Robbinhood, un particolare ransomware che può entrare nei sistemi con svariati modi, era stata richiesto un riscatto di 13 Bitcoin (76.000 dollari). Gli aggressori, entrati nella rete attraverso hardware e software vecchi e non aggiornati, hanno bloccato il servizio del server, impedendo il normale utilizzo della rete. Il riscatto non è stato pagato, ma il ripristino del servizio è stato stimato in oltre 9 milioni di dollari. [18] Non sottostare alle richieste è costato quasi 120 volte di più allo stato per riportare alla normalità il sistema.

In alcuni casi può essere più conveniente abbandonare il vecchio sistema per costruirne uno nuovo. Una contea statunitense infettata da Ryuk, un potente ransomware, ha deciso di non pagare i richiesti 1,2 milioni di dollari in cambio della chiave di decriptazione per sbloccare i server ma invece spendere 1 milione di dollari per comprare nuovi equipaggiamenti e pagare un' assistenza tecnica per ricostruire i loro sistemi.

Nonostante ci sia stata una riduzione nel numero di aziende che rilevano attività di ransomware — passando dal 22% di cinque anni fa al 13% nella prima metà del 2023 — questo non significa che la

minaccia del ransomware stia diminuendo. Al contrario, suggerisce che gli attacchi sono diventati più selettivi e mirati. Le bande di ransomware stanno affinando i loro modelli di business, orientandosi verso azioni più focalizzate e impiegando tattiche avanzate e flessibili. Questo cambiamento indica che, sebbene il numero totale di rilevazioni possa essere diminuito, l'impatto e la sofisticatezza degli attacchi sono in realtà aumentati. [20]

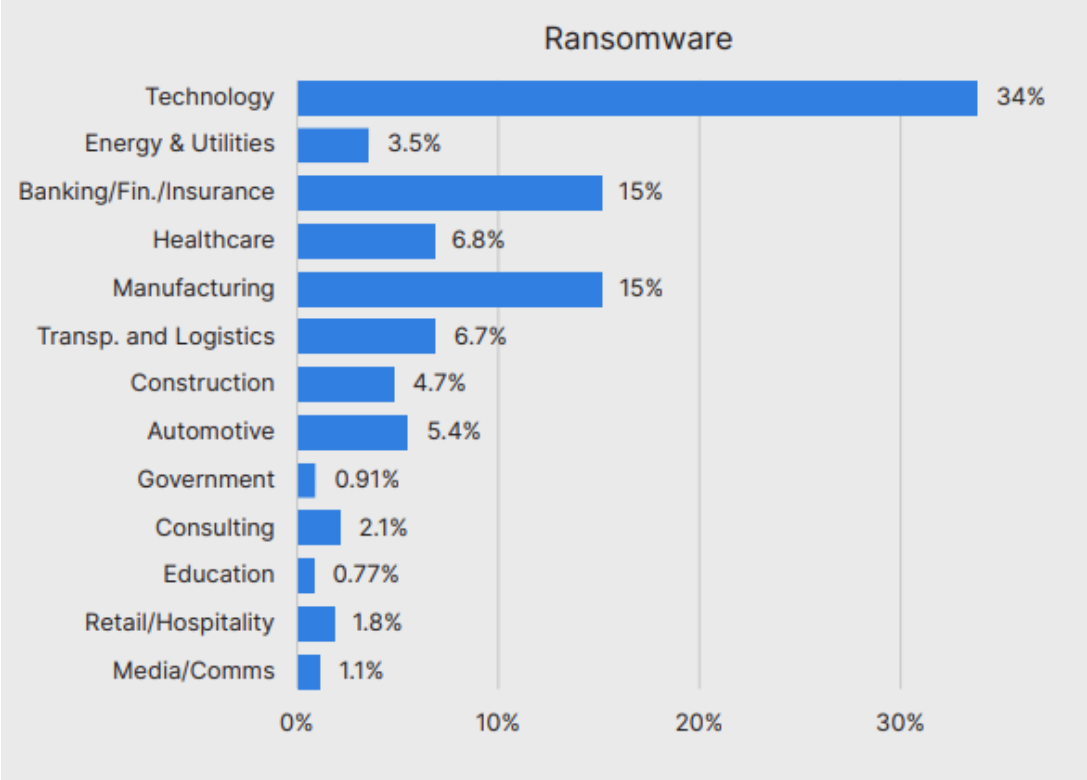

Figura 9. Distribuzione per settore di attacchi ransomware [20]

Nel recente rapporto sulle previsioni delle minacce per il 2024 di Fortinet [20], è stata evidenziata l'aspettativa che i criminali, alla ricerca di profitti maggiori, si concentrino su settori chiave quali sanità, servizi pubblici, produzione e finanza. Durante la seconda metà del 2023, si è notato un cambiamento nell'approccio dei criminali informatici, che hanno abbandonato la tradizionale tattica del "spray and pray" a favore di strategie più selettive e richieste di riscatto esorbitanti.

Il grafico riportato sopra mostra la distribuzione per settore degli attacchi ransomware registrati nella seconda metà del 2023, evidenziando una significativa presenza nei settori dell'energia, della sanità, dell'industria manifatturiera, dei trasporti e della logistica, e del automotive. Questi dati confermano le previsioni, con il 44% degli attacchi ransomware concentrati nei settori industriali in questo periodo. Questa tendenza è motivo di preoccupazione per diverse ragioni, in particolare per il potenziale impatto negativo e considerevole che le violazioni in questi settori critici possono avere sulla società.

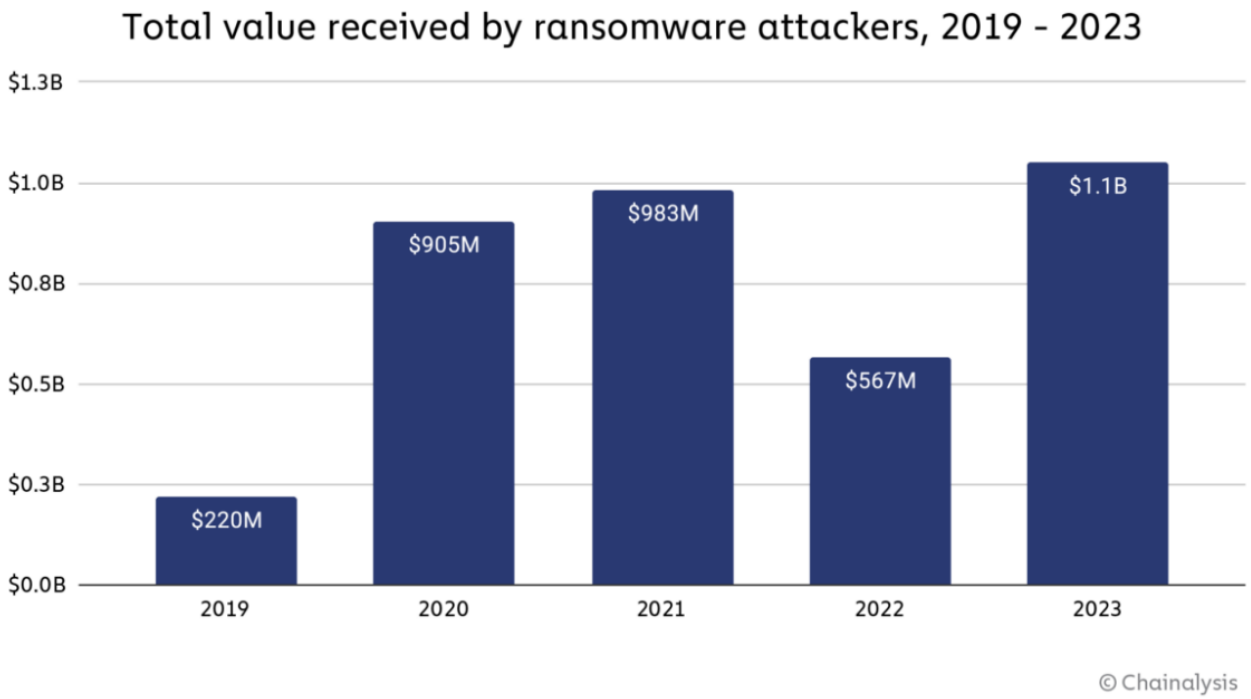

Figura 10. Totale per anno del valore dei riscatti pagati a seguito di un attacco ransomware [21]

Secondo un recente studio di Chainalysis, nel 2023, i pagamenti effettuati per i riscatti ransomware hanno raggiunto la cifra record di oltre un miliardo di dollari, il valore più elevato mai registrato. Anche se nel 2022 si è assistito a una riduzione nel volume dei pagamenti ransomware, l'analisi della tendenza generale dal 2019 al 2023 dimostra che il ransomware è un problema in costante crescita. È importante sottolineare che questa cifra non include l'impatto economico derivante dalla perdita di produttività e dai costi di riparazione legati agli attacchi. [21]

Per questo motivo, la lotta contro i ransomware non si limita soltanto all'implementazione di soluzioni tecniche avanzate; richiede anche una profonda comprensione del panorama delle minacce e un'attenta valutazione delle politiche di sicurezza a livello globale. Le strategie di prevenzione e mitigazione dei ransomware devono essere integrate e multifocali, combinando tecnologia, formazione umana e cooperazione internazionale.

Così come contro il Phishing, per combattere i ransomware la formazione e la consapevolezza degli utenti risultano essere uno strumento tanto efficace quanto le innovative soluzioni tecnologiche. Educare i dipendenti e gli utenti finali sulle migliori pratiche di sicurezza informatica, come l'importanza degli aggiornamenti software, può ridurre significativamente la superficie di attacco disponibile ai criminali. Inoltre, l'implementazione di politiche di backup regolari e verificate può salvaguardare i dati essenziali, permettendo alle organizzazioni di ripristinare le informazioni senza dover pagare il riscatto.

Dal punto di vista tecnologico, le soluzioni di sicurezza devono essere costantemente aggiornate per rispondere alle nuove varianti di ransomware che emergono continuamente. Questo include l'uso di software antivirus e antimalware sofisticati, firewall robusti e sistemi di rilevamento e risposta agli incidenti che possono isolare rapidamente gli attacchi e minimizzare i danni.

A livello internazionale, la cooperazione tra le agenzie di applicazione della legge di diversi paesi è cruciale. Condividere informazioni sulle minacce emergenti, coordinare le indagini e agire collettivamente contro le infrastrutture dei cybercriminali possono rafforzare le difese globali contro i

ransomware. Questo approccio collaborativo è essenziale per combattere un fenomeno che non conosce confini geografici.

La risposta legale ai ransomware sta diventando sempre più pertinente. Legislazioni che obbligano le organizzazioni a segnalare gli attacchi di ransomware e altre misure regolatorie possono aiutare a creare un ambiente meno permissivo per i criminali. In parallelo, il dibattito etico e legale sul pagamento dei riscatti necessita di una riflessione approfondita, considerando sia le immediate necessità operative delle organizzazioni colpite sia le implicazioni a lungo termine per la sicurezza collettiva.

Rimane quindi il dibattito sulla risposta ai ransomware: pagare il riscatto può sembrare una soluzione immediata per recuperare l'accesso ai dati, ma alimenta anche un'economia criminale e potrebbe non garantire realmente il recupero delle informazioni criptate. Questo contesto di incertezza rende i ransomware una delle sfide più significative nell'ambito della cybersecurity moderna.

2.4 Hacktivism

L'hacktivism, o attivismo informatico, è un fenomeno relativamente recente che combina l'hacking con l'attivismo politico o sociale. Si tratta di un modo per gli attivisti di promuovere cambiamenti sociali, politici o ambientali attraverso l'uso di tecniche informatiche. Il termine "hacktivism" è emerso durante le prime manifestazioni di disobbedienza civile digitale e si attribuisce la sua creazione ad una famosa organizzazione di proteste e movimenti digitali chiamata “Cult of the Dead Cow” quando un membro nominato Omega lo riporta in una email inviata internamente ad altri membri dell’organizzazione. Questa forma di attivismo si è sviluppata all'inizio degli anni '90, mano a mano che Internet è diventato uno strumento sempre più accessibile e influente. Originariamente, fu associato agli autori dei primi netstrike globali, organizzati per protestare contro violazioni dei diritti civili, governi corrotti o decisioni giudiziarie che prevedevano la pena capitale. I primi hacktivisti erano spesso hacker o gruppi di hacker che vedevano Internet come uno spazio ideale per promuovere la libertà di espressione e opporsi a politiche governative oppressive o a pratiche aziendali ritenute ingiuste. Con il tempo, l'uso del termine si è esteso a descrivere le azioni di coloro che, attraverso un uso innovativo delle reti e dei computer, hanno sfidato le politiche di governi e multinazionali. Questo include la creazione di petizioni online, lo sviluppo di virus non dannosi, la fondazione di siti web per la controinformazione, e lo sviluppo di altri strumenti volti a garantire la libera comunicazione elettronica per tutti i cittadini. [22]

Gli hacktivisti utilizzano una grande varietà di metodi. Le tattiche più comuni includono gli attacchi DDoS (Distributed Denial-of-Service), che mirano a chiudere i siti web sovraccaricandoli di traffico; le fughe di dati, in cui le informazioni sensibili vengono esposte pubblicamente; e il web defacement, che altera i siti web per visualizzare i messaggi degli attivisti. Questi metodi sono scelti in base alla loro capacità di attirare l'attenzione e influenzare l'opinione pubblica o politica.

All'interno della comunità hacktivista, esistono divergenze su quali metodi siano considerati accettabili. Ad esempio, sebbene gli hacktivisti spesso promuovano la libertà di espressione come un valore fondamentale, l'impiego di attacchi DDoS, il defacement di siti web e il furto di dati, che possono limitare o inibire la libertà di espressione, possono risultare contraddittori rispetto a tale valore. I metodi adottati dagli hacktivisti sono tecnicamente illegali e rientrano nella categoria dei crimini informatici. Nonostante ciò, spesso questi atti non sono oggetto di perseguimento giudiziario, poiché le forze dell'ordine tendono a non indagare su di essi frequentemente. Le difficoltà nel tracciare gli autori degli attacchi e l'entità relativamente minore dei danni spesso contribuiscono a questa situazione.

Gli attacchi hacktivistici non sono di natura violenta e non espongono i partecipanti a rischi di danni fisici, a differenza delle proteste fisiche. Tuttavia, in certi contesti, l'hacktivismo può potenzialmente

incitare a violenze. Inoltre, l'hacktivismo offre la possibilità di supportare cause in luoghi geograficamente distanti senza la necessità di spostarsi fisicamente. Questo permette anche a persone sparse in diverse località ma unite da obiettivi comuni, di collaborare e agire insieme a favore di una causa condivisa. [23]

I principali metodi di attacco sono:

- Blog online: Le cosiddette "talpe" richiedono la tutela della propria identità, specialmente quando prevedono di divulgare informazioni su figure di spicco. Un blog anonimo fornisce agli hacktivisti un mezzo sicuro per attirare attenzione sulla loro causa senza esporre dettagli che potrebbero identificarli.
- DDoS: L'attacco distributed denial-of-service rappresenta un'efficace strategia per interrompere le operazioni aziendali, danneggiando le attività e l'immagine di un'azienda agli occhi dei clienti e causando perdite economiche che possono ascendere a milioni di euro.
- Doxing: Il doxing si verifica quando informazioni personali e confidenziali di un individuo vengono esposte online. Questa pratica può essere particolarmente problematica quando la vittima, come un politico con un passato controverso, si trova a dover affrontare la pubblicazione online di vecchi problemi legali, danneggiando gravemente la propria carriera.
- Fughe di informazioni: Funzionari, dipendenti o ex collaboratori con rivelazioni da fare riguardo ai governi o alle aziende per cui hanno lavorato, trasmettono ai giornalisti documenti che supportano le argomentazioni degli hacktivisti, oppure pubblicano informazioni anonimamente per rimanere nascosti. Le informazioni diffuse possono avere un impatto significativo sull'opinione pubblica.
- Vandalismo dei siti web: Prendere il controllo di un sito web consente agli hacktivisti di esporre pubblicamente i loro messaggi di protesta e alterare il contenuto di siti aziendali o governativi.
- Clonazione dei siti web: Similmente al phishing, gli hacktivisti replicano un sito web utilizzando un URL leggermente diverso per indurre gli utenti a visitare la versione falsa, che sembrerà identica a quella originale ma mostrerà i messaggi degli hacktivisti anziché i contenuti legittimi.

Tra i più grandi esponenti di questa pratica, sicuramente Wikileaks e Anonymous sono i più celebri, sia per l’importanza delle loro azioni che per le organizzazioni contro cui si sono poste.

WikiLeaks, fondata nel 2006 da Julian Assange, è un'organizzazione internazionale che pubblica notizie e documenti classificati, rivelando spesso segreti di stato, dettagli su pratiche governative e scandali. L'organizzazione si è fatta un nome per il suo impegno nel promuovere la trasparenza e la libertà di informazione, esponendo abusi di potere e corruzione attraverso la divulgazione di informazioni riservate. Ha guadagnato l'attenzione globale nel 2010 con la pubblicazione di diversi grandi insiemi di documenti. Tra questi, spiccano il "Collateral Murder" video, che mostra il coinvolgimento delle forze armate americane in uccisioni di civili e giornalisti in Iraq, e i diari di guerra in Afghanistan, che rivelano informazioni sugli incontri di combattimento e l'intelligence operativa.

Un altro momento significativo nella storia di WikiLeaks è stata la pubblicazione di circa 250.000 cablogrammi diplomatici statunitensi nel 2010, noti come "Cablegate". Questi documenti hanno esposto valutazioni franche di leader stranieri e piani politici americani, provocando imbarazzo a numerosi governi. Questa pubblicazione ha scatenato un dibattito globale sull'equilibrio tra privacy, sicurezza e trasparenza, ponendo questioni legali e etiche sulla divulgazione di informazioni riservate.

La rivelazione nel 2016 delle email del Comitato Nazionale Democratico americano ha ulteriormente alimentato le controversie, con accuse che WikiLeaks avrebbe potuto essere usata come strumento di influenze politiche straniere, in particolare da parte della Russia. Le email hanno messo in luce strategie interne contro Bernie Sanders nella corsa presidenziale democratica, accendendo dibattiti sulla legittimità e l'imparzialità delle primarie democratiche.

Nonostante il suo ruolo nell'illuminare questioni nascoste e talvolta scomode, WikiLeaks è stata oggetto di numerose critiche per il potenziale pericolo che le sue pubblicazioni possono rappresentare per la sicurezza delle persone coinvolte nei documenti rivelati, spesso senza un'adeguata censura delle identità. [24]

Al pari di Wikileaks per quanto riguarda questa sfera di attivismo si mette in luce il gruppo di hacker che si inseriscono all'interno della famosa organizzazione Anonymous.

Anonymous è infatti un collettivo di hacker attivisti noto per le sue azioni di cyberattacco contro governi, organizzazioni e individui che considera coinvolti in comportamenti oppressivi, corrotti o ingiusti. Nato intorno alla metà degli anni 2000, Anonymous si distingue da Wikileaks per la sua struttura decentralizzata e anonima, priva di una leadership formale come quella di Julian Assange e senza un noto fondatore. I membri del collettivo si identificano spesso con la maschera di Guy Fawkes, resa celebre dal film "V per Vendetta", simbolo di resistenza contro l'oppressione.

Tra i più celebri attacchi del gruppo si evidenza l'operazione Payback del 2010, nata in risposta ai tentativi di diverse organizzazioni di fermare la pirateria online. Il gruppo ha condotto attacchi DDoS contro siti web di organizzazioni come la RIAA (Recording Industry Association of America) e la MPAA (Motion Picture Association of America), che erano state attive nel combattere il file sharing. Quando Visa, Mastercard e PayPal hanno bloccato i pagamenti verso WikiLeaks, Anonymous ha esteso l'operazione contro di loro, paralizzandone i servizi online.

Per quanto riguarda il panorama Italiano, l'hacktivismo si presenta come un problema in forte crescita negli ultimi anni, evidenziando come l'attivismo digitale sia una attività che raggiunge ed ispira sempre più persone.

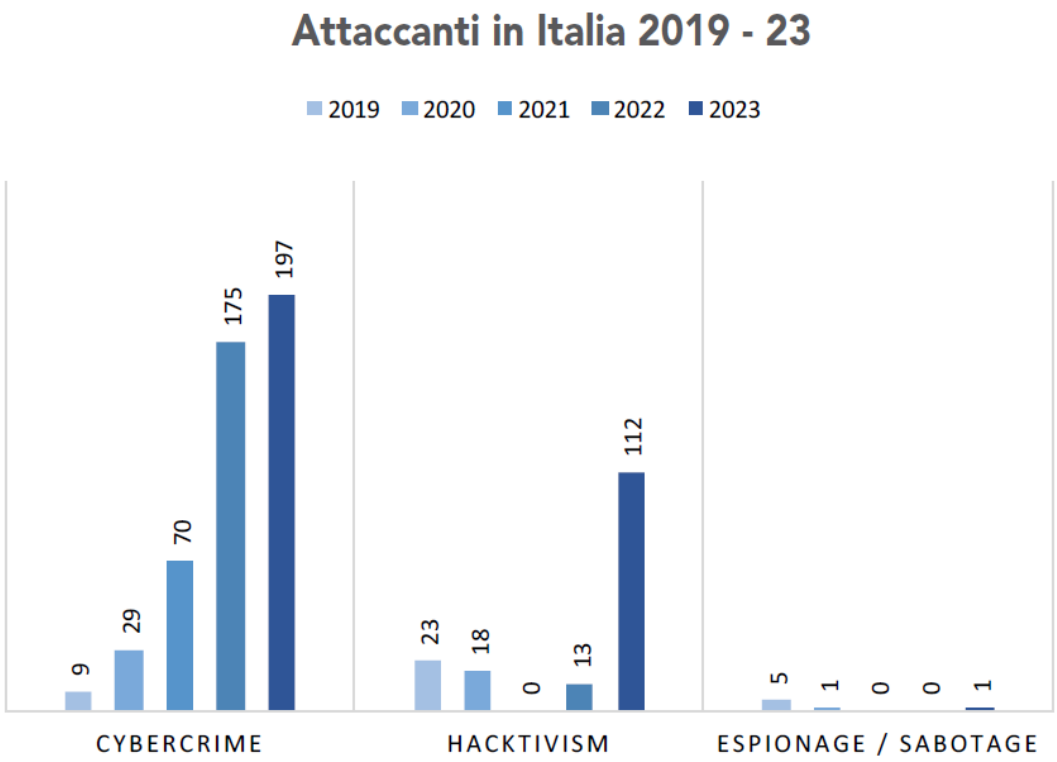

Figura 11. Rapporto Clusit 2024: Distribuzione dei cyberattacchi in Italia dal 2019 al 2023 [25]

Secondo l'ultimo rapporto Clusit del 2024 sulla sicurezza ICT in Italia, il 36% degli incidenti è classificato come Hacktivism. Il trend più marcato riguarda l'aumento degli attacchi di questo tipo, che sono

cresciuti dal 7% del campione nel 2022 (13 eventi) al 36% nel 2023 (112 eventi), registrando un incremento del 761%. Questo fenomeno esacerba una tendenza globale già allarmante, con gli attacchi Hacktivism che quasi triplicano, passando da 84 nel 2022 a 239 nel 2023, e un incremento di 6 punti percentuali. In Italia, gli incidenti di questa categoria rappresentano una percentuale molto più alta (36%) rispetto a quella globale (9%): circa il 47% del totale degli attacchi globali con finalità "Hacktivism" che rientrano nel nostro campione ha colpito organizzazioni italiane.

Secondo invece la Relazione annuale al Parlamento del 2023 [26], prodotta dall'Agenzia per la Cybersicurezza Nazionale, i numeri così elevati derivano dall'intensificarsi delle tensioni geopolitiche, legate sia alla continua guerra tra Russia e Ucraina sia ai cambiamenti degli equilibri in Medio Oriente a causa degli attacchi di Hamas contro Israele. Secondo la relazione, infatti, queste azioni hanno lo scopo di sostenere la causa di una delle parti in conflitto attraverso azioni *cyber* malevole con impatti chiaramente visibili, rivendicati successivamente dal gruppo stesso. Si tratta principalmente di eventi di tipo DDoS a danno di siti web di Pubbliche Amministrazioni e imprese che consistono nel modificare pagine di siti web (in genere obsoleti e poco protetti), sostituendole con un messaggio di rivendicazione, di apologia e simili.

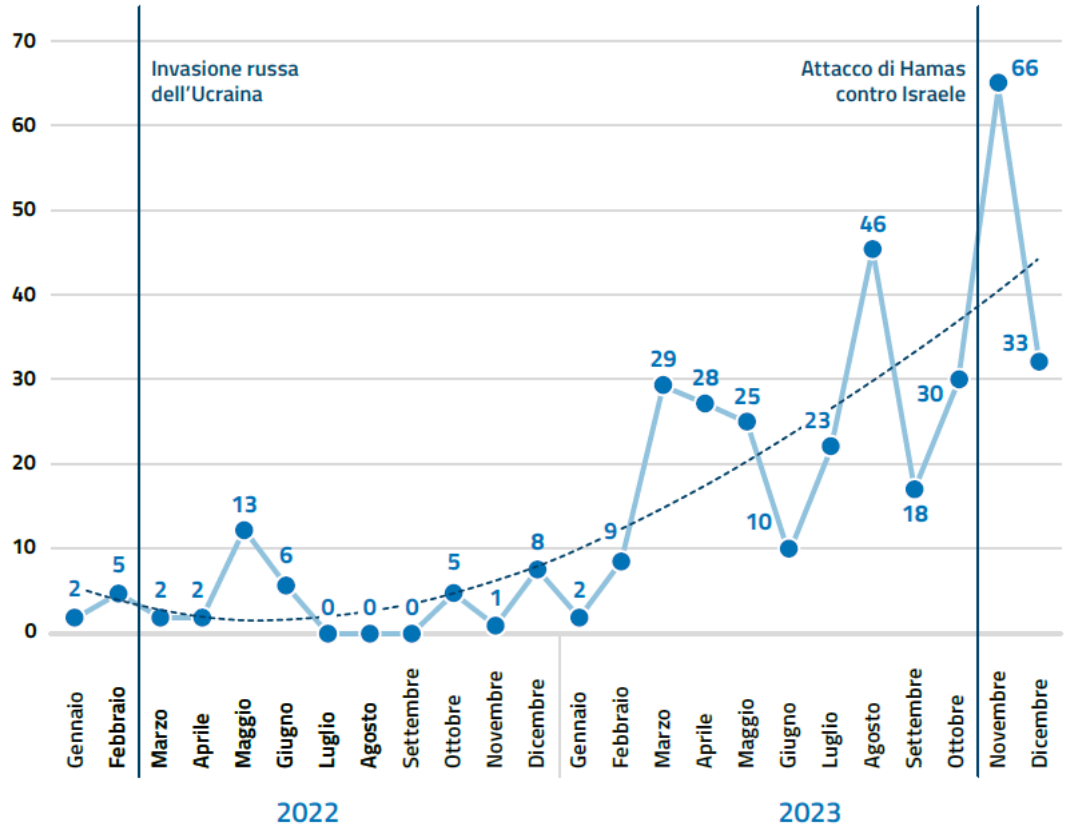

Figura 12. ACN: Numero attacchi DDoS mensili registrati in Italia [26]

Secondo l'analisi dell'ACN, come riportato in figura la maggior parte degli eventi è stata rivendicata da collettivi filorussi, mentre un gruppo filopalestinese ha condotto una singola campagna con 15 attacchi DDoS. I restanti eventi DDoS, non essendo stati rivendicati, non possono essere associati a specifiche compagini o ricondotti ai conflitti in atto.

Capitolo 3: Il panorama legislativo

Nell'era digitale, la cybersicurezza è diventata un pilastro fondamentale per la salvaguardia delle informazioni e la continuità operativa di enti pubblici e aziende private. Con l'escalation di minacce informatiche sempre più sofisticate, la necessità di un quadro normativo robusto e coerente è essenziale per prevenire, mitigare e rispondere efficacemente agli attacchi cyber. In questo contesto, le policy di cybersicurezza non solo costituiscono una risposta necessaria ai rischi emergenti ma rappresentano anche un impegno verso la protezione dei dati sensibili e la stabilità dei sistemi informativi.

In Italia, la sicurezza informatica è una priorità che viene gestita attraverso un'attenta regolamentazione governativa e una serie di incentivi statali. Questi strumenti legislativi e finanziari sono fondamentali non solo per tutelare le informazioni sensibili, ma anche per offrire una protezione efficace contro le minacce informatiche in crescita. Le normative dettagliano precise linee guida che le aziende devono seguire per assicurare la protezione dei dati dei loro clienti e delle loro operazioni.

Il ruolo degli incentivi governativi è vitale per promuovere l'adozione di standard elevati di sicurezza informatica. Attraverso benefici come agevolazioni fiscali, sussidi per la formazione del personale e finanziamenti per la ricerca e sviluppo, lo stato motiva le imprese a investire in soluzioni avanzate di sicurezza informatica. Questi incentivi non solo spingono le aziende a migliorare le proprie difese, ma rafforzano anche la resilienza nazionale di fronte alle cyber minacce.

Oltre a incentivare la sicurezza a livello aziendale, le normative e direttive del governo sono essenziali per facilitare la collaborazione tra il settore pubblico e quello privato. Queste direttive incoraggiano le aziende a condividere le informazioni sugli incidenti di sicurezza e le nuove minacce identificate, permettendo alle autorità di reagire prontamente e con maggiore efficacia. La comprensione e l'applicazione delle direttive governative relative alla cybersicurezza sono cruciali per mantenere sicura l'infrastruttura digitale italiana, sostenere l'innovazione tecnologica e proteggere le informazioni sensibili sia delle imprese che dei cittadini. Questo impegno congiunto tra pubblico e privato nel campo della cybersicurezza è indispensabile per affrontare le sfide della modernità digitale.

Questo capitolo esamina in modo approfondito le norme e gli obblighi legislativi che regolano la cybersicurezza in Italia, focalizzandosi tanto sul settore pubblico quanto su quello privato. Verranno trattate le principali leggi, regolamenti e standard internazionali, esplorando come questi influenzino la gestione della sicurezza delle informazioni a livello nazionale. L'obiettivo è delineare un panorama chiaro delle responsabilità legali e delle prassi operative che enti e aziende devono adottare per navigare efficacemente nel complesso ambiente della cybersicurezza odierna. Si discuterà delle sfide che entrambi i settori affrontano nell'adempimento di tali obblighi, dalle difficoltà tecniche e finanziarie alla necessità di una costante aggiornamento delle competenze. L'introduzione di normative specifiche e la loro applicazione pratica non solo aumentano la sicurezza informatica ma rafforzano anche la fiducia tra i consumatori e i cittadini, creando un ambiente digitale più sicuro e stabile.

3.1 Le prime normative e l’intervento dell’UE

Il Decreto Legislativo 7 marzo 2005, n. 82, noto come "Codice dell'Amministrazione Digitale" (CAD), rappresenta una pietra miliare nella legislazione italiana per quanto riguarda la digitalizzazione della Pubblica Amministrazione. Questo decreto ha lo scopo di regolamentare l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) all'interno delle amministrazioni pubbliche per migliorare l'efficienza e la trasparenza dei servizi pubblici offerti ai cittadini e alle imprese. Nel corso degli anni questo decreto è stato modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il

decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale. L'ultimo aggiornamento normativo ha permesso una sua significativa razionalizzazione, grazie anche all'intervento dell'Agenzia per l'identità digitale che riassume quali siano stati i punti focali di cambiamento e aggiornamento del decreto [27]:

- è stata sottolineata con maggior forza la natura di carta di cittadinanza digitale della prima parte del CAD con disposizioni volte ad attribuire a cittadini e imprese i diritti all'identità e al domicilio digitale, alla fruizione di servizi pubblici online e mobile oriented, a partecipare effettivamente al procedimento amministrativo per via elettronica e a effettuare pagamenti online;
- è stata promossa l'integrazione e l'interoperabilità tra i servizi pubblici erogati dalle pubbliche amministrazioni in modo da garantire a cittadini e imprese il diritto a fruirne in maniera semplice;
- è stata garantita maggiore certezza giuridica alla formazione, gestione e conservazione dei documenti informatici prevedendo che non solo quelli firmati digitalmente – o con altra firma elettronica qualificata - ma anche quelli firmati con firme elettroniche diverse possano, a certe condizioni, produrre gli stessi effetti giuridici e disporre della stessa efficacia probatoria senza prevedere l'intervento di un giudice caso per caso;
- è stata rafforzata l'applicabilità dei diritti di cittadinanza digitale e promosso l'innalzamento del livello di qualità dei servizi pubblici e fiduciari in digitale, sia istituendo presso l'AgID l'Ufficio del Difensore civico per il digitale, sia aumentando la misura delle sanzioni irrogabili qualora i fornitori di servizi fiduciari violino le norme;
- è stato promosso un processo di valorizzazione del patrimonio informativo pubblico riconducendolo tra le finalità istituzionali di ogni amministrazione.

Questo processo ha comportato un'efficace deregolamentazione, attraverso la semplificazione del linguaggio utilizzato e la sostituzione delle precedenti regole tecniche con linee guida più flessibili. Questo cambiamento facilita un'adozione più agile e reattiva delle norme, permettendo una risposta più immediata all'evoluzione tecnologica. La sicurezza e la privacy sono anch'esse al centro delle preoccupazioni del CAD. Nel regolamentare l'uso delle tecnologie digitali, il decreto enfatizza la necessità di proteggere i dati personali dei cittadini. Implementando standard rigorosi per la sicurezza dei dati e conformandosi alle normative sulla privacy, il CAD garantisce che le informazioni personali siano trattate con la massima cura e sicurezza.

Gli sforzi per la definizione di normative in materia di sicurezza digitale arrivano anche dall'Unione Europa con la Direttiva (UE) 2016/1148, comunemente nota come Direttiva NIS (Network and Information Systems), che rappresenta la volontà di rafforzare la sicurezza delle reti e dei sistemi informativi a livello comunitario. Adottata il 6 luglio 2016, questa direttiva punta a migliorare il livello generale di cybersicurezza degli Stati membri, garantendo una maggiore uniformità nella protezione delle infrastrutture critiche.

Questa direttiva stabilisce determinate misure e obblighi che gli stati membri devono implementare per "conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno" [28] in risposta ad un aumento dell'intensità, la frequenza e le conseguenze degli incidenti di sicurezza che costituiscono una minaccia seria per la stabilità delle reti e dei sistemi informativi. Questi sistemi rischiano di essere presi di mira attraverso attacchi deliberati volti a danneggiarli o a interromperne le operazioni. Tali incidenti, infatti, possono bloccare le attività economiche, generare significative perdite finanziarie, erodere la fiducia degli utenti e infliggere danni considerevoli all'economia dell'Unione Europea. Nella direttiva si evidenzia inoltre come le reti e i sistemi informativi, con Internet in prima linea, rivestano un ruolo cruciale nel facilitare i movimenti transfrontalieri di beni, servizi e persone. Data la loro natura transnazionale, qualsiasi grave perturbazione di questi sistemi, che sia

intenzionale o accidentale, può avere ripercussioni dirette sugli Stati membri e sull'intera Unione Europea e quindi la sicurezza di queste reti e sistemi informativi è fondamentale per garantire il corretto funzionamento del mercato interno.

La normativa, dopo aver espresso le motivazioni della necessità di una pratica comune, procede ad elencare le direttive che vengono individuate per affrontare comunitariamente queste problematiche. Nello specifico la normativa riporta:

a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;
b) istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;
c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace
d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;
e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

La normativa si occupa anche di andare a definire i termini chiave e fondamentali per comprendere e applicare le disposizioni sulla sicurezza delle reti e dei sistemi informativi. In questo modo è possibile uniformare la comunicazione tra le organizzazioni, primo passo necessario per affrontare a livello comunitario le difficoltà che questo settore presenta. In particolare definisce:

- Rete e sistema informativo: qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali
- Sicurezza della rete e dei sistemi informativi: la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi
- Incidente: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi

Nell'articolo 7 si richiede ad ogni stato membro la definizione di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, in particolare si richiede la definizione di obiettivi e le priorità della strategia, di una governance per conseguire tali obiettivi, misure di preparazione, risposta e recupero ed anche un piano per la valutazione dei rischi.

Richiede anche la strutturazione di CSIRT (Computer Security Incident Response Team) ovvero delle strutture responsabili della gestione degli incidenti di sicurezza informatica e della fornitura di assistenza per la gestione e la risposta a tali incidenti. I CSIRT operano a livello nazionale e aiutano a coordinare la risposta agli incidenti e a migliorare la resilienza dei sistemi informativi. I compiti principali di questi team sono la creazione di una rete di comunicazione internazionale, così che si renda possibile "scambiare informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione", "scambiare e mettere a disposizione su base volontaria informazioni non riservate su singoli incidenti" ed anche "fornire sostegno agli Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria". La Direttiva stabilisce quindi un quadro per la condivisione di informazioni e la cooperazione tra gli Stati membri, inclusa la creazione di un gruppo di cooperazione e di team di risposta agli incidenti informatici per facilitare la risposta coordinata agli incidenti di sicurezza.

L'obiettivo principale della Direttiva è quello di migliorare la sicurezza delle reti e dei sistemi informativi, cruciali per il funzionamento quotidiano delle società moderne. Di fronte all'aumento della frequenza e dell'impatto degli attacchi informatici, che possono impedire le attività economiche e provocare notevoli perdite finanziarie, nonché minare la fiducia degli utenti e causare danni economici significativi, l'UE ha riconosciuto la necessità di un approccio armonizzato e cooperativo alla sicurezza informatica.

In risposta all'emanazione di questa normativa, in Italia viene presentato il Decreto Legislativo n. 65/2018 ovvero l'implementazione delle misure presenti nella normativa. Il decreto si concentra principalmente sull'identificazione di operatori di servizi essenziali (OSE) nei settori dell'energia, trasporti, salute, banche, infrastrutture di mercato finanziario, fornitura e distribuzione d'acqua potabile, e infrastrutture digitali. Una volta identificati, questi operatori sono tenuti a prendere misure tecniche e organizzative adeguate per gestire i rischi per la sicurezza delle reti e dei sistemi informativi utilizzati nell'erogazione dei servizi essenziali. Inoltre, il decreto stabilisce l'obbligo per gli OSE e per i fornitori di servizi digitali di notificare senza ingiustificato ritardo all'autorità nazionale competente gli incidenti che hanno un impatto significativo sulla continuità dei servizi essenziali. Questa disposizione mira a migliorare la consapevolezza nazionale e la risposta complessiva agli incidenti di sicurezza informatica.

Viene anche stabilita la creazione del CSIRT, in particolare è incaricato di svolgere vari compiti essenziali per la sicurezza informatica, tra cui la gestione degli incidenti, la collaborazione rapida ed efficace tra enti e la protezione delle infrastrutture critiche.

In particolare, il CSIRT italiano funziona come il punto focale nazionale per la gestione degli incidenti di sicurezza informatica, coordinando con altre autorità nazionali e internazionali per garantire una risposta tempestiva e efficace. Le attività principali includono la raccolta e l'analisi delle informazioni sugli incidenti, la fornitura di supporto tecnico agli enti colpiti e la diffusione di avvisi di sicurezza.

Il CSIRT collabora strettamente con altri CSIRT europei e internazionali per scambiare informazioni e pratiche migliori, contribuendo così a un approccio più coordinato e robusto alla sicurezza informatica a livello transnazionale. [29]

3.2 PNRR

Nel 2021 in Italia viene ufficialmente approvato il Piano di ripresa e resilienza, meglio noto come PNRR, che ha come intento il rilancio dell'economia a seguito della pandemia di COVID-19, grazie ad importanti investimenti in ambito green e digitale.

In particolare in ambito digitale, grazie alle possibilità di investimento nate dallo sblocco di questi fondi europei, nasce in l'Agenzia per la cybersicurezza nazionale (ACN), che, come riportato sul sito ufficiale: "è stata istituita dal Decreto Legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico" [30].

L'agenzia opera come autorità nazionale per la cybersicurezza e da punto di contatto per tutte le questioni relative alla sicurezza cibernetica, coordinando gli sforzi tra le varie entità governative e il settore privato. I principali compiti di questa organizzazione sono quelli di tutelare la sicurezza e la resilienza nello spazio cibernetico, di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica. La creazione dell'ACN rappresenta un passo fondamentale per l'Italia, in risposta all'aumento delle minacce cyber a livello globale e alla necessità di una strategia unificata che possa garantire una difesa efficace contro gli attacchi informatici. L'agenzia si impegna anche nella promozione di una cultura della sicurezza informatica, supportando lo sviluppo di competenze avanzate e la ricerca in questo campo critico.

Con la sua creazione è stata progettata una strategia, composta da multiple milestone corrispondenti a determinati obiettivi, volta a pianificare, coordinare e attuare misure tese a rendere l'Italia un paese più sicuro e resiliente. Il piano prevede il raggiungimento di 82 misure specifiche entro il 2026, con l'obiettivo di rendere il Paese più sicuro e resiliente di fronte alle minacce informatiche.

Questa strategia si concentra su diversi aspetti chiave:

1. **Innovazione e Rafforzamento della Sicurezza**: La strategia si impegna a innovare e rafforzare la sicurezza attraverso lo sviluppo e l'implementazione di nuove tecnologie e pratiche. Questo include il miglioramento della sicurezza delle infrastrutture critiche e il rafforzamento delle difese contro gli attacchi cyber.

2. **Collaborazione Pubblico-Privato**: Un elemento centrale della strategia è facilitare una maggiore collaborazione tra il settore pubblico e quello privato. Questo approccio collaborativo è essenziale per una risposta efficace e tempestiva alle minacce informatiche, permettendo una condivisione di risorse e informazioni che può accelerare la reazione agli attacchi e migliorare la prevenzione.

3. **Formazione e Sensibilizzazione**: Un altro pilastro della strategia è la formazione e la sensibilizzazione sia per i cittadini che per le imprese. La strategia prevede iniziative educative per diffondere una cultura della sicurezza digitale più robusta, sensibilizzando la popolazione sui rischi del cyber spazio e su come proteggersi efficacemente.

4. **Sgravi Fiscali e Incentivi**: Per supportare queste iniziative, la strategia include anche misure di incentivazione economica come sgravi fiscali per le aziende che investono in cybersecurity. Questo aspetto è volto a stimolare ulteriormente gli investimenti nel settore e a supportare le imprese nello sviluppo di soluzioni innovative.

L'ACN, attraverso questa strategia, mira a creare un ambiente digitale sicuro che protegga i cittadini e le infrastrutture nazionali dalle crescenti minacce cyber, garantendo così la stabilità e la sicurezza del sistema Paese nel suo complesso.

All'interno dell'organizzazione sono presenti diverse divisioni con compiti specifici, in modo da poter lavorare in modo mirato sulle principali necessità del paese.

- **CSIRT**: per la gestione delle risposte agli incidenti di sicurezza informatica è stato formato un **Computer Security Incident Response Team**. I CSIRT sono organismi essenziali alle organizzazioni per cercare di difendersi contro le minacce informatiche e mitigare rapidamente qualsiasi danno causato da tali incidenti. Il CSIRT dell'ACN ha la funzione di rispondere in modo coordinato agli incidenti di sicurezza, assicurando che le violazioni siano contenute e che i sistemi colpiti siano ripristinati e resi sicuri il più velocemente possibile. È anche responsabile del monitoraggio degli incidenti a livello nazionale, emettere preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti, l'analisi dinamica dei rischi e degli incidenti, la sensibilizzazione situazionale e la partecipazione alla rete dei CSIRT. Mensilmente si occupa anche della redazione di un documento riportante i numeri e gli indicatori relativi alle attività operative dell'Agenzia, articolazione tecnico-operativa e hub nazionale delle notifiche di incidenti previste per legge.
- **CVCN**: Il Centro di Valutazione e Certificazione Nazionale è incaricato di valutare la sicurezza di beni, sistemi e servizi ICT che verranno utilizzati all'interno del Perimetro, conformemente alle categorie stabilite dal DPCM del 15 giugno 2021. Il CVCN ha implementato le metodologie utilizzate durante il processo di valutazione, come quella per l'elaborazione dell'analisi del rischio, che le entità all'interno del Perimetro utilizzano per preparare la documentazione da allegare alla comunicazione

di affidamento. Le funzioni del CVCN sono affidate al Servizio Certificazione e Vigilanza di ACN. I principali ambiti di competenza sono:

  - **Le comunicazioni di affidamento**: prevede l'esecuzione di test hardware e software sui componenti della fornitura. In questo processo, il CVCN si coordina con i Centri di Valutazione (CV) presso i Ministeri della Difesa e dell'Interno e può avvalersi del supporto di una rete di Laboratori Accreditati di Prova (LAP).
  - **Coordinamento per l'esercizio dei poteri speciali:** L'Agenzia, per le materie di sua competenza, è parte del gruppo di coordinamento incaricato dell'esercizio dei poteri speciali, specificatamente per l'analisi degli aspetti tecnici di cybersicurezza in riferimento alle notifiche legate alla tecnologia 5G e, prospetticamente, ad altri settori tecnologici che saranno inclusi nella normativa Golden Power a seguito di recenti aggiornamenti legislativi. Nello stesso contesto, l'Agenzia partecipa anche al Comitato di monitoraggio, il quale si occupa di verificare il rispetto delle prescrizioni e delle condizioni stabilite dal provvedimento dei poteri speciali.
  - **Accreditamento LAP:** Il CVCN è l'ente di accreditamento dei Laboratori Accreditati di Prova (LAP) che potranno fornire supporto nella fase di esecuzione dei test.

- **NCC**: Il Centro Nazionale di Coordinamento Italiano assiste il Centro europeo di competenza in cybersecurity (ECCC) nel suo obiettivo di rafforzare l'autonomia strategica dell'Unione Europea, supportando lo sviluppo di capacità, risorse e competenze tecnologiche. In particolare, l'NCC agisce come intermediario tra la "community" nazionale di stakeholder attivi nel campo della cybersicurezza e l'ECCC e le sue attività sono gestite dall'Agenzia per la cybersicurezza nazionale. La missione dell'ECCC e della rete di NCC a livello nazionale è di rafforzare l'autonomia strategica dell'Unione Europea nel campo della cybersicurezza. Questo include il sostegno allo sviluppo di capacità, risorse e competenze tecnologiche e l'incremento della competitività internazionale dell'industria cyber europea. L'obiettivo è assicurare standard elevati e trasformare la cybersicurezza in un leva competitiva per altri settori industriali dell'Unione. Inoltre favorisce, stimola e facilita l'ingresso della società civile, dell'industria, in particolare delle startup e delle piccole e medie imprese (PMI), della comunità accademica e della ricerca, nonché di altri attori nazionali, nei progetti transfrontalieri e nelle iniziative legate alla cybersicurezza che sono finanziati dai programmi pertinenti dell'Unione Europea.

Capitolo 4: Il cyber risk nelle imprese

4.1 I rischi della digital transformation

Nel contesto economico contemporaneo, caratterizzato da un'intensa digitalizzazione, il cyber risk rappresenta una minaccia crescente per le imprese di ogni dimensione e settore. L'incremento della connettività e l'adozione massiva delle tecnologie informatiche hanno indubbiamente apportato benefici in termini di efficienza e innovazione. Tuttavia, hanno altresì esposto le aziende a nuovi vulnerabilità e rischi come la perdita di dati sensibili, i furti di proprietà intellettuale, gli attacchi ai sistemi di pagamento online e le interruzioni dell'operatività che possono avere conseguenze disastrose sul piano economico e legale.

L'introduzione del cyber risk nelle strategie di gestione aziendale non è solo una questione di sicurezza IT, ma un aspetto cruciale della governance aziendale che impatta sulla stabilità finanziaria e sulla reputazione dell'organizzazione.

Per affrontarlo efficacemente, le imprese devono implementare un framework di sicurezza informatica che includa la valutazione continua delle vulnerabilità, l'adozione di tecnologie di protezione avanzate, la formazione degli impiegati sulle migliori pratiche di sicurezza e la creazione di un piano di risposta agli incidenti che permetta di reagire prontamente in caso di attacchi. Inoltre, la collaborazione con esperti di sicurezza e l'aggiornamento costante sulle nuove minacce sono fondamentali per anticipare e mitigare i rischi.

La sfida principale nel gestire il cyber risk è che il paesaggio delle minacce è in continua evoluzione, con attori delle minacce che sviluppano continuamente nuovi metodi per sfruttare vulnerabilità note e ignote. Di conseguenza, per le aziende diventa essenziale non solo proteggersi dagli attacchi, ma anche essere resilienti, ossia capaci di reagire rapidamente e efficacemente in caso di incidenti, minimizzando i danni e ripristinando le operazioni nel più breve tempo possibile.

L'importanza della resilienza cibernetica è sottolineata anche dalla crescente regolamentazione in materia di sicurezza informatica, che impone alle aziende di adottare misure preventive e di risposta agli incidenti cyber. Le imprese sono quindi chiamate a investire in tecnologie avanzate di sicurezza, formazione del personale e politiche di gestione del rischio che considerino le minacce cyber come una componente cruciale del rischio aziendale complessivo.

In questo scenario, diventa imperativo per i leader aziendali comprendere appieno le implicazioni del cyber risk e integrare la gestione di tale rischio nella pianificazione strategica dell'azienda. Solo attraverso un impegno congiunto e coordinato è possibile proteggere le risorse aziendali critiche e garantire la continuità operativa in un'era definita da minacce cyber in costante evoluzione.

Tra il 2019 e il 2023, sono stati registrati 653 attacchi di particolare gravità che hanno coinvolto entità italiane. Di questi, 310 incidenti si sono verificati nell'ultimo anno, rappresentando oltre il 47% del totale degli attacchi censiti in Italia a partire dal 2019. La percentuale sale addirittura al 76% se si considerano gli incidenti avvenuti a partire dal 2022, con 498 eventi su 653 totali.

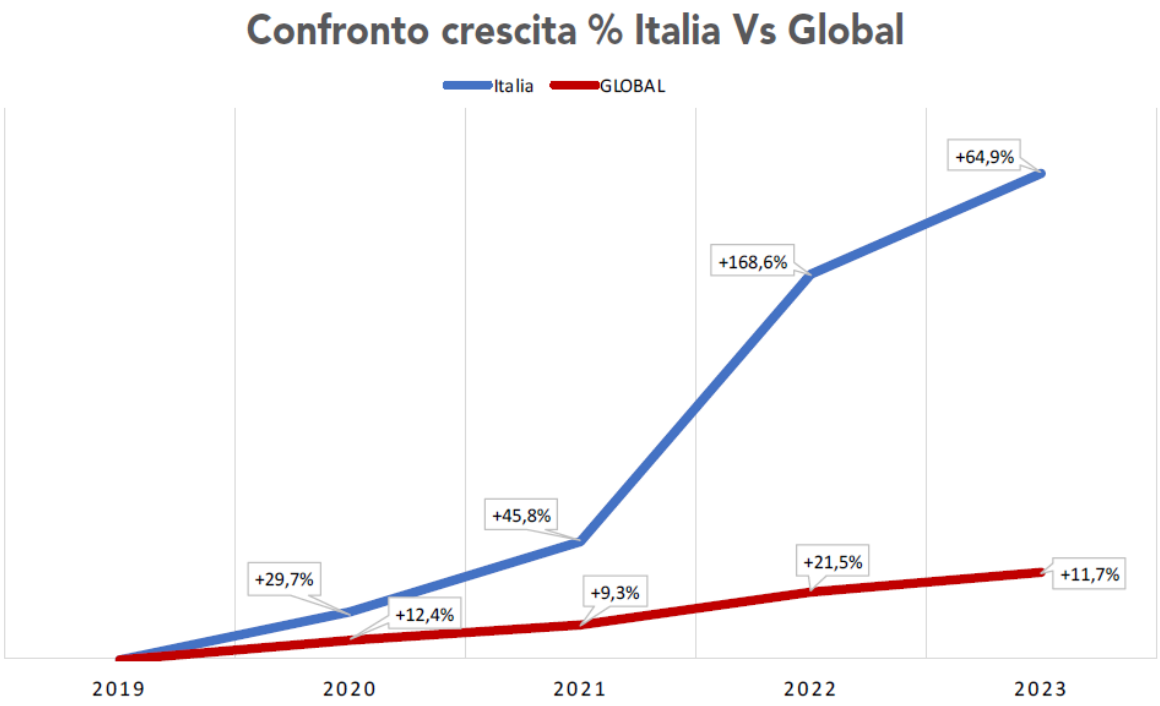

Figura 13. Crescita percentuale di cyber attacchi Italia Vs Global [25]

Il numero di incidenti rilevati è aumentato del 65% rispetto all'anno precedente, un incremento che segue il preoccupante +169% registrato tra il 2021 e il 2022. La situazione in Italia diventa ancora più allarmante se confrontata con la crescita globale: mentre gli attacchi in Italia hanno segnato un aumento del 65%, a livello mondiale l'incremento è stato molto più moderato, del 12%. Questo suggerisce che gli attacchi in Italia stanno crescendo a un ritmo particolarmente elevato, il che potrebbe indicare una tendenza dei cybercriminali a prendere di mira specificamente le vittime italiane o, più probabilmente, una loro insufficiente capacità di protezione. Questo è particolarmente grave considerando che gli investimenti in sicurezza in Italia continuano a crescere.

Esaminando la distribuzione delle vittime, la categoria "Government" si distingue per il maggior numero di attacchi, rappresentando il 19% del totale, in gran parte a causa dell'escalation degli eventi di "Hacktivism". Segue il "Manufacturing" con il 13%, più frequentemente bersaglio di attacchi di matrice criminale.

La ripartizione è notevolmente diversa rispetto a quella globale, dove queste due categorie rappresentano rispettivamente solo il 12% e il 6% degli attacchi, posizionandosi al terzo e settimo posto. Sorprendentemente, un quarto del totale degli attacchi globali al "Manufacturing" coinvolge realtà italiane. Questi dati delineano un panorama preoccupante per la capacità di protezione sia delle organizzazioni pubbliche sia delle imprese: è evidente che le tecniche difensive attuali non sono all'altezza di quelle degli attaccanti e che la presenza di vulnerabilità rende questi obiettivi particolarmente attraenti per gli hacker. Questa tendenza merita un'attenzione particolare e potrebbe aggravarsi ulteriormente, dato che le tecniche di attacco diventano sempre più sofisticate, anche con l'uso di "Artificial Intelligence". È essenziale che le contromisure adottate dalle organizzazioni si evolvano per equipararsi al livello tecnologico degli attaccanti.

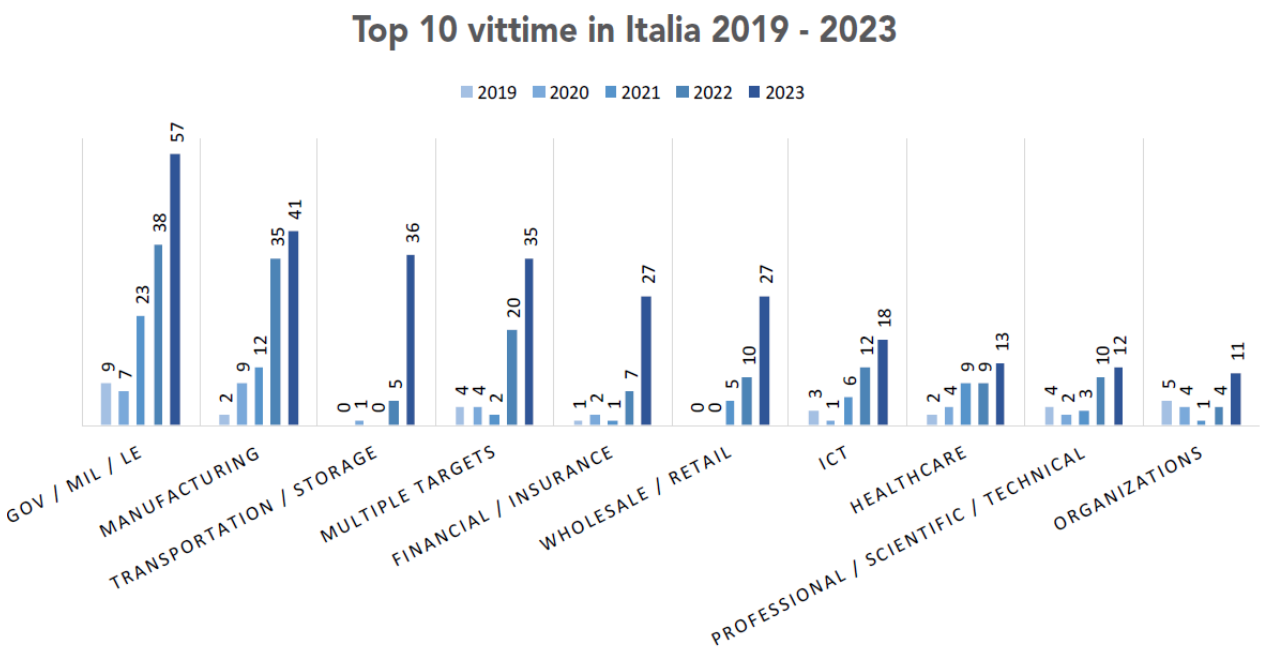

Figura 14. Numero di attacchi cyber subiti per settore 2019-2023 [25]

Se si considerano i valori assoluti (Fig. 14), il settore "Transportation" evidenzia un aumento del 620% rispetto al 2022, seguito dai settori "Financial / Insurance" (+286%), "Organizations" (+175%), "Wholesale / Retail" (+170%) e "Telco" (+133%). Tra i settori più colpiti, il "Government" ha visto un incremento del 50% degli attacchi, da 38 nel 2022 a 57 nel 2023, mentre il "Manufacturing" ha registrato un incremento più contenuto del 17%.

Analizzando l'evoluzione nel tempo della distribuzione percentuale degli incidenti (Fig. 15), il segmento "Multiple Targets" mostra un leggero aumento rispetto al dato globale, che invece registra una notevole diminuzione. Questo suggerisce che il livello di preparazione delle aziende italiane ha un impatto significativo sulla crescita del numero di incidenti.

Per quanto riguarda l'incidenza sul totale degli attacchi, il settore "Transportation" in Italia mostra un'impennata di ben 9 punti percentuali, simile a quanto osservato nei settori "Wholesale/Retail" e "Financial", che registrano un aumento della loro incidenza rispettivamente di 3,5 e 5 punti percentuali.

La marcata crescita di questi settori (Multiple Targets, Transportation, Wholesale/Retail, Financial) influisce sulla variazione, rispetto al 2022, nella distribuzione delle percentuali dei settori colpiti nel 2023. Per esempio, nel settore "Government" si registra una diminuzione percentuale, nonostante un incremento degli attacchi in termini assoluti. Lo stesso fenomeno si verifica per i settori "Healthcare", "Manufacturing" e "Professional".

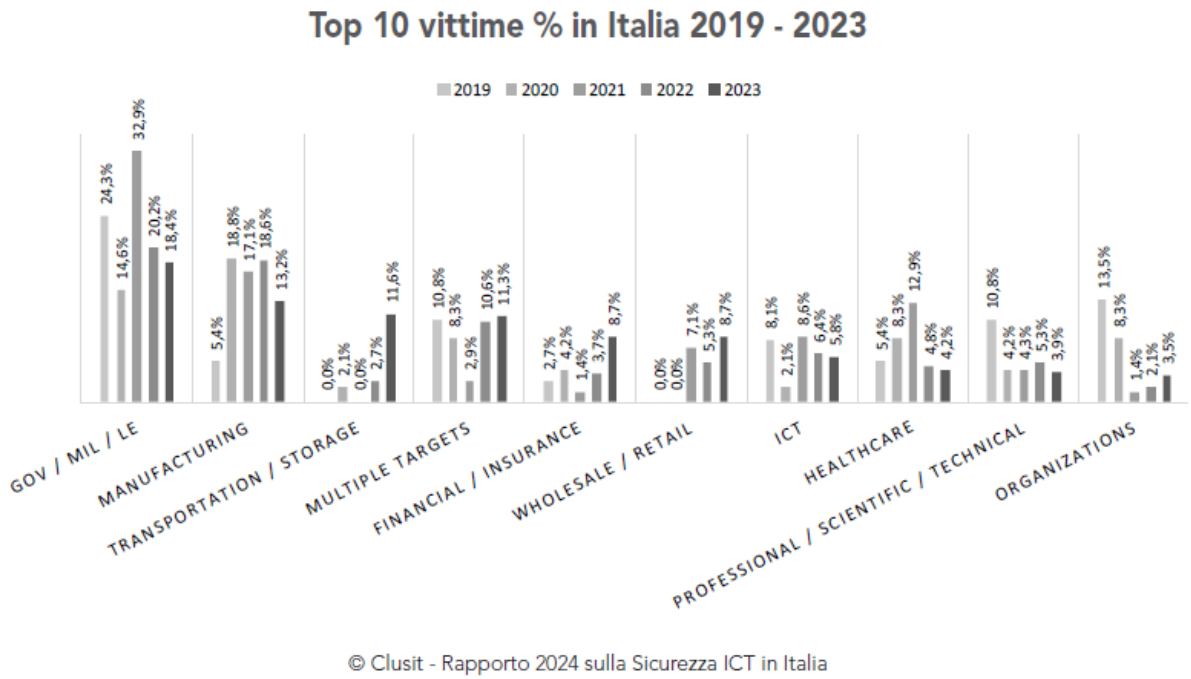

Figura 15. [25]

4.2 Il Dataset

Il dataset utilizzato per esaminare l'impatto economico della sicurezza informatica nelle imprese italiane deriva dalla rilevazione annuale condotta dall'Istituto Nazionale di Statistica (Istat) sulle tecnologie dell'informazione e della comunicazione (ICT). La raccolta dei dati è effettuata tramite questionari elettronici, con le imprese selezionate casualmente e stratificate per settore economico, ripartizione territoriale e classe di addetti. Questo metodo di campionamento stratificato garantisce che tutte le categorie di imprese siano adeguatamente rappresentate. Dal 2005 al 2010, il questionario era disponibile sia in formato cartaceo che online, ma dal 2011 in poi, l'Istat ha adottato esclusivamente il formato elettronico.

Questa indagine è rivolta alle imprese attive nei vari settori economici che contano almeno 10 dipendenti. Per questo studio specifico, sono stati selezionati i dati raccolti negli anni 2019 e 2022, permettendo così di tracciare le evoluzioni e identificare le tendenze nelle pratiche di sicurezza adottate dalle imprese nel corso del tempo.

La rilevanza di questi dati sta nella loro capacità di illustrare come l'introduzione di tecnologie avanzate e l'implementazione di misure di sicurezza informatica influenzino vari aspetti dell'operatività aziendale. Le misure di sicurezza esaminate nel dataset includono l'implementazione di sistemi avanzati di autenticazione, l'utilizzo di firewall e antivirus, nonché la definizione di politiche di sicurezza che tutelano l'integrità e la confidenzialità dei dati aziendali. Queste pratiche non solo servono a proteggere le imprese dalle minacce esterne, ma contribuiscono anche a ridurre i costi legati alla gestione dei rischi informatici e a rafforzare la fiducia di consumatori e partner commerciali.

Il dataset offre una panoramica dettagliata su diverse dimensioni dell'uso delle ICT nelle imprese, focalizzandosi in modo particolare sui dati relativi alla sicurezza informatica. Le categorie principali di dati includono:

- **Dati Base**: Si riferiscono a informazioni demografiche e strutturali sulle imprese, come il settore di attività, il numero di dipendenti e la forma giuridica.

- **Uso delle ICT**: Dettaglia il livello di adozione delle tecnologie digitali, includendo aspetti come la connettività a banda larga, l'utilizzo di cloud computing e la presenza di un sito web.
- **Sicurezza Informatica**: Descrive le misure di sicurezza adottate dalle imprese, incluse le politiche di backup dei dati, l'utilizzo di software di protezione e la gestione delle reti aziendali.
- **Impatto Economico**: Analizza gli effetti delle tecnologie ICT e delle misure di sicurezza sulle performance economiche delle imprese, evidenziando variazioni quali l'aumento del fatturato e la riduzione dei costi.

Ogni anno, le variabili rilevate vengono decise a livello comunitario, e, a parte alcuni indicatori 'core' analizzati annualmente o biennalmente, alcune sezioni del questionario vengono approfondite solo in specifici anni. Questo approccio permette di aggiornare e adattare l'indagine alle mutevoli necessità informative, garantendo che gli indicatori rilevanti siano sempre inclusi. Inoltre, alcuni indicatori diffusi in un particolare anno potrebbero non avere valori negli anni successivi a causa di questi adattamenti. Tuttavia non permette di poter analizzare determinati dati con continuità storica rilevante, per questo motivo nell'analisi sono stati individuati i parametri che meglio permettono uno studio temporale.

I dati raccolti sono poi ponderati utilizzando coefficienti di rappresentatività per ciascuna impresa nel proprio strato, assicurando che i dati raccolti riflettano accuratamente la realtà nazionale. Questa metodologia fornisce una stima precisa dell'impatto delle ICT e della sicurezza informatica sull'economia aziendale, offrendo un quadro chiaro ed esaustivo delle dinamiche in gioco nel contesto delle imprese italiane.

Le domande del questionario soggette ad analisi sono:

Q1. L'impresa applica qualcuna delle seguenti misure di sicurezza informatica sui propri sistemi ICT?

a) *Autenticazione con password forte (ad esempio lunghezza minima di 8 caratteri, uso di numeri e caratteri speciali, cambio password periodico)*
b) *Autenticazione dell'utente tramite metodi biometrici utilizzati per accedere ai sistemi ICT dell'impresa (ad esempio l'autenticazione basata su impronte digitali, voce, viso)*
c) *Tecniche di crittografia per dati, documenti o e-mail*
d) *Backup dei dati in una posizione separata dagli originali (incluso il backup nel cloud)*
e) *Controllo dell'accesso alla rete aziendale (gestione dei diritti di accesso alla rete aziendale)*
f) *VPN (Virtual Private Network estende una rete privata su una rete pubblica per consentire lo scambio sicuro di dati su rete pubblica)*
g) *Conservazione dei file di registro che consentono analisi successive agli incidenti di sicurezza informatica*
h) *Valutazione del rischio informatico, ovvero periodica valutazione della probabilità e delle conseguenze relative agli incidenti di sicurezza informatica*
i) *Test di sicurezza informatica (ad esempio esecuzione di test di penetrazione, test del sistema di allarme, revisione delle misure di sicurezza, test dei sistemi di backup)*

Q2. Quando sono stati definiti o rivisti l'ultima volta i documenti dell'impresa relativi a misure, pratiche o procedure sulla sicurezza informatica?

- *Negli ultimi 12 mesi*
- *Più di 12 e fino a 24 mesi fa*
- *Più di 24 mesi fa*

Q3. Nel corso dell'anno precedente, l'impresa ha avuto incidenti di sicurezza informatica che hanno determinato le seguenti conseguenze?

a) *Indisponibilità di servizi informatici a causa di attacchi dall'esterno (ad esempio attacchi ransomware, denial of service)*
b) *Distruzione o corruzione dei dati a causa di software dannoso o intrusione non autorizzata*
c) *Divulgazione di dati riservati a causa di intrusioni, pharming, attacchi di phishing, azioni intenzionali da parte dei propri dipendenti*

Q4. L'impresa è assicurata contro gli incidenti connessi alla sicurezza informatica?

- *Si*
- *No*

Per quando riguarda il campione di riferimento, come riportato sopra, la suddivisione è disposta per anni, 2019 e 2022, e successivamente per Codice Ateco e quindi per area commerciale in cui operano le aziende intervistate. Essendo la categorizzazione Ateco una struttura molto elaborata e fin troppo specifica ai fini dell'analisi, si è ritenuto fosse più significativo un raggruppamento ulteriore per macrosettori, risultando quindi in:

- **Attività manifatturiere (c):** comprendente tutte le attività della sottocategoria C
- **Fornitura di energia elettrica, gas, vapore e aria condizionata, acqua, reti fognarie, attività di gestione dei rifiuti e risanamento (d-e):** comprendente tutte le attività delle sottocategorie D e E e di seguito rinominata "Fornitura di servizi energetici"
- **Costruzioni (f):** comprendente tutte le attività della sottocategoria F
- **Totale servizi non finanziari (g-n, incluso 951, escluso k):** comprendente tutte le attività delle sottocategorie dalla G alla N, con esclusione della categoria K ovvero le attività relative ai servizi finanziari e assicurativi, non presi in considerazione durante l'intervista, e di seguito rinominata "Totale servizi non finanziari".

4.3 Analisi degli strumenti primari

L'obiettivo dell'analisi del dataset è esaminare la situazione delle pratiche di cybersecurity nelle aziende italiane, con particolare attenzione su come queste si proteggono da divulgazioni, corruzioni o distruzioni di dati sensibili, sia a livello interno che esterno. Per fare ciò si intende dividere gli indicatori, determinati dalle domande presenti nei questionari, analizzando in primo luogo quelli che fanno riferimento a sistemi di protezione più facilmente impiegabili e quindi fondamentali in ciascuna impresa, per passare poi a quelli più complessi ed elaborati, che determinano quindi un sistema di sicurezza più avanzato. A seguito di ciò si procede con l'analisi di procedure per la prevenzione del rischio per poi verificare infine quale sia stato il reale effetto dei precedenti indicatori studiando gli attacchi, divisi per tipologia, subiti dalle imprese negli anni in analisi.

Al termine dell'analisi l'obiettivo è comparare la variazione dei due anni presi in considerazione per verificare la variazione degli utilizzatori di assicurazioni contro incidenti di sicurezza informatica.

Primo indicatore in analisi è quello riguardante l'utilizzo di una password complessa, composta cioè da almeno 8 caratteri, al cui interno siano presenti numeri e caratteri speciali, e con l'obbligo di essere cambiata periodicamente.

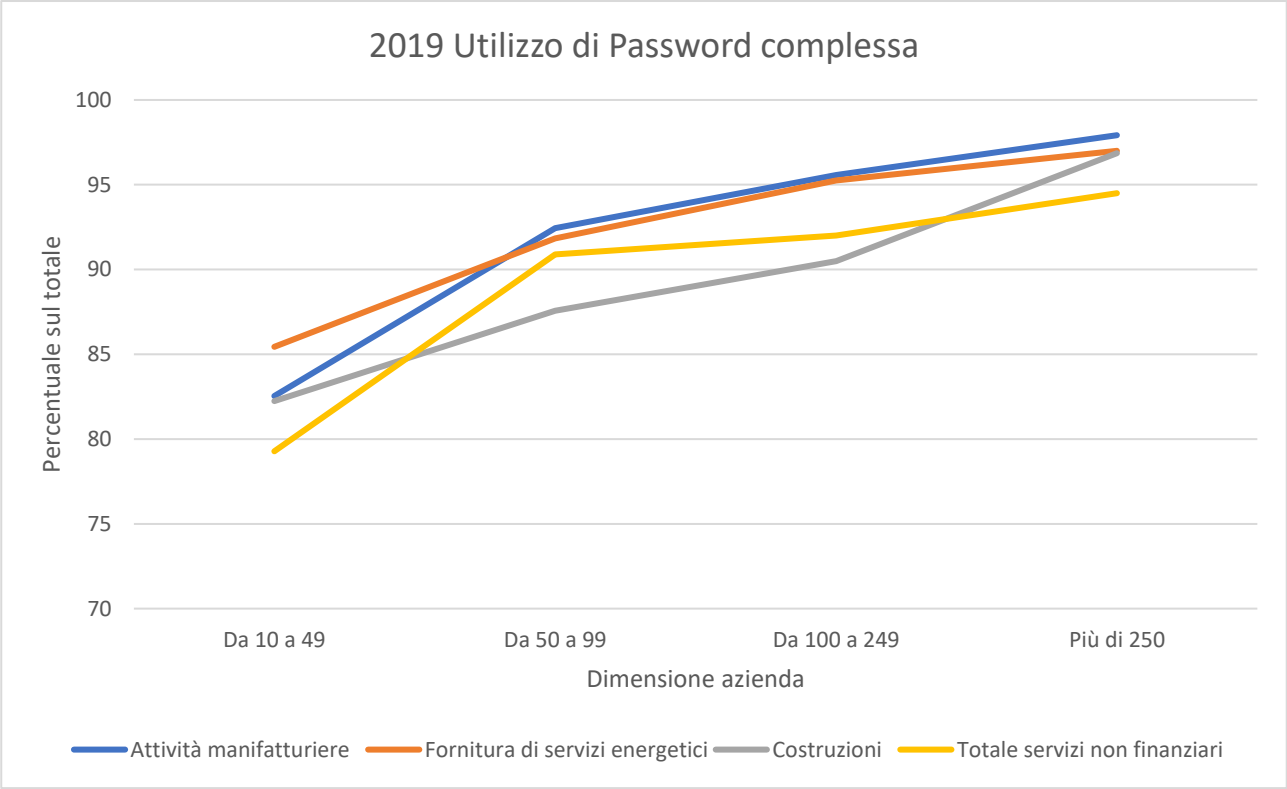

Figura 16. 2019 Percentuale di aziende che utilizzano Password complessa per settore e dimensione

L'analisi dei dati del 2019 rivela un notevole impegno da parte delle imprese nel rispettare i requisiti per una password complessa, sottolineando una crescente consapevolezza delle necessità di migliorare le pratiche di sicurezza informatica. Nonostante ciò, l'adozione di queste misure presenta una variazione significativa a seconda delle dimensioni aziendali. Ad esempio, le aziende con un organico tra 10 e 49 dipendenti mostrano una minore adesione, possibile indicatore di una ridotta percezione del rischio o di una valutazione non adeguata delle potenziali minacce informatiche.

Focalizzandosi sul macrosettore dei "Totale servizi non finanziari", si osserva che nel 2019, solo il 79% delle piccole imprese implementava password di almeno 8 caratteri con inclusione di simboli speciali. Questa percentuale aumenta progressivamente con la dimensione dell'azienda, raggiungendo il 91% nelle imprese con 50-99 dipendenti, il 92% in quelle con 100-249 dipendenti, e il 95% nelle aziende con più di 250 dipendenti. L'incremento può essere attribuito alla maggiore consapevolezza dei rischi e alla disponibilità di risorse più consistenti nelle grandi aziende, che investono attivamente nella protezione di dati sensibili e infrastrutture critiche.

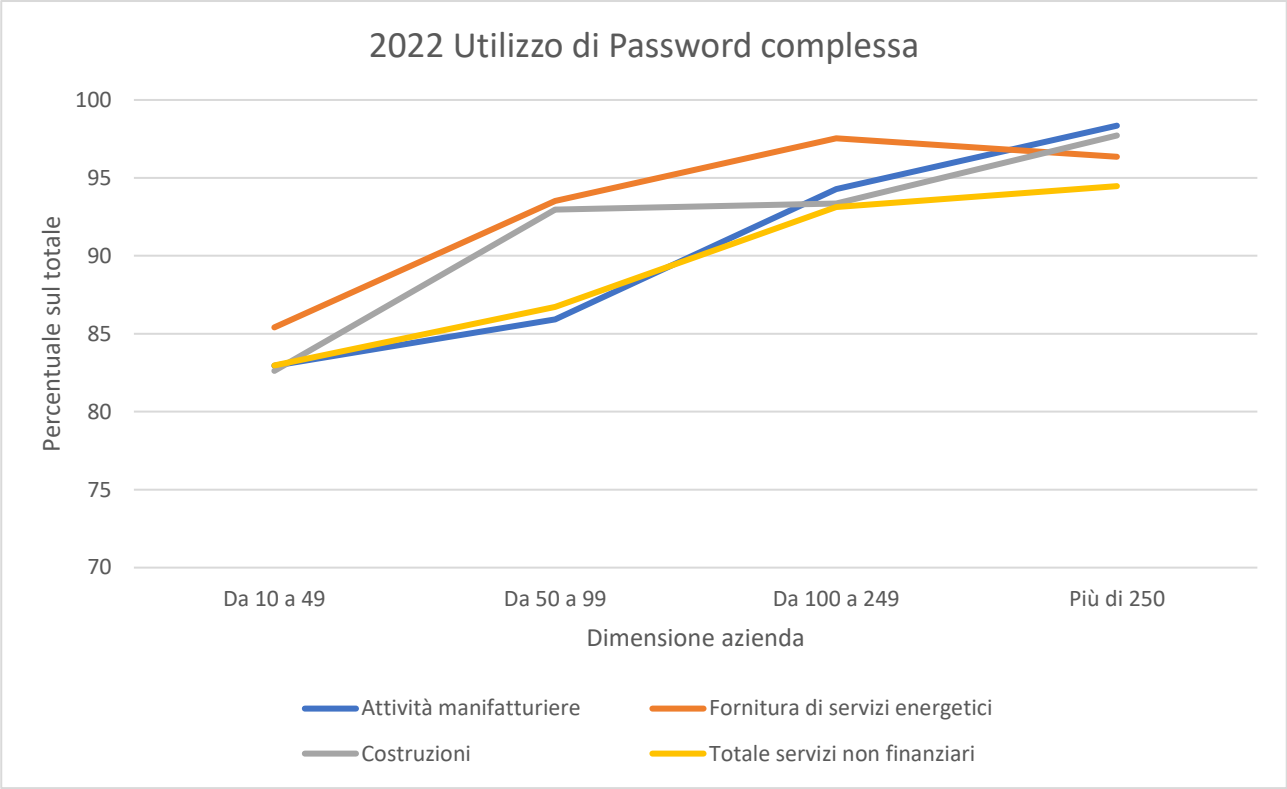

Figura 17. 2022 Percentuale di aziende che utilizzano Password complessa per settore e dimensione

Nell'analisi delle risposte ai questionari del 2022, emergono differenze significative rispetto ai dati raccolti nel 2019. Le piccole imprese del settore dei servizi non finanziari, ad esempio, hanno mostrato un notevole aumento nell'uso di password di almeno 8 caratteri, registrando un incremento di circa il 4% in tre anni. Anche nel settore delle costruzioni si osserva un miglioramento generalizzato, particolarmente evidente nelle aziende con 50-99 dipendenti, dove l'utilizzo di password complesse è salito dall'88% al 93%.

Tuttavia, alcuni settori hanno mostrato un declino nelle loro statistiche. Specificamente, le medie imprese nel settore delle attività manifatturiere hanno visto una riduzione dell'utilizzo di password sicure, passando dal 92% al 86% per quelle con 50-99 dipendenti e dal 96% al 94% per quelle con 100-250 dipendenti. Per contro, le cifre relative alle grandi aziende sono rimaste stabili, indicando un'adesione costante alle pratiche di sicurezza, sebbene una piccola frazione di queste non abbia ancora adottato tali misure e non sembri incline a farlo.

Questo scenario riflette la possibile esistenza di regolamenti più rigorosi che influenzano le grandi aziende, le quali sono spesso soggette a normative che impongono standard di sicurezza elevati. Questo aspetto è particolarmente rilevante in settori dove si gestiscono dati sensibili, richiedendo protezioni avanzate per prevenire violazioni che potrebbero avere serie conseguenze finanziarie e legali.

La variazione nell'adozione di pratiche di sicurezza come l'utilizzo di password sicure evidenzia un'urgente necessità di aumentare la sensibilizzazione sulle questioni di cybersicurezza, specialmente tra le piccole e medie imprese. Iniziative come seminari, workshop e consulenze personalizzate potrebbero rivelarsi strategie efficaci per migliorare la sicurezza delle aziende di minori dimensioni. Questi sforzi possono giocare un ruolo cruciale nell'incrementare la resilienza del tessuto economico nel suo complesso, proteggendolo meglio dalle minacce informatiche.

Terminata l’analisi dei due anni in esame relativa all’utilizzo di una password complessa, il backup dei dati emerge come un indicatore cruciale per valutare la preparazione del campione di rispondenti a fronteggiare minacce informatiche.

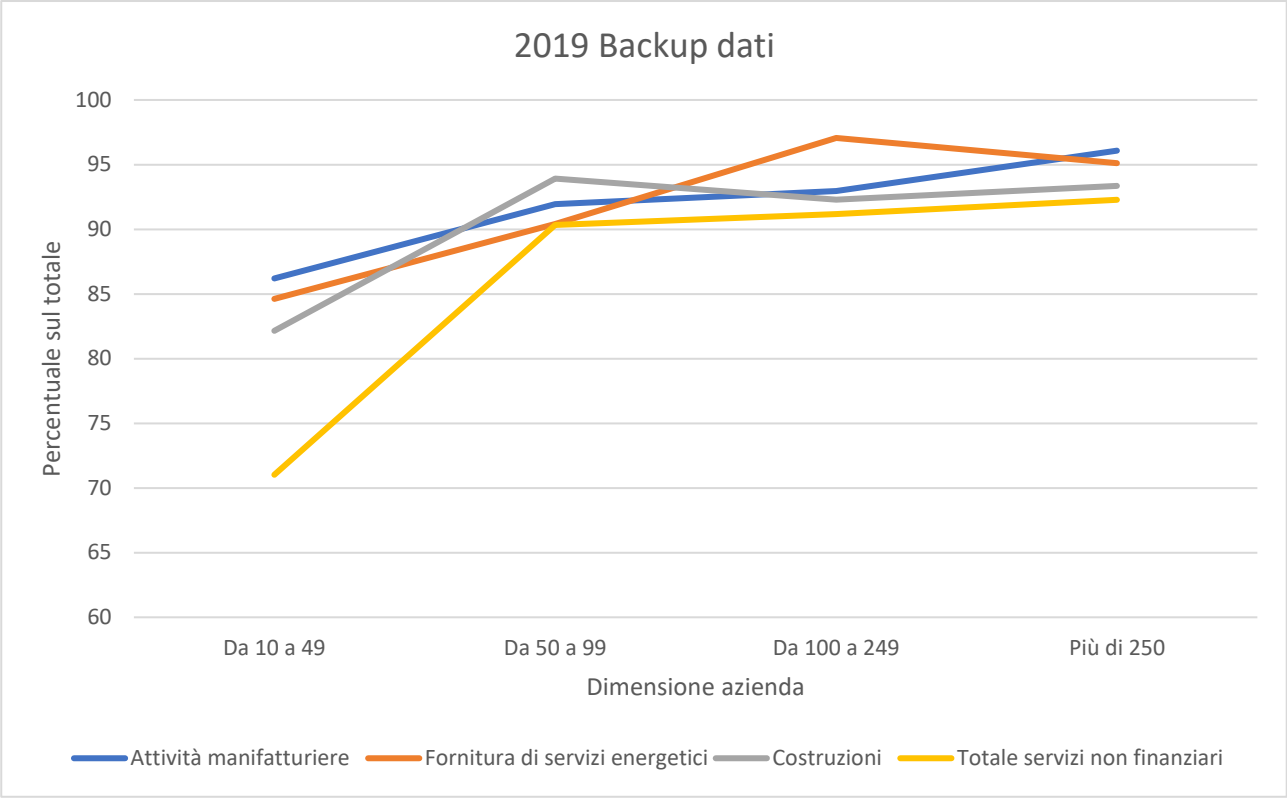

Figura 18. 2019 Percentuale di aziende che utilizza Backup di dati per dimensione e settore

Per l'anno 2019 si rivela che in tutti i settori è prassi comune predisporre il backup dei dati aziendali per prevenire la perdita di informazioni in caso di guasti ai sistemi o altri incidenti. Nei settori con aziende che contano più di 50 dipendenti, almeno il 90% delle imprese implementa regolarmente questa procedura. Il settore della fornitura di servizi energetici si distingue particolarmente, con un tasso di adozione che raggiunge il 97% tra le aziende con 100-249 dipendenti.

La situazione è meno ottimale per le piccole imprese. Nonostante l'importanza fondamentale del backup dei dati per garantire la continuità operativa in caso di problemi, la percentuale di aziende che adottano questa pratica è significativamente più bassa nelle imprese di dimensioni ridotte. Ad esempio, nel settore dei "Totale servizi non finanziari", solo il 71% delle piccole imprese ha risposto positivamente a questa pratica nel questionario. Questo tasso è sensibilmente inferiore rispetto ad altri settori, dove le percentuali si attestano all'86% per le attività manifatturiere, all'85% per la fornitura di servizi energetici e all'82% per il settore delle costruzioni. In generale, questi settori superano le piccole imprese di almeno 11 punti percentuali, evidenziando una disparità significativa nell'adozione di misure di sicurezza essenziali tra le aziende di diverse dimensioni.

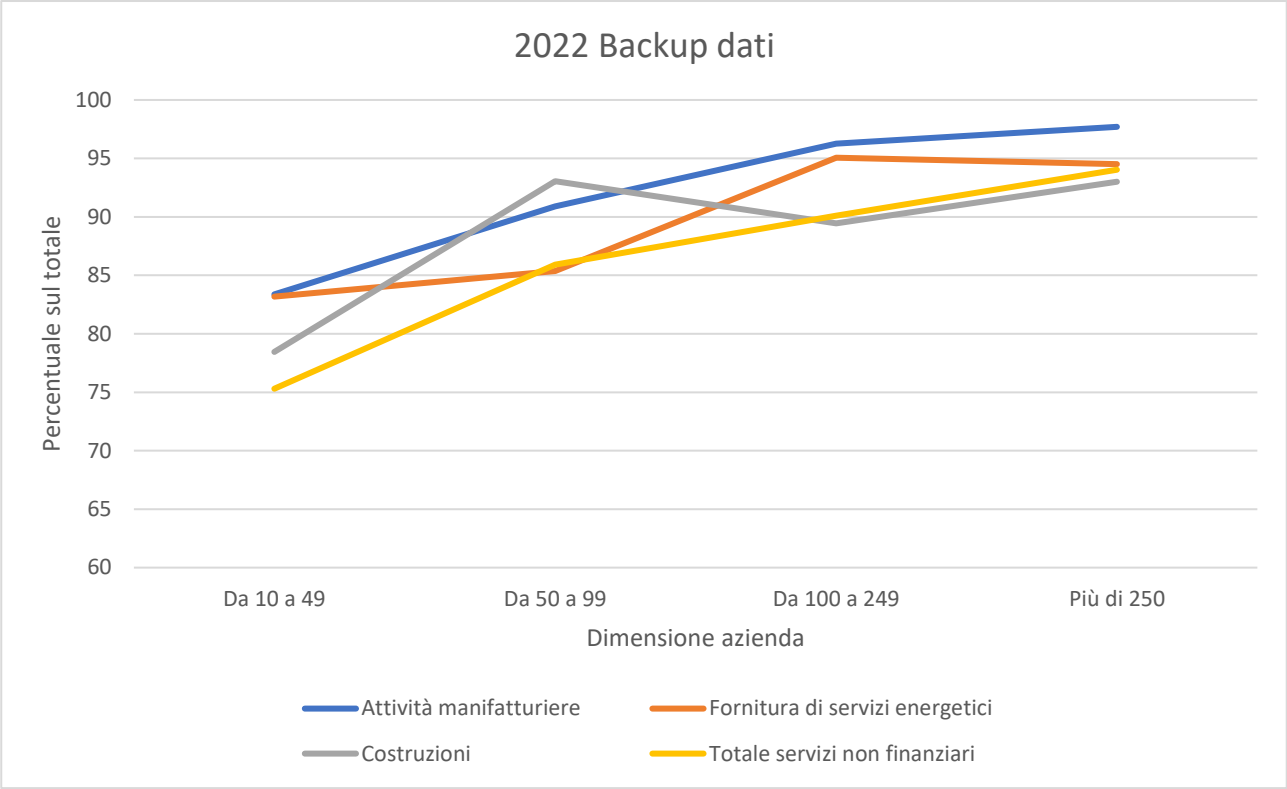

Figura 19. 2022 Percentuale di aziende che utilizza Backup di dati per dimensione e settore

Confrontando i dati del 2019 con quelli del 2022 è immediata la differenza tra le code a sinistra riferite alle piccole imprese con meno di 50 dipendenti. Si evidenzia una variazione positiva per i servizi non finanziari, di molto distaccati nel precedente anno di analisi con un incremento rilevante di circa il 4%, tuttavia gli altri valori non soddisfano come il precedente, per tutti gli altri settori, sempre nel contesto delle piccole imprese, si presenta una diminuzione di qualche punto percentuale. È un fenomeno che si verifica in modo diffuso, infatti se nel grafico precedente si può percepisce un andamento piatto tra le medie e le grandi imprese, il 2022 si presenta molto più simile ad una curva concava, simbolo che le medie imprese non hanno investito in sistemi di backup come negli anni precedenti.

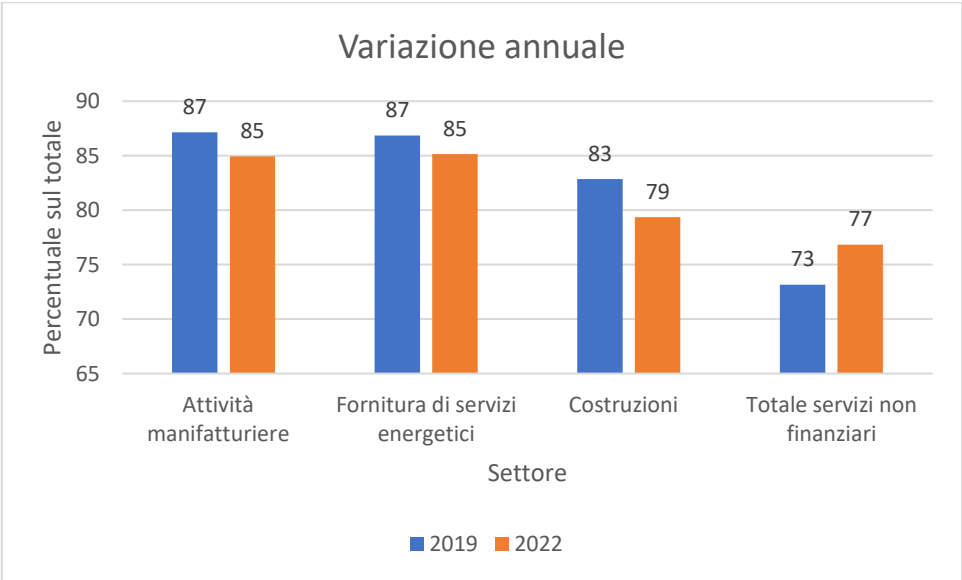

Figura 20. Variazione della percentuale di utilizzatori di backup di dati per settore 2019vs2022

È un dato preoccupante, infatti, così come per le password complesse, ci si aspetterebbe un andamento crescente nel tempo, fenomeno dovuto all'aggiornarsi dei sistemi tecnologici e della consapevolezza comune riguardo al digitale. Una tendenza inversa, seppur minima, preannuncia una diminuzione di investimenti in sistemi di salvataggio dati e di procedure regolari per fare uso di dati salvati in caso di malfunzionamento dei sistemi aziendali. Un problema ai server, senza un adeguato backup dei dati, può infatti compromettere la continuità operativa del business, e si rischia di perdere definitivamente una porzione significativa del lavoro fatto.

Si procede quindi all'analisi dell'ultimo dei tre indicatori fondamentali per una cybersicurezza di base all'interno delle organizzazioni, quello relativo alla protezione per l'accesso alla rete aziendale. Questi indicatori sono considerati essenziali perché, in linea di principio, dovrebbero rappresentare pratiche standard per qualsiasi tipo di dispositivo o apparecchio elettronico esposto a interventi intrusivi o non autorizzati, che costituiscono proprio la ragione per cui è stata sviluppata la cybersecurity.

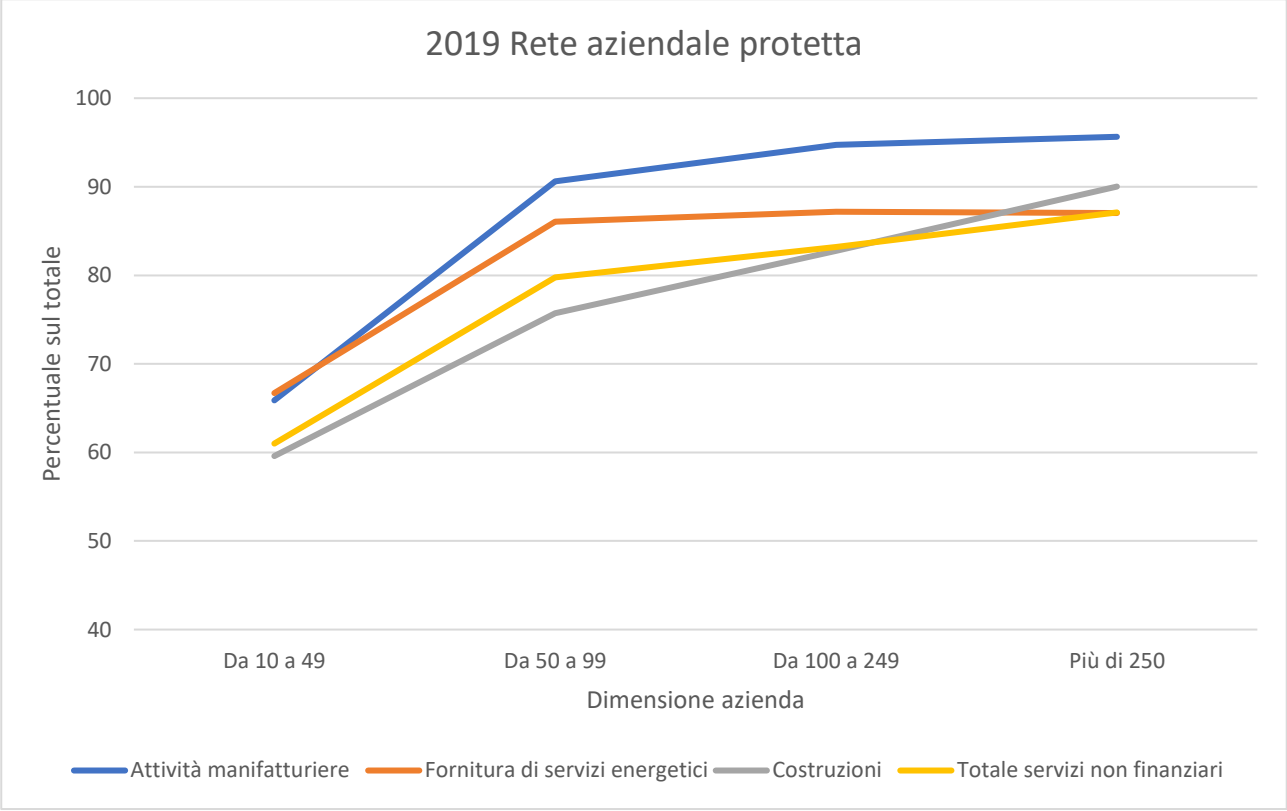

Figura 21. 2019 Percentuale di aziende che utilizza una Rete aziendale protetta per dimensione e settore

Per questo motivo, si analizzano i risultati relativi alla presenza di controlli per l'accesso alla rete aziendale, in particolare attraverso la richiesta di diritti d'accesso. Nel 2019, i dati di questo indicatore mostrano una tendenza simile a quella osservata per l'utilizzo di password complesse, con un trend crescente all'aumentare delle dimensioni aziendali, mantenendosi comunque su percentuali elevate. Le aziende nel settore delle "Attività manifatturiere" sono quelle che adottano più efficacemente questa pratica: circa il 96% delle grandi imprese, con più di 250 dipendenti, implementa questi controlli, con un leggero calo al 95% nelle medie imprese (100-249 dipendenti), al 91% nelle imprese di dimensioni intermedie (50-99 dipendenti) e una riduzione significativa al 66% nelle piccole imprese (10-49 dipendenti).

Questo notevole calo, corrispondente a 25 punti percentuali, nell'adozione di controlli di accesso nelle piccole imprese può essere spiegato considerando le peculiarità del contesto aziendale. In Italia, le piccole imprese sono spesso a conduzione familiare, dove i dipendenti tendono ad avere rapporti diretti e di fiducia

con i proprietari o i responsabili della sicurezza. Questa familiarità rende meno impellente l'esigenza di controlli severi sull'accesso alla rete, poiché si presume un ambiente di fiducia.

Tuttavia, questa fiducia può a volte tradursi in una vulnerabilità maggiore agli attacchi informatici, in quanto la sicurezza informatica non viene percepita come prioritaria. Man mano che la dimensione aziendale cresce, si attenuano i rapporti personali e aumenta la necessità di implementare politiche di sicurezza più rigide e sistematiche per proteggere i dati aziendali da possibili intrusioni esterne. Questo cambiamento è cruciale per mitigare i rischi legati alla perdita di dati sensibili.

Inoltre, nelle aziende più grandi, la complessità dei sistemi informativi richiede una gestione della sicurezza più sofisticata e multi-livello, che va oltre il semplice controllo degli accessi, includendo monitoraggio continuo, autenticazione multifattoriale e formazione periodica dei dipendenti sulle migliori pratiche di sicurezza informatica.

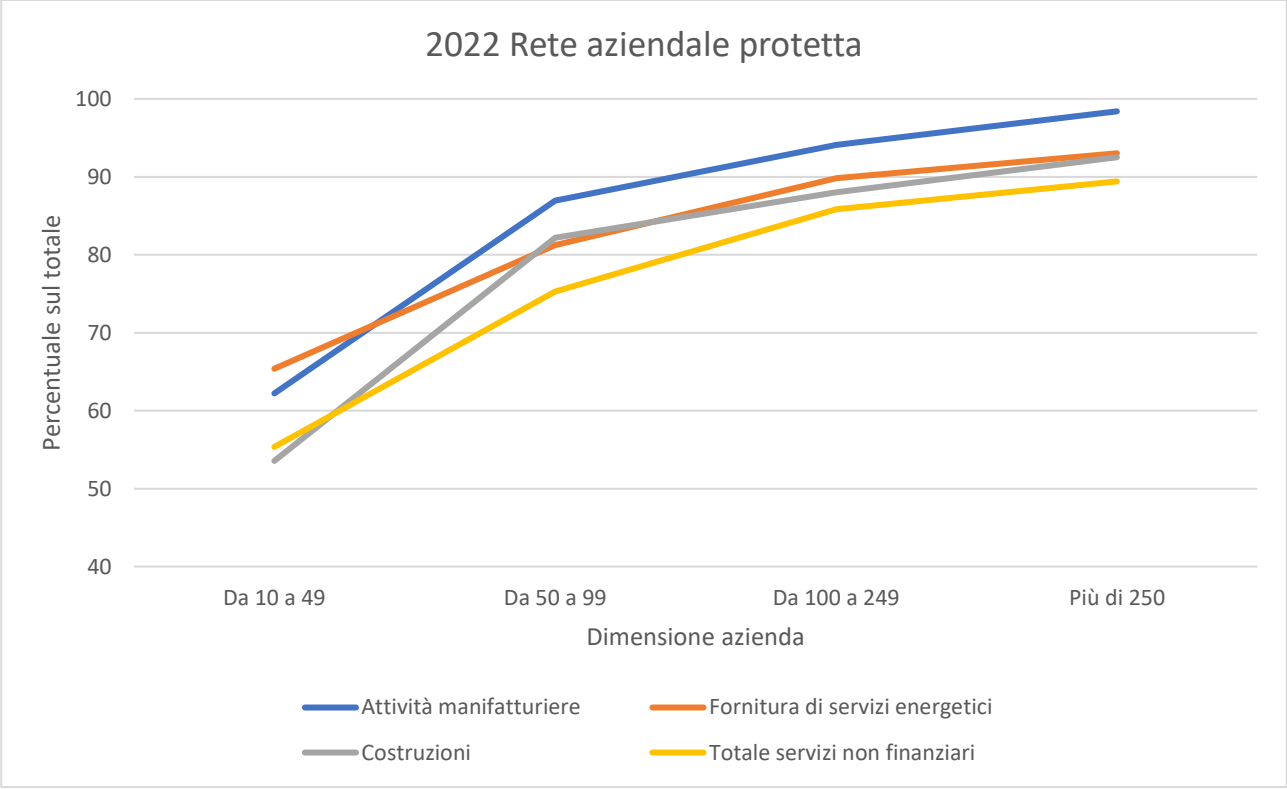

Figura 22. 2022 Percentuale di aziende che utilizza una Rete aziendale protetta per dimensione e settore

Nel 2019, le piccole imprese mostravano un'adozione delle misure di sicurezza compresa tra il 60% e il 70%, tuttavia, i dati raccolti nel 2022 indicano una riduzione significativa di tali pratiche, soprattutto nel settore dei servizi non finanziari, dove si evidenzia un calo marcato nella sicurezza informatica. Questa tendenza alla diminuzione si manifesta non solo nelle piccole imprese ma, a differenza di quanto osservato in precedenza, anche nelle medie e grandi imprese. Analizzando più nel dettaglio, si nota che nel grafico precedente era possibile osservare un appiattimento della curva per le medie e grandi imprese, indicativo di una stabilizzazione nell'adozione di pratiche di sicurezza. Contrariamente, nel 2022, alla riduzione della dimensione aziendale, si registra una diminuzione generalizzata del numero di aziende che implementano controlli di accesso efficaci alle loro reti aziendali. Tale calo interessa trasversalmente tutti i livelli aziendali, evidenziando una possibile lacuna nell'aggiornamento e nel mantenimento delle infrastrutture di sicurezza o forse una minore percezione del rischio.

Nonostante il contesto generale di riduzione, le "attività manifatturiere" si distinguono per una maggiore resilienza nelle pratiche di sicurezza. In questo settore, la continuità nell'implementazione del controllo d'accesso alla rete aziendale da parte delle imprese con almeno 50 dipendenti rimane superiore alla media, con un picco di utilizzo che raggiunge il 98% nelle grandi imprese con più di 250 dipendenti. Questo dato risalta non solo per l'elevata percentuale di adozione ma anche perché rappresenta quasi la totalità delle imprese considerate in questa fascia di dimensione, dimostrando un impegno costante nel proteggere le risorse informatiche aziendali in un settore critico come quello manifatturiero.

Una riflessione approfondita su questo indicatore mette in luce una marcata differenza tra le piccole e le grandi imprese nel campo della sicurezza informatica. Mentre per altri elementi analizzati le discrepanze erano già notevoli, per questo specifico indicatore, esse risultano ancora più pronunciate e crescenti nel tempo. Inizialmente, nel 2019, il divario tra piccole e grandi aziende era mediamente del 25%, un valore già significativo che riflette le diverse capacità e risorse disponibili in termini di cybersecurity. Questo gap si è ulteriormente ampliato nel 2022, raggiungendo circa il 30%.

Le ragioni dietro questa crescente divergenza sono varie e complesse. Le grandi imprese, gestendo strutture più complesse e avendo maggiori risorse, tendono naturalmente a dedicare più attenzione e investimenti alla sicurezza informatica. Questa maggiore enfasi sulla sicurezza è cruciale, data l'elevata esposizione al rischio di attacchi informatici che può derivare da una gestione inadeguata. D'altra parte, le piccole imprese, specialmente quelle che interagiscono direttamente con il pubblico, possono affrontare sfide diverse. Molti piccoli esercizi commerciali optano per rendere le proprie reti più accessibili al pubblico, cercando di attrarre una clientela più giovane e di aumentare la propria competitività in mercati affollati. Questa scelta, sebbene possa avere benefici immediati in termini di attrattiva commerciale, può comportare rischi significativi per la sicurezza informatica. L'accessibilità di rete aumentata, senza le dovute protezioni, può esporre l'impresa a vulnerabilità e attacchi.

4.4 Analisi degli strumenti secondari

Dopo aver analizzato i requisiti base per una sicurezza informatica efficiente, si procede a prendere in considerazione le risposte relative alle domande che contemplano l’utilizzo di sistemi di cybersicurezza più elaborati, o quantomeno che possono non definirsi una pratica comune nella normalità aziendale.

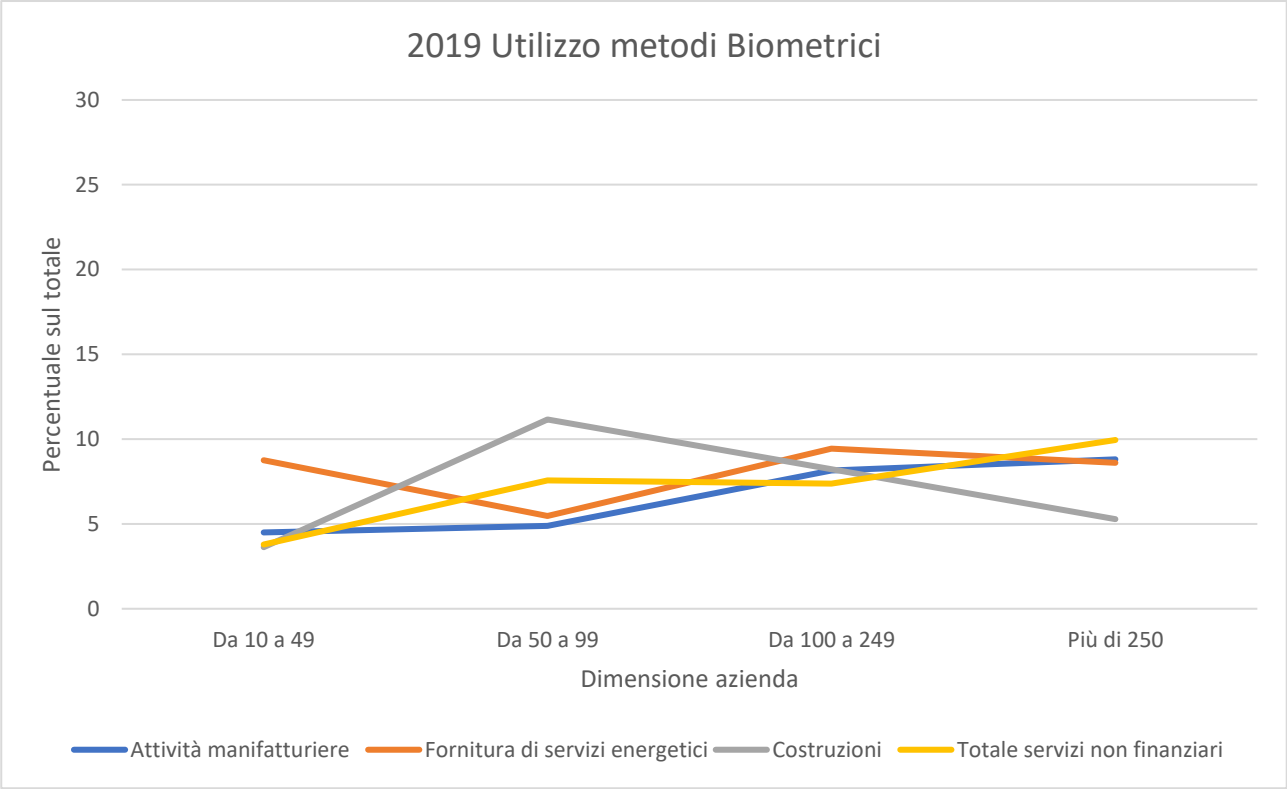

Figura 23. 2019 Percentuale di aziende che utilizza riconoscimenti biometrici per dimensione e settore

Uno dei principali indicatori di sicurezza esaminati riguarda l'utilizzo dei metodi di riconoscimento biometrico per l'autenticazione degli utenti, quali impronte digitali, riconoscimento facciale o vocale. È cruciale evidenziare che tali tecnologie dipendono spesso dai dispositivi in uso presso i dipendenti, come computer, smartphone o tablet, che incorporano questi sistemi avanzati. Nonostante la loro complessità e l'efficacia nella protezione contro intrusioni esterne, nonché la capacità di tracciare specificamente gli accessi, è sorprendente notare come nel 2019 meno del 15% delle imprese italiane, indipendentemente dal settore o dalle dimensioni, abbiano adottato diffusamente queste tecnologie.

In particolare, nel settore delle costruzioni, tra le imprese con 10-49 dipendenti, solo il 3,63% fa uso di questi metodi biometrici. La percentuale sale all'11% per le aziende con 50-99 dipendenti, ma poi diminuisce nuovamente, attestandosi all'8,23% per quelle con 100-249 dipendenti e al 5,29% per quelle con più di 250 dipendenti. Questa variazione non segue il trend di aumento generalmente osservato con la crescita delle dimensioni aziendali negli altri indicatori di sicurezza, suggerendo che la scarsa adozione non è attribuibile unicamente alla complessità delle strutture aziendali o alla completezza delle procedure. Piuttosto, appare come un problema ampiamente diffuso che attraversa tutti i livelli e dimensioni aziendali, evidenziando una significativa opportunità di miglioramento nella protezione dei dati aziendali attraverso l'implementazione di tecnologie biometriche.

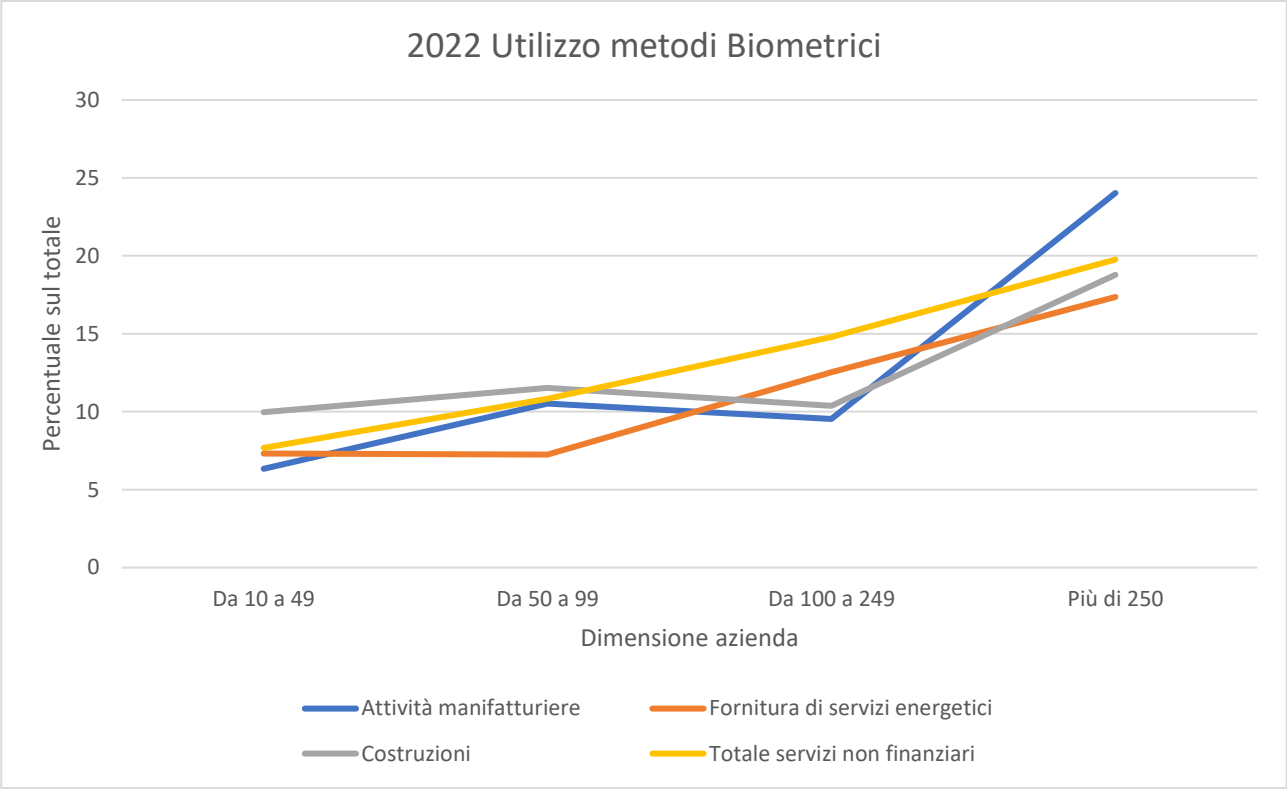

Figura 24. 2022 Percentuale di aziende che utilizza riconoscimenti biometrici per dimensione e settore

Nel confronto dei risultati tra il 2019 e il 2022, è evidente un'evoluzione significativa nel corso dei tre anni intercorsi tra le due rilevazioni. Le piccole imprese, in particolare, mostrano un incremento notevole nell'adozione delle tecnologie, a partire da percentuali basse di utilizzo. Il settore delle costruzioni, che nel 2019 registrava il tasso più basso di adozione, ha visto più che raddoppiare la percentuale di imprese che utilizzano sistemi di riconoscimento biometrico, raggiungendo quasi il 10%. Questo incremento è notevole, considerando il punto di partenza relativamente modesto e indica una crescente consapevolezza delle necessità di sicurezza avanzata.

Tuttavia, è tra le grandi imprese che si osserva il cambiamento più marcato. Queste aziende hanno implementato in modo massiccio i nuovi sistemi di sicurezza biometrica. A differenza del 2019, quando l'incremento nell'utilizzo di tali sistemi era quasi uniforme tra le varie dimensioni aziendali, nel 2022 i dati mostrano una configurazione più dinamica. La distribuzione dei dati ora presenta una leggera concavità verso l'alto, indicando che l'aumento dell'adozione di sistemi di sicurezza biometrica è più pronunciato nelle aziende più grandi rispetto a quelle più piccole.

Questo cambiamento di tendenza suggerisce una divergenza crescente nelle capacità di implementazione delle tecnologie di sicurezza avanzate tra aziende di diverse dimensioni. Le grandi imprese, con più risorse e forse sotto la pressione di requisiti normativi più stringenti, sembrano essere in grado di adottare tecnologie più avanzate e complesse a un ritmo accelerato. Questo si traduce in un miglioramento della sicurezza complessiva, ma anche in una crescente disparità tra grandi e piccole imprese in termini di capacità di proteggere i propri dati e infrastrutture.

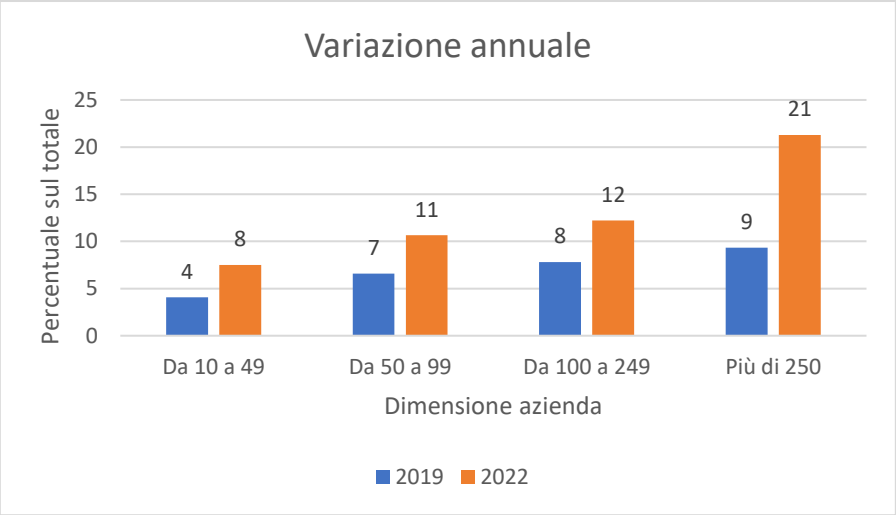

Figura 25. Variazione della percentuale di utilizzatori di riconoscimenti biometrici per dimensione 2019vs2022

Nella Figura 25, che presenta la variazione annuale dell'uso di sistemi di riconoscimento biometrico per dimensione aziendale, senza considerare la divisione per tipologia di settore, si può osservare chiaramente che l'adozione di queste tecnologie sta diventando sempre più diffusa come pratica di sicurezza attraverso tutte le tipologie di imprese. Nello specifico, si evidenzia un incremento medio del 4% per tutte le dimensioni aziendali con meno di 250 dipendenti, e di un importante 12% di incremento per le grandi imprese con più di 250 dipendenti. Questi valori mostrano come più l'impresa diventi grande e più diventi importante investire in nuovi sistemi di cybersecurity.

Il rafforzamento della sicurezza attraverso tecnologie biometriche, riconosciute per la loro capacità di offrire una verifica dell'identità più sicura e meno incline a frodi o errori rispetto ai metodi tradizionali, rispecchia un cambiamento importante nel modo in cui le imprese di varie dimensioni percepiscono e rispondono alle minacce alla sicurezza. L'aumento dell'uso di tali tecnologie riflette anche una maggiore consapevolezza delle potenziali minacce informatiche e un impegno crescente verso la protezione dei dati sensibili e delle risorse aziendali.

Questo trend, inoltre, solleva questioni rilevanti riguardo alla necessità di aggiornamenti continui nella formazione e nelle competenze tecnologiche per i dipendenti di tutte le aziende, per garantire che l'implementazione di queste tecnologie avanzate sia efficace e che le operazioni aziendali rimangano sicure e inattaccabili da minacce esterne. Inoltre, suggerisce la necessità per le aziende di continuare a investire in soluzioni di sicurezza che possano adattarsi rapidamente all'evoluzione del panorama delle minacce, garantendo così un ambiente sicuro e resiliente.

Il secondo indicatore analizzato riguardante gli strumenti digitali utilizzati dalle aziende per la protezione dei dati è la VPN, che offre diverse forme di sicurezza dei dati, tra cui confidenzialità, integrità, autenticazione e protezione da attacchi esterni. Introdotte relativamente di recente nel campo della sicurezza informatica, le VPN sono diventate essenziali per le aziende che necessitano di salvaguardare i dispositivi dei dipendenti quando si collegano a reti esterne.

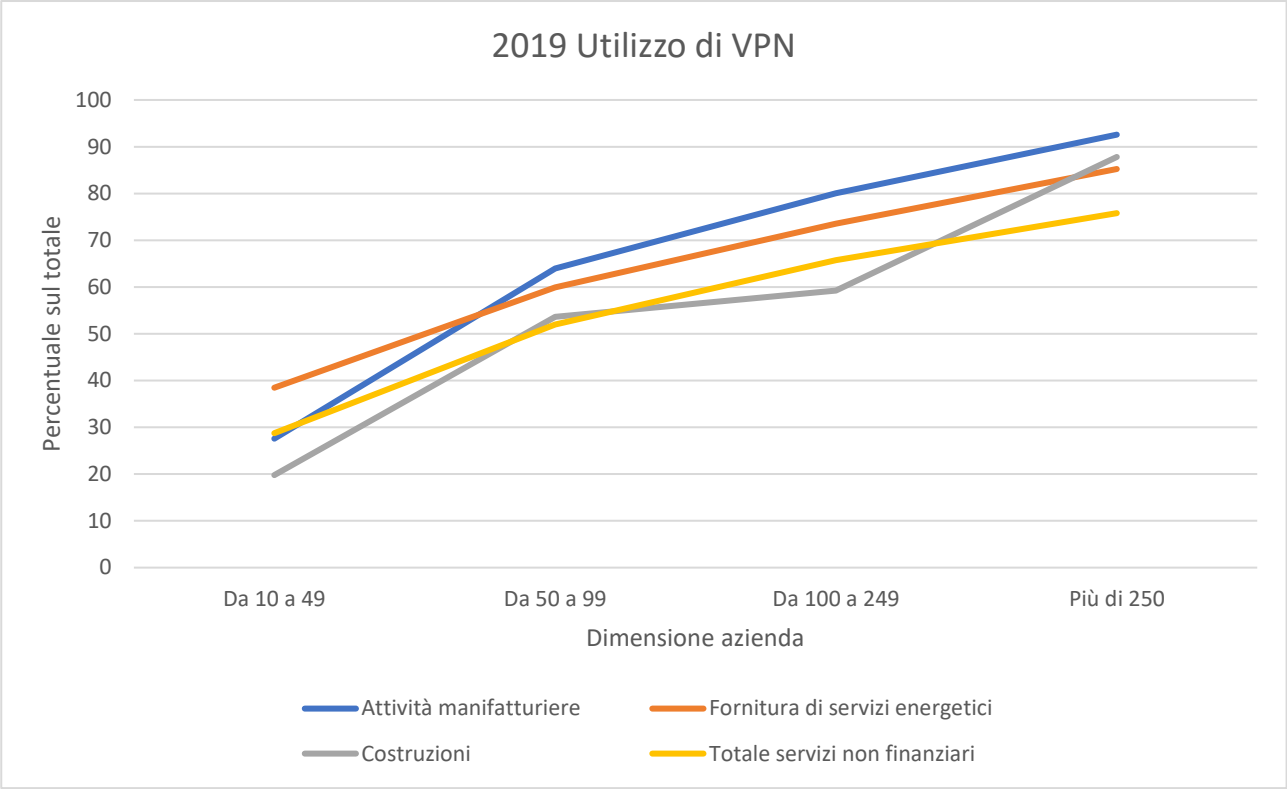

Figura 26. 2019 Percentuale di aziende che utilizza VPN per dimensione e settore

Il rischio di connettersi a una rete pubblica o non sicura è elevato e poiché i dati trasmessi possono essere intercettati questa problematica è diventata particolarmente rilevante con la diffusione dello smart working, pratica che permette ai dipendenti di lavorare da remoto, necessitando quindi di connessioni sicure non solo alla rete domestica ma anche a reti pubbliche per garantire flessibilità e continuità lavorativa.

In termini di numeri, nel 2019 l'utilizzo delle VPN nelle aziende manifatturiere con 10-49 dipendenti è stato rilevato al 28%, ma con un notevolmente aumento nelle aziende con 50-99 dipendenti raggiungendo quasi il 64%. Questa percentuale cresce ulteriormente al 80% per le aziende con 100-249 dipendenti e arriva al 93% nelle organizzazioni con più di 250 collaboratori, evidenziando come l'adozione di questa tecnologia sia fortemente influenzata dalle dimensioni aziendali e dalla necessità di supportare modelli di lavoro più flessibili e sicuri. L'adozione delle VPN mostra infatti un chiaro trend di crescita in relazione alla dimensione dell'azienda. L'implementazione su larga scala richiede competenze specifiche e un investimento significativo, fattori che possono essere più gestibili per le aziende più grandi. Queste ultime, spesso con un elevato numero di dipendenti, tendono a favorire modalità di lavoro ibrido, che combinano presenza in ufficio e lavoro da remoto, una pratica meno comune nelle piccole realtà dove il contatto diretto tra i dipendenti è ancora cruciale.

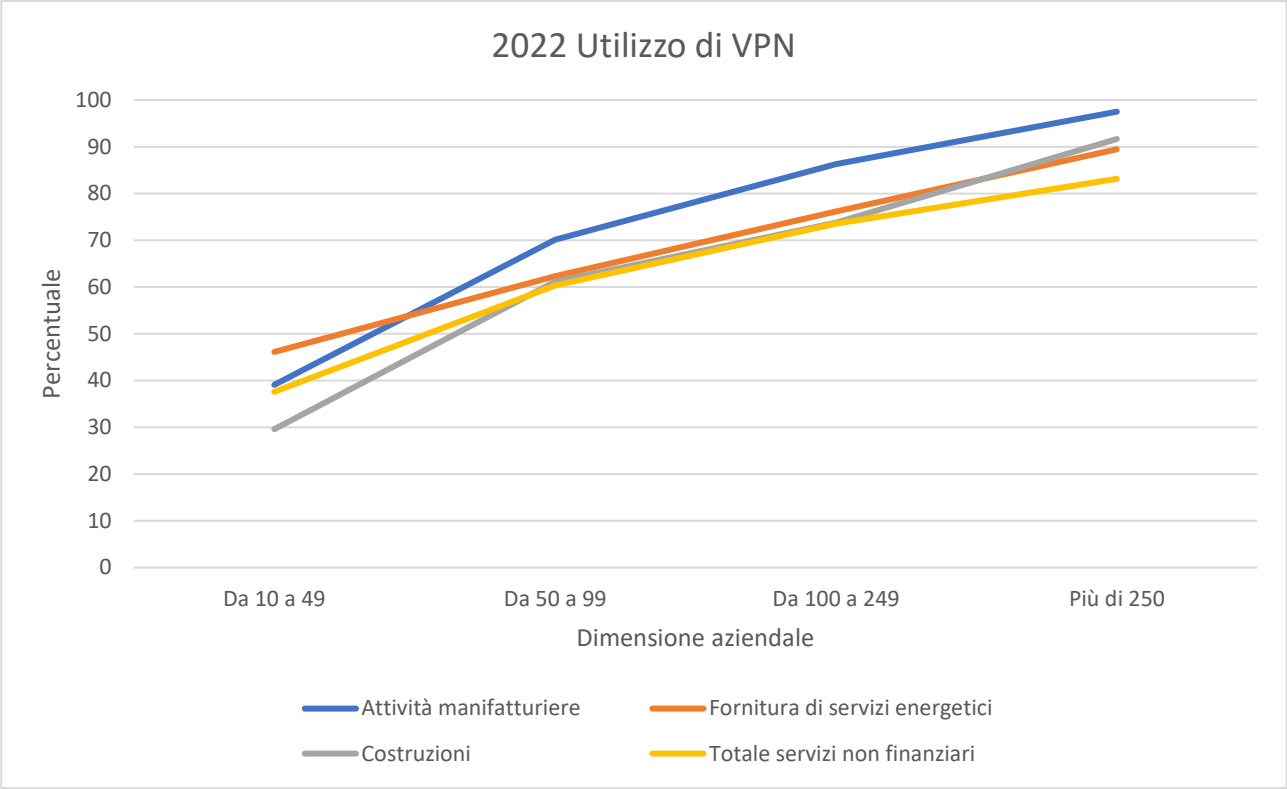

Figura 27. 2022 Percentuale di aziende che utilizza VPN per dimensione e settore

In riferimento al 2022, le attività manifatturiere si confermano come le maggiori utilizzatrici di questo servizio, in particolar modo per quanto riguarda le grandi imprese, quasi la totalità infatti fa uso di reti provate virtuali, con un tasso di utilizzo del 97,5%. Altra differenza sostanziale si osserva per le imprese di costruzioni di medie dimensioni con dipendenti compresi tra i 100 ed i 249, per le quali si presenta un aumento di circa 15 punti percentuali tra i due anni di analisi. In generale le curve generate dalle risposte al questionario riflettono molto l'andamento di quelle del 2019, con la differenza nella percentuale media di utilizzatori.

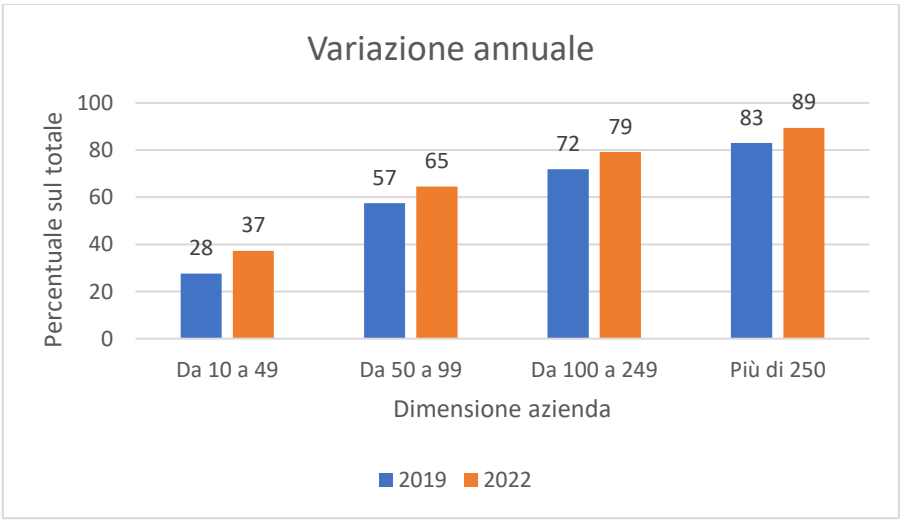

Figura 28. Variazione della percentuale di utilizzatori di VPN per dimensione 2019vs2022

Il settore delle VPN sta vivendo una fase di notevole crescita nel contesto aziendale italiano, segnando un aumento trasversale che interessa aziende di tutte le dimensioni. Questa tendenza è particolarmente evidente nelle piccole imprese, che hanno registrato un incremento impressionante di 9 punti percentuali

nell'adozione di queste tecnologie. Questo aumento sostanziale riflette l'importanza crescente che le VPN stanno acquisendo nel panorama delle infrastrutture IT, specialmente per le aziende che cercano soluzioni sicure per navigare e operare online. L'incremento nell'uso delle reti private virtuali testimonia l'efficacia di questa tecnologia nel garantire sicurezza e privacy nelle comunicazioni aziendali. Le VPN offrono una serie di benefici chiave, come la crittografia end-to-end dei dati trasferiti, l'occultamento dell'indirizzo IP per proteggere l'identità degli utenti e la possibilità di bypassare le restrizioni geografiche, che sono particolarmente vantaggiose per le aziende che operano in mercati internazionali o che necessitano di accedere a risorse localizzate in diverse regioni. Questi fattori fanno delle VPN uno strumento indispensabile per le imprese che desiderano mantenere elevati standard di sicurezza, soprattutto in un'era in cui le minacce informatiche sono in costante evoluzione e dove la protezione dei dati aziendali diventa una priorità assoluta.

L'ultimo degli indicatori analizzati nel contesto del supporto alla cybersicurezza aziendale riguarda la percentuale di rispondenti che adottano la crittografia per proteggere dati, documenti e, in particolare, email. Questo indicatore è cruciale per comprendere come le imprese gestiscono la sicurezza dei dati sensibili, che spesso rischiano di essere intercettati da terzi o condivisi incautamente. La posta elettronica, frequentemente utilizzata per comunicazioni interne ed esterne, è uno strumento di semplice impiego anche per utenti meno esperti. Tuttavia, senza misure adeguate, non garantisce la protezione necessaria per la trasmissione di dati sensibili.

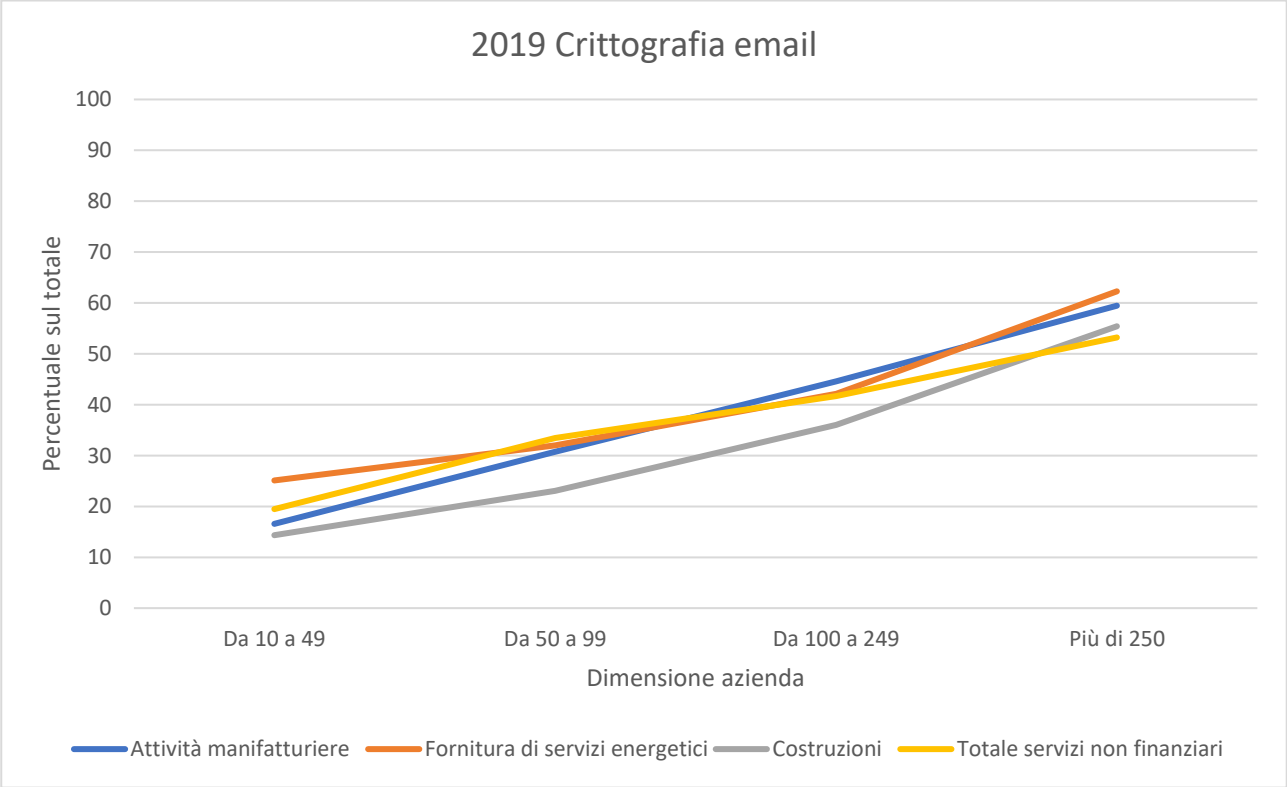

Figura 29. 2019 Percentuale di aziende che utilizza crittografia delle mail per dimensione e settore

Implementare la crittografia per documenti ed email è quindi essenziale per prevenire la divulgazione non autorizzata delle informazioni. Questo metodo implica l'utilizzo di una password che deve essere inserita per accedere ai contenuti delle email o dei documenti, bloccando così l'accesso a soggetti non autorizzati. Se correttamente implementata, la crittografia si rivela uno strumento efficace per elevare il livello di sicurezza delle comunicazioni aziendali.

Dall'analisi delle risposte al questionario Istat 2019, emerge che le piccole imprese sono le meno propense all'uso della crittografia, soprattutto nel settore delle costruzioni, dove solo il 14,34% adotta questa pratica. Anche nelle imprese di dimensioni leggermente superiori, i numeri rimangono preoccupanti: solo il 23% delle aziende con 50-99 dipendenti cripta i propri documenti. Tuttavia, si nota un miglioramento nelle aziende più grandi, con una percentuale che cresce al 36% per quelle con 100-249 dipendenti e al 55% per quelle con più di 250 dipendenti, dimostrando una correlazione positiva tra la dimensione dell'azienda e l'adozione di pratiche di sicurezza avanzate come la crittografia.

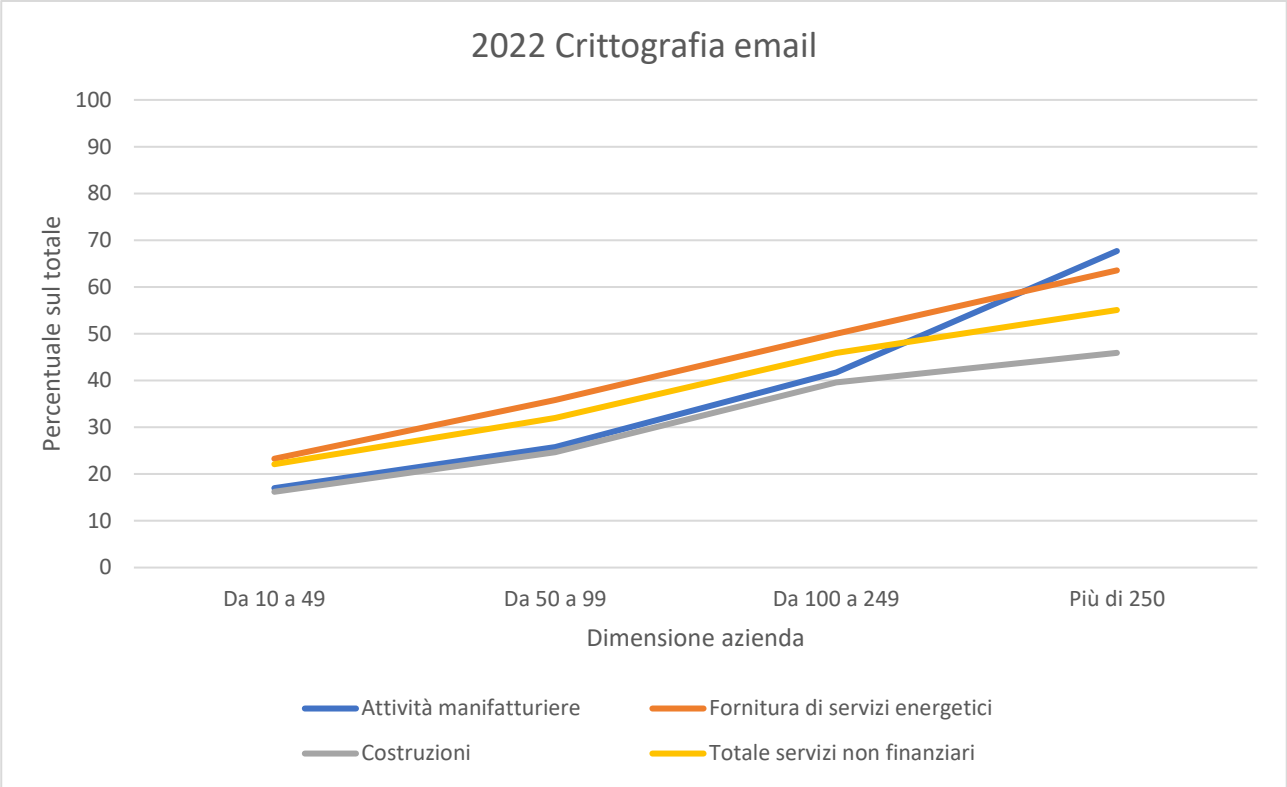

Figura 30. 2022 Percentuale di aziende che utilizza crittografia delle mail per dimensione e settore

Informazioni similari sono raccolte con il questionario relativo all'anno 2022, non si evidenzia un cambiamento significativo a livello di settori e di dimensioni aziendali. Il settore delle costruzioni si conferma il peggior adottatore di questa pratica, raggiungendo un livello di picco nelle grandi imprese con almeno 250 dipendenti per il quale si registra un tasso di utilizzo di crittografia delle mail pari al 46%, minore di quello registrato nel 2019.

4.5 Analisi sulla prevenzione del rischio

Dopo aver analizzato lo stato dei principali strumenti in merito alla cybersecurity all'interno di una azienda, si procede a studiare l'andamento di quelle che sono le misure attuate per prevenire e mitigare i rischi di un possibile incidente tecnologico. Non è infatti sufficiente implementare complessi sistemi di difesa da azioni esterne, ma è necessario effettuare verifiche costanti per monitorare qualora queste misure si rendano efficaci e aggiornare costantemente i propri sistemi per rimanere al passo con le innovazioni in ambito di sicurezza informatica. Per questo motivo in questo paragrafo vengono analizzate le risposte fornite dal campione di imprese a riguardo delle domande relative all'implementazione di una procedura di analisi del rischio informatico e di test di sicurezza per verificare l'efficacia delle misure di protezione.

Il primo indicatore analizzato riguarda l'adozione di un processo di valutazione del rischio informatico. Tale valutazione è definita come una revisione periodica che quantifica la probabilità di occorrenza di un incidente informatico e valuta l'impatto potenziale di tali incidenti sull'operatività aziendale. L'analisi del

rischio è cruciale non solo nel contesto della cybersecurity, ma in tutti i progetti aziendali che comportano una serie di attività operative. È essenziale, infatti, anticipare e prepararsi per le situazioni che potrebbero arrecare danni, sia economici sia operativi, attraverso l'elaborazione di un piano di gestione del rischio. L'obiettivo di questo processo è identificare i rischi potenziali a cui l'azienda può essere esposta e sviluppare strategie per affrontarli, che prevedano la mitigazione o il trasferimento del rischio stesso.

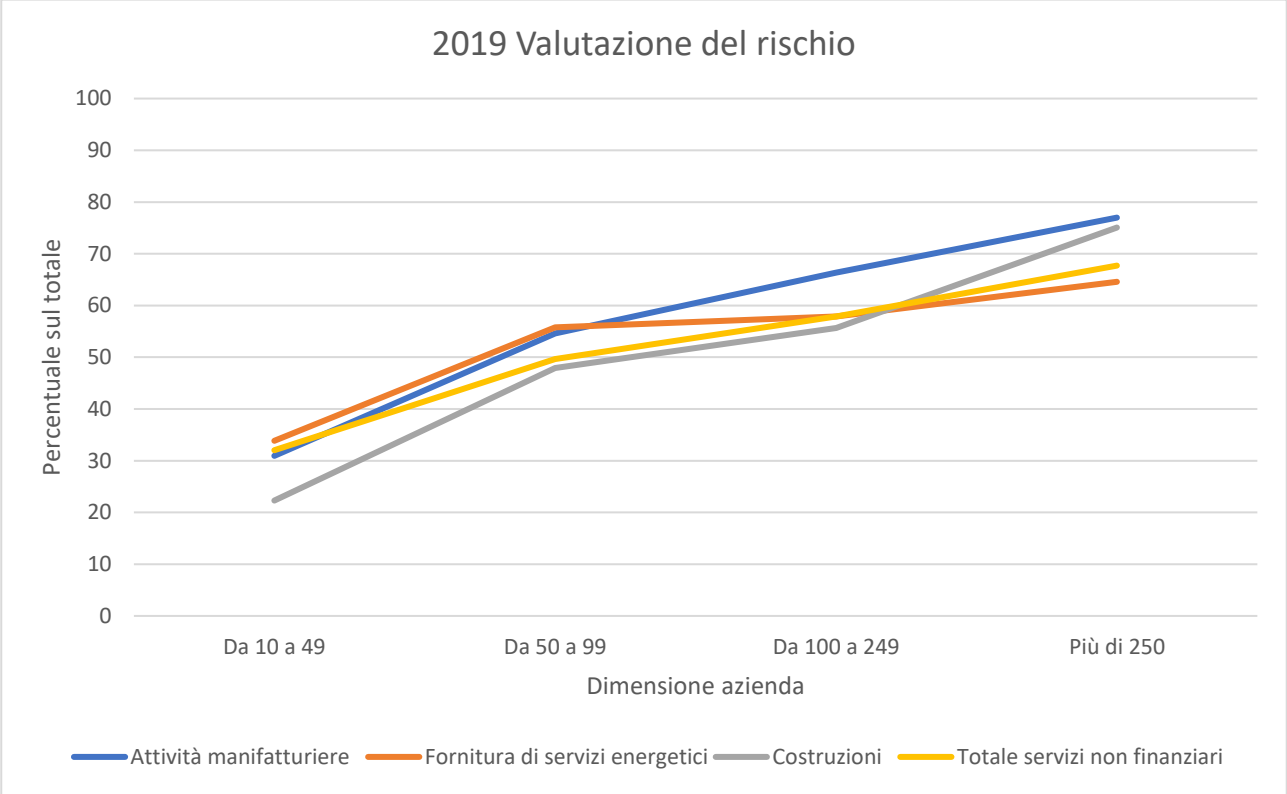

Figura 31. 2019 Percentuale di aziende che utilizza sistemi di valutazione del rischio per dimensione e settore

Relativamente al 2019, un approfondimento sull'impiego di questa strategia nei settori delle costruzioni e della fornitura di servizi energetici mostra differenze significative. Nelle piccole aziende, con un numero di dipendenti compreso tra 10 e 49, solo il 22,3% delle imprese nel settore delle costruzioni implementa un piano di valutazione del rischio, mentre nel settore della fornitura di servizi energetici la percentuale è ben più alta, arrivando al 34%. Questo dimostra una maggiore attenzione al rischio in quest'ultimo settore, anche se su scala ridotta.

Tuttavia, con l'aumento delle dimensioni aziendali, si verifica un cambiamento notevole. Entrambi i settori mostrano un incremento nella percentuale di aziende che adottano la valutazione del rischio, ma con dinamiche diverse. Per le grandi imprese con più di 250 dipendenti, il settore delle costruzioni registra un significativo 75,07% di aziende che conducono valutazione del rischio, posizionandosi appena dietro al settore delle attività manifatturiere. Al contrario, il settore della fornitura di servizi energetici mostra una percentuale inferiore, con solo il 64,58% delle aziende che implementano tale pratica, evidenziando una disparità superiore ai 10 punti percentuali rispetto alle costruzioni. Questa variazione sottolinea come l'attenzione al rischio informatico possa variare notevolmente in base al settore e alla dimensione dell'impresa, influenzando le strategie di gestione del rischio adottate.

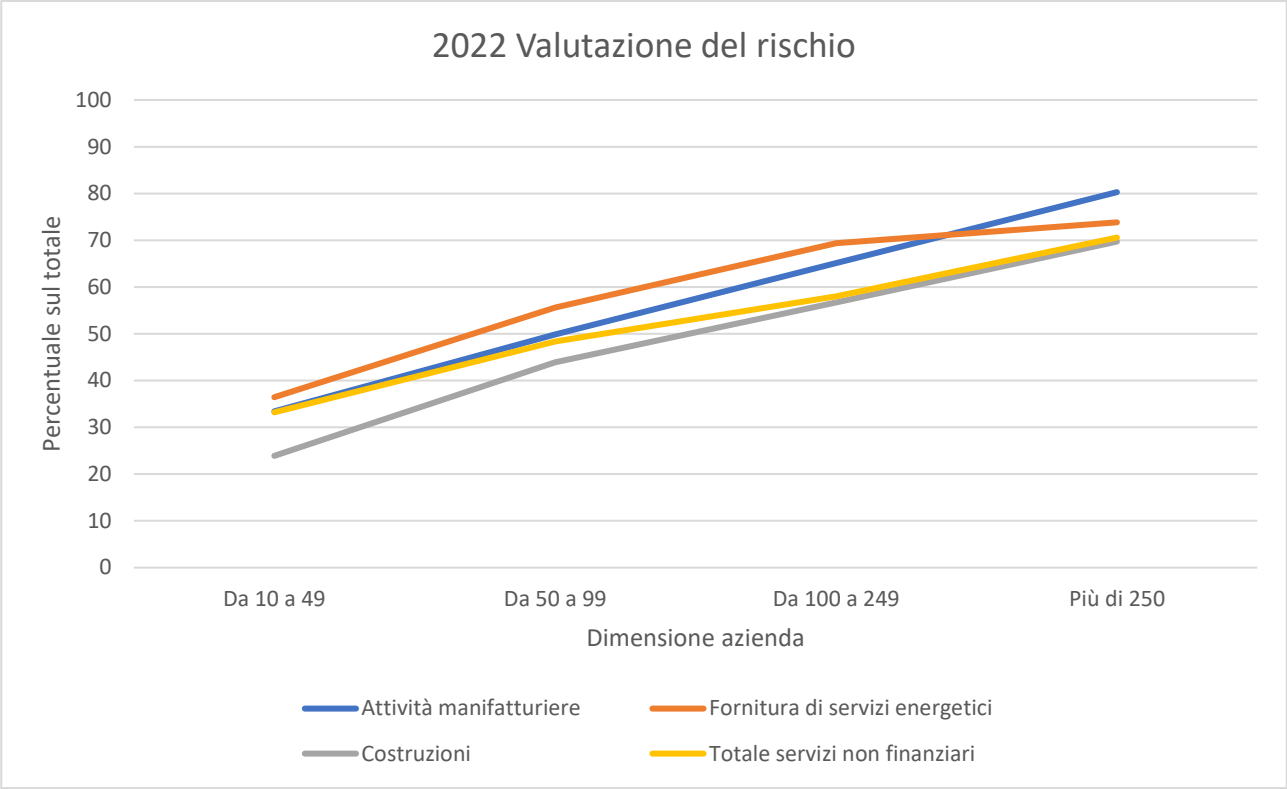

Figura 32. 2022 Percentuale di aziende che utilizza sistemi di valutazione del rischio per dimensione e settore

Nel 2022, l'analisi dei dati mostra delle linearità molto più marcate rispetto alle rilevazioni dell'anno precedente, evidenziando una costanza nella gerarchia di utilizzo delle pratiche di valutazione del rischio nei vari settori al variare delle dimensioni aziendali. Sebbene la maggior parte dei settori presenti un andamento quasi lineare nell'incremento del tasso di utilizzo di queste pratiche, le imprese di fornitura di servizi energetici rappresentano un'eccezione notevole, soprattutto quelle con più di 250 dipendenti, le quali hanno mostrato un incremento di utilizzo rilevante se confrontato con il 2019.

Al contrario, altri settori come le attività manifatturiere dimostrano un aumento quasi costante e prevedibile del tasso di utilizzo delle valutazioni di rischio, confermando una tendenza verso una maggiore consapevolezza e implementazione di misure di sicurezza robuste al crescere della dimensione dell'azienda. Questa tendenza è particolarmente evidente nelle imprese di medie e grandi dimensioni che, nel complesso, hanno aumentato significativamente il loro tasso di utilizzo di queste pratiche rispetto al 2019.

Un esempio significativo di questa dinamica si osserva nel settore della fornitura di servizi energetici. Qui, le medie imprese con un numero di dipendenti tra i 100 e i 249 hanno registrato un aumento dell'11% nell'adozione di pratiche di valutazione del rischio, salendo dal 58% al 69%. Questo incremento sottolinea un rafforzamento delle politiche di sicurezza all'interno di queste aziende, probabilmente in risposta a esigenze emergenti di protezione e compliance. Al contrario, il settore delle costruzioni per le grandi imprese mostra una dinamica opposta, con una diminuzione di circa il 5% nell'utilizzo di queste pratiche, suggerendo forse una diversa prioritizzazione o sfide nella gestione della sicurezza.

L'utilizzo di sistemi di valutazione del rischio è un indicatore fondamentale per valutare il livello di cybersecurity in Italia. L'implementazione di queste pratiche riflette non solo la percezione del rischio ma anche la maturità delle politiche di sicurezza all'interno delle aziende. L'evoluzione di questi indicatori offre quindi un quadro dettagliato di come le imprese italiane stiano rispondendo alle sfide del panorama di minacce in continua evoluzione, adattando le loro strategie per proteggere efficacemente le risorse aziendali e le informazioni sensibili.

Parallelamente all'attività di valutazione del rischio, la conduzione regolare di test di sicurezza rappresenta un'altra misura fondamentale nella prevenzione dei rischi. Questi test, noti come test di penetrazione, simulano attacchi esterni con l'intento di identificare e sfruttare le vulnerabilità nei sistemi aziendali, permettendo così di scoprire e correggere le falle di sicurezza prima che possano essere sfruttate da malintenzionati. Ma i test non si limitano a questo: essi includono anche la verifica dei sistemi di allarme e di backup, indispensabili per rilevare intrusioni e salvaguardare i dati in caso di attacchi riusciti.

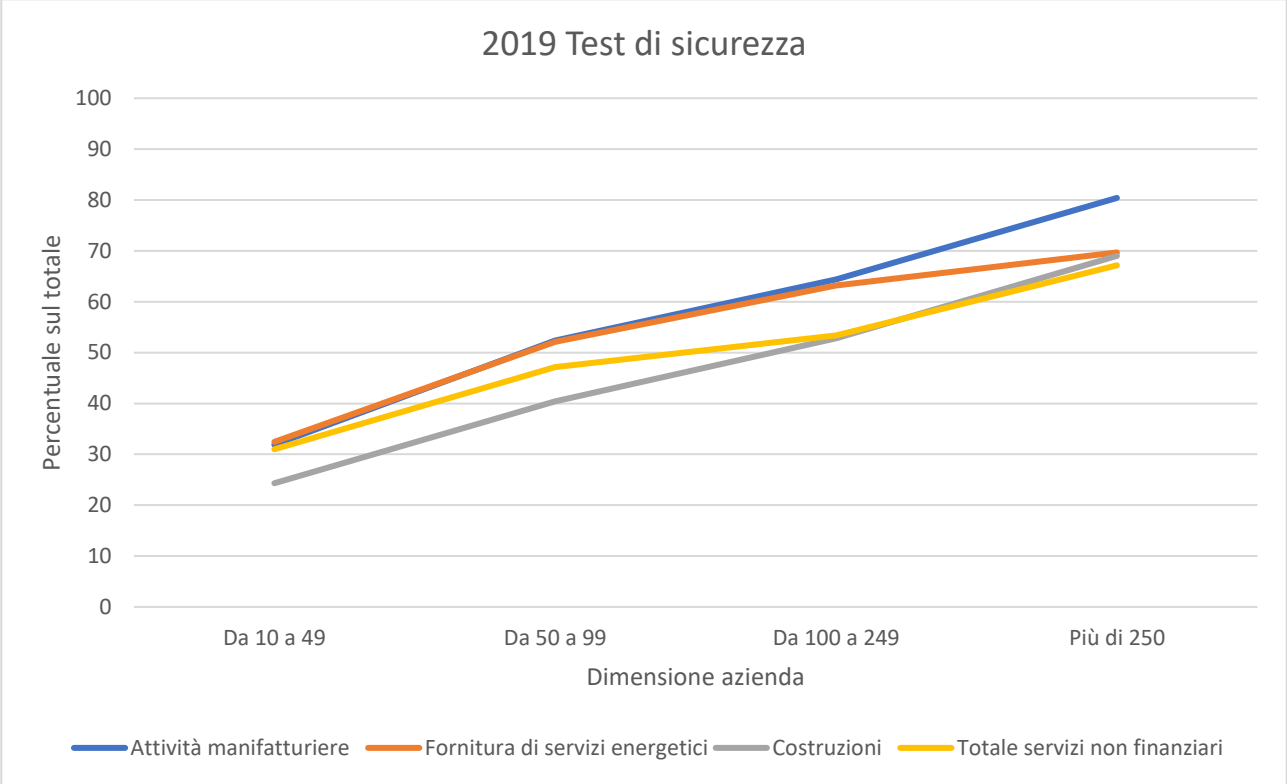

Figura 33. 2019 Percentuale di aziende che utilizza Test di sicurezza per dimensione e settore

L'indicatore relativo al tasso di utilizzo di test di sicurezza rispecchia molto quello precedentemente analizzato relativo alla valutazione del rischio informatico. Si evidenzia per il 2019 come la dimensione aziendale sia direttamente proporzionale al tasso di utilizzo, con un andamento lineare e senza importanti scalini nel passaggio tra piccole, medie e grandi imprese. Rimane comunque importante la pendenza di questo andamento, infatti, prendendo d'esempio le attività manifatturiere, per le imprese con dipendenti compresi tra 10-49 la percentuale di test è pari al 31,88% che aumenta a 52,38% per quelle 50-99, a 64,41% per quelle 100-249, fino a toccare un massimo anche tra gli altri settori per quelle con più di 250 dipendenti, pari ad un 80,4%.

Sono differenze significative, infatti solo 2 imprese manifatturiere su 10 quando raggiungono una grossa dimensione non si impegnano ad effettuare test per la sicurezza, sintomo di grande consapevoleza dei pericoli di un sistema vulnerabile e della necessità di verificare costantemente la presenza di problemi. Allo contrario, solo 3 aziende manifatturiere su 10 con dimensioni ridotte ritengono sia importante testare i proprio sistemi di sicurezza, numero che scende a 2,5 su 10 per quelle del mondo delle costruzioni.

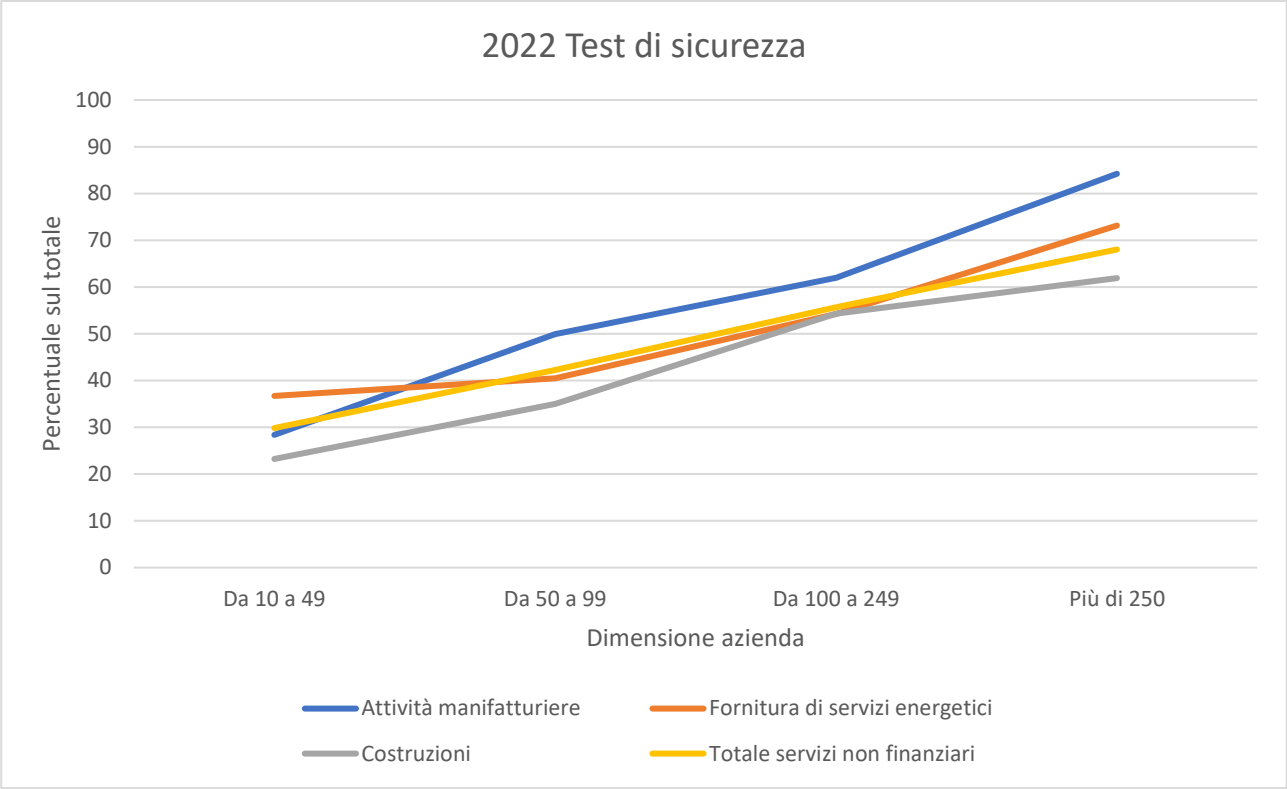

Figura 34. 2022 Percentuale di aziende che utilizza Test di sicurezza per dimensione e settore

Analizzando le risposte del 2022 si nota come queste differenze sostanziali tra le dimensioni aziendali diventino negli anni sempre più rilevanti. La pendenza media delle rette è infatti in aumento rispetto al 2019 dimostrando in parte un aumento della sensibilità alle tematiche di sicurezza informatica nelle medie e grandi imprese, ma allo stesso tempo una diminuzione degli investimenti e delle pratiche nell piccole imprese. Il già basso 31,88% delle piccole imprese manifatturiere scende a poco più del 28%, mentre per le grandi imprese si passa dal precedente 80,4% ad un 84,2%. Il settore che sembra implementare in modo peggiore queste pratiche è quello delle costruzioni che presenta una diminuzione di 5 punti percentuali per le medie imprese e di 7 punti percentuali per le grandi.

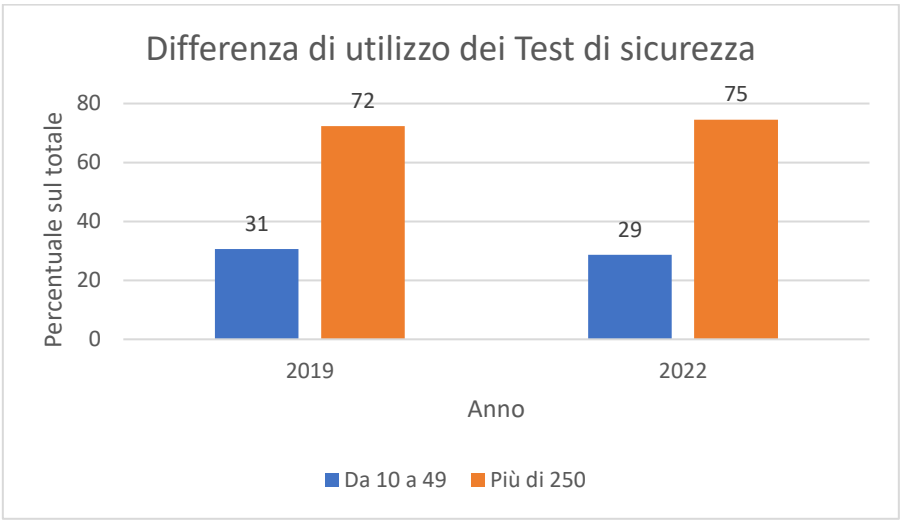

Figura 35. Variazione della percentuale di utilizzatori di test di sicurezza per dimensione 2019vs2022

Nel corso degli ultimi anni, l'analisi delle differenze nell'utilizzo medio dei test di sicurezza tra le imprese di piccole dimensioni e quelle di grandi dimensioni ha mostrato un trend preoccupante dato dall'aumento del

divario. Mentre nel 2019 la differenza nel tasso di adozione di test di sicurezza tra queste due categorie di imprese era già notevole, corrispondendo a circa 41 punti percentuali, tale gap si è ulteriormente ampliato, raggiungendo i 46 punti percentuali in soli tre anni. Questo allargamento del divario evidenzia una crescente disparità nelle capacità e nelle risorse dedicate alla sicurezza informatica, con le grandi imprese che continuano a investire e migliorare le loro pratiche di sicurezza, mentre le piccole imprese sembrano rimanere indietro.

Questa tendenza riflette dinamiche simili osservate negli indicatori di valutazione del rischio, confermando una correlazione attesa tra l'esecuzione di test di sicurezza e la valutazione complessiva del rischio. I test di sicurezza, come gli audit e le simulazioni di attacco, sono fondamentali per identificare vulnerabilità e punti deboli nelle difese aziendali. Questi test sono spesso integrati nella valutazione del rischio, fornendo dati concreti su quali aree necessitano di maggiori controlli o di un rafforzamento delle misure di protezione. Non sorprende quindi che le aziende che adottano un approccio proattivo e sistematico nella valutazione del rischio tendano anche a essere più diligenti nell'esecuzione di test di sicurezza.

D'altra parte, le aziende che non integrano pienamente queste pratiche nella loro strategia di sicurezza spesso espongono sé stesse a rischi maggiori. La mancanza di test di sicurezza regolari può lasciare non rilevate le vulnerabilità, aumentando il rischio di violazioni dei dati e di attacchi informatici. Inoltre, la sottovalutazione dell'importanza di una valutazione del rischio completa e dettagliata può portare a una scarsa comprensione delle minacce potenziali, rendendo le aziende meno preparate a difendersi efficacemente.

In questo contesto, è essenziale che tutte le imprese, indipendentemente dalle loro dimensioni, riconoscano l'importanza di investire in pratiche robuste di sicurezza informatica. Per le piccole imprese, in particolare, diventa cruciale cercare soluzioni accessibili e efficaci per colmare il divario tecnologico e risorse con le loro controparti più grandi. Solo attraverso un impegno condiviso nel rafforzare la sicurezza informatica, il panorama aziendale può sperare di resistere alle crescenti e sempre più sofisticate minacce informatiche.

4.6 Analisi degli Attacchi

Dopo aver analizzato quale sia stata l'evoluzione dei sistemi di sicurezza e controllo nelle imprese di diverse dimensioni e settore, è necessario studiare l'andamento degli attacchi, in modo da poter determinare quale sia stato l'effetto di questi cambiamenti nel tempo. Nello specifico l'obiettivo è capire quale fosse il livello di impatto di ciascuna tipologia di attacco nel 2019 e vedere la sua evoluzione nel 2022, andando a spiegare il motivo di queste variazioni in relazione alle variabili studiate nei precedenti paragrafi.

Prima di partire con lo studio è necessario sintetizzare i risultati raccolti in modo da poter prevedere il cambiamento dell'incidenza degli attacchi e capire quali indicatori siano i principali determinati delle diverse tipologie di attacco.

1. **Gli strumenti primari**: Le analisi sui primi tre indicatori rivelano tendenze diversificate in base alla dimensione aziendale e al settore di appartenenza. Per l'uso di password robuste, si osserva un aumento tra le piccole imprese mentre le medie imprese mostrano una riduzione, anche se nel settore dei servizi non finanziari si registra un incremento. Per quanto riguarda il backup dei dati, il livello di protezione è generalmente elevato in tutti i settori ed anche in tutte le dimensioni, ciò nonostante la tendenza è al ribasso in tutti i settori, eccetto nei servizi non finanziari dove si nota un aumento, essendo il livello di partenza inferiore alla media. Non emergono variazioni significative di questo trend tra i due anni analizzati in relazione alla dimensione delle aziende. Infine, il controllo della rete evidenzia un calo generalizzato in tutti i settori, marcato soprattutto nelle aziende con meno di 100 dipendenti, sebbene si constati un lieve miglioramento nelle grandi aziende che superano i 100 dipendenti.

2. **Gli strumenti secondari:** I risultati relativi all'utilizzo di dati biometrici mostrano significative variazioni a seconda del settore e della dimensione aziendale. Si nota un aumento complessivo nell'adozione di questa tecnologia, con i settori delle costruzioni e dei servizi non finanziari che registrano un marcato incremento, simile a quello osservato nelle grandi imprese, particolarmente attive nell'integrare queste soluzioni. Analogamente, l'uso delle VPN ha visto un incremento generalizzato, con le piccole e medie imprese che aumentano il loro tasso di adozione in misura maggiore rispetto alle grandi imprese, le quali partivano già da basi elevate. In tutti i settori, l'aumento medio è di circa 10 punti percentuali. Per quanto riguarda la crittografia delle email, non emergono differenze significative nell'utilizzo tra i due anni considerati nell'analisi.
3. **La prevenzione del rischio:** L'analisi dell'indicatore sulla valutazione del rischio mostra una tendenza generale all'incremento tra i due anni considerati in tutti i settori e per tutte le dimensioni aziendali, con l'eccezione delle medie imprese dove si registra una leggera diminuzione. Gli aumenti osservati non sono particolarmente marcati, attestandosi mediamente intorno ai 3 punti percentuali per i vari settori. Per quanto riguarda le dimensioni aziendali, i valori rimangono sostanzialmente stabili, eccetto che per le grandi imprese che evidenziano un incremento di circa 4 punti. I risultati per l'indicatore dei test di sicurezza presentano, al contrario, una tendenza generale alla diminuzione in tutti i settori nel periodo considerato, ad eccezione del settore della fornitura di servizi energetici. Anche per le dimensioni aziendali, si osserva una riduzione, eccetto nelle grandi imprese che, simile a quanto osservato per la valutazione del rischio, mostrano un aumento percentuale analogo.

Il primo indicatore analizzato è quello riguardante l'indisponibilità di servizi informatici a causa di attacchi dall'esterno come, ad esempio, attacchi ransomware o denial of service.

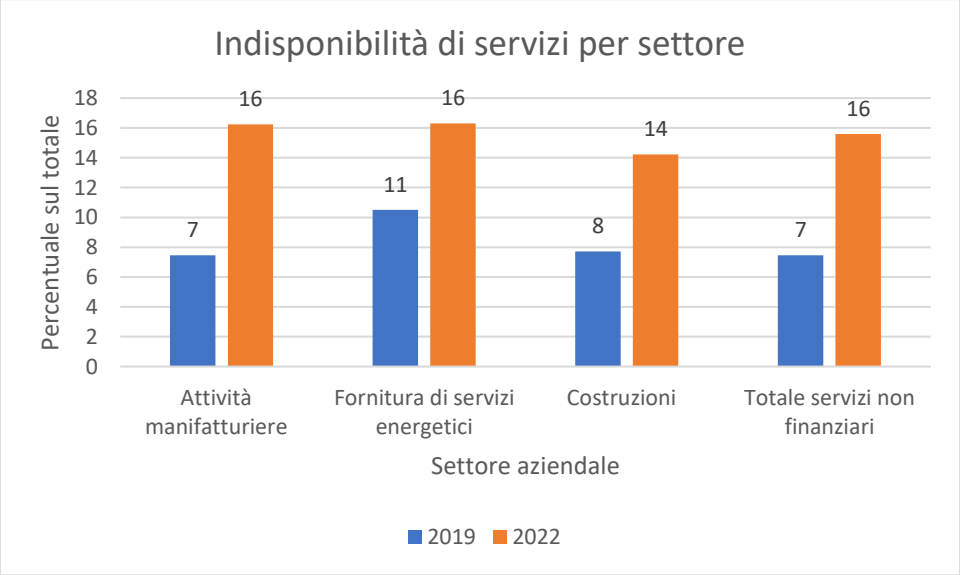

Figura 36. Variazione della percentuale di aziende che hanno subito una indisponibilità di servizi digitali per settore 2019vs2022

La figura illustra l'evoluzione tra il 2019 e il 2022 delle percentuali di aziende, categorizzate per settore, che hanno subito almeno un attacco da un agente esterno, risultando in una indisponibilità dei servizi digitali. Si osserva un notevole aumento degli attacchi in tutti i settori, con un incremento medio che si stabilizza intorno al 16% per l'intero mercato. In particolare, le aziende operanti nel settore manifatturiero e nei servizi non finanziari hanno registrato un aumento di circa 9 punti percentuali in soli tre anni, più che raddoppiando la percentuale rispetto al 2019.

Questi nuovi dati, sorprendentemente simili nonostante le diverse aree di mercato, si possono attribuire all'aumentata tendenza delle aziende verso la digitalizzazione. Se in passato alcuni settori potevano evitare di adattarsi completamente alla digitalizzazione del mercato, oggi questa transizione è diventata un'esigenza sempre più impellente. Questo processo ha spesso portato a una implementazione non ottimale delle misure di sicurezza necessarie, rendendo le infrastrutture aziendali più vulnerabili agli attacchi informatici.

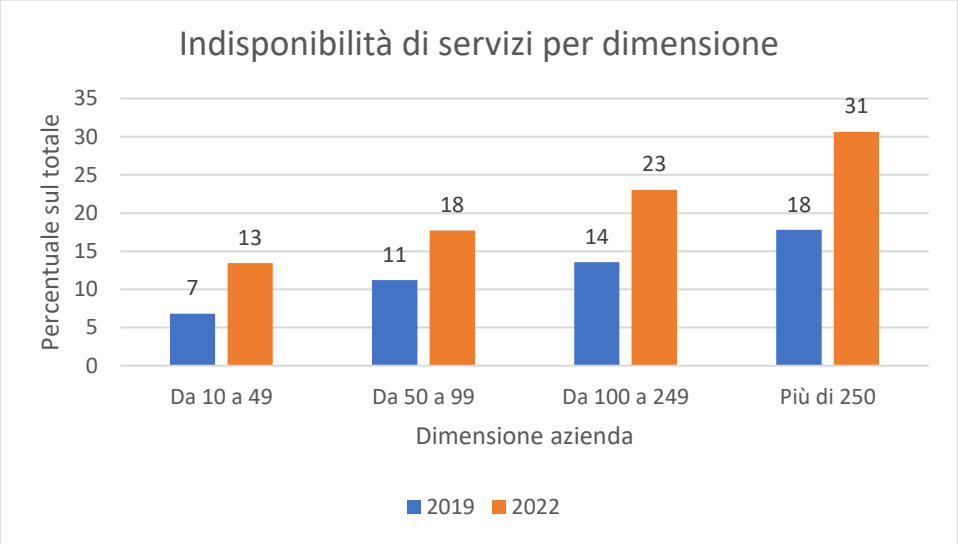

Figura 37. Variazione della percentuale di aziende che hanno subito una indisponibilità di servizi digitali per dimensione 2019vs2022

Questo secondo grafico rivela come la percentuale di attacchi vari in base alla dimensione aziendale. Confermando le analisi precedenti, le piccole imprese risultano essere quelle che meno investono in sistemi di sicurezza informatica, spesso con una tendenza alla diminuzione di tali investimenti nel tempo. Di conseguenza, era prevedibile assistere a un aumento delle aziende colpite da attacchi informatici. Sorprendentemente, nel 2022, oltre una piccola impresa su dieci ha subito almeno un'incursione. In dettaglio, le piccole imprese hanno registrato un incremento medio degli attacchi di 6 punti percentuali rispetto alle rilevazioni precedenti, mentre le medie imprese hanno visto un incremento tra 7 e 9 punti percentuali. Per le grandi imprese, la percentuale di quelle che hanno subito un'interruzione dei servizi digitali è salita dal 18% al 31% in soli tre anni, un dato sorprendente considerando gli investimenti significativi in sicurezza che queste aziende tendono a fare.

Il dato più significativo emerge dall'analisi annuale relativa alla dimensione aziendale, mostrando una correlazione diretta tra la dimensione dell'azienda e l'aumento degli attacchi tra i due anni in esame. Contrariamente a quanto ci si potrebbe aspettare data la loro avanzata implementazione di sistemi di sicurezza, le grandi aziende hanno registrato il maggiore incremento percentuale di attacchi. Questo fenomeno sottolinea come la visibilità e la grandezza di un'azienda la rendano un bersaglio più attraente per gli attacchi di hacker esterni.

Nonostante le grandi aziende dispongano di maggiori risorse economiche, che possono essere richieste come riscatto in caso di successo dell'attacco, la loro estensione e il vasto numero di dipendenti possono paradossalmente aumentarne la vulnerabilità. Infatti, la grande scala operativa può facilitare episodi di phishing e altri schemi di inganno mirati ai dipendenti, rendendo queste imprese potenzialmente più esposte nonostante gli elevati investimenti in sicurezza. Questi risultati evidenziano l'importanza di non solo investire in tecnologie di sicurezza avanzate, ma anche di mantenere una costante vigilanza e formazione dei dipendenti per mitigare il rischio di attacchi informatici.

Il secondo indicatore analizzato riguardante gli attacchi subiti dalle imprese italiane nei due anni rilevati risulta essere frutto delle risposte relative alla domanda sull'aver subito una corruzione o distruzione dei dati a causa di un attacco esterno.

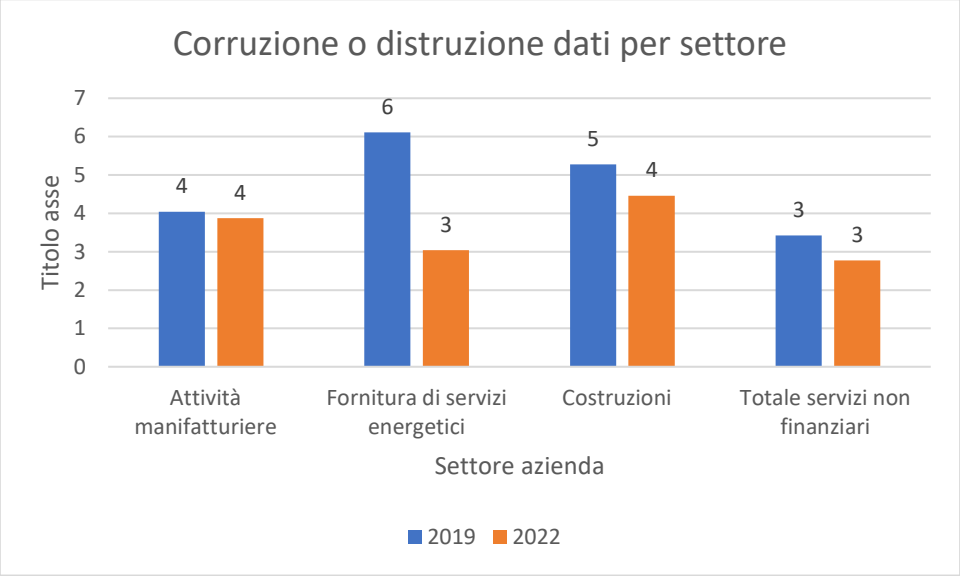

Figura 38. Variazione della percentuale di aziende che hanno subito una corruzione od distruzione di dati per settore 2019vs2022

La differenza tra i dati attuali e quelli raccolti dall'indicatore precedente è notevolmente evidente. Mentre nel 2022 la percentuale di aziende che hanno subito corruzione o distruzione dei propri dati si stabilizza intorno al 3-4%, questo valore è sensibilmente inferiore rispetto al 16% registrato precedentemente e mostra anche una diminuzione rispetto al 2019. Questo scarto può essere attribuito alla natura distinta degli incidenti: mentre l'indisponibilità di servizi può derivare da un blocco temporaneo dei sistemi, la corruzione o distruzione dei dati implica una perdita parziale o totale di informazioni essenziali nei database aziendali.

Un aspetto cruciale per comprendere meglio questo indicatore è l'efficacia delle strategie di backup dei dati. Le analisi precedenti evidenziano che sia nel 2019 sia nel 2022, le aziende hanno mantenuto livelli elevati di utilizzo delle pratiche di backup, il che spiega la difficoltà nell'osservare casi di perdita completa di dati sensibili. In un ambiente aziendale dove i dati sono sempre più digitalizzati, il backup regolare e affidabile diventa un pilastro fondamentale per mitigare il rischio di perdite catastrofiche di informazioni.

Inoltre, la resilienza informatica si rafforza non solo attraverso il backup, ma anche attraverso l'adozione di strategie di valutazione del rischio. Come precedentemente analizzato, queste pratiche sono in aumento generale in tutti i settori in analisi, motivo per il quale, nell'avvenimento di una intrusione con possibile corruzione di dati, possono essere predisposte contromisure efficaci per la salvaguardia delle informazioni.

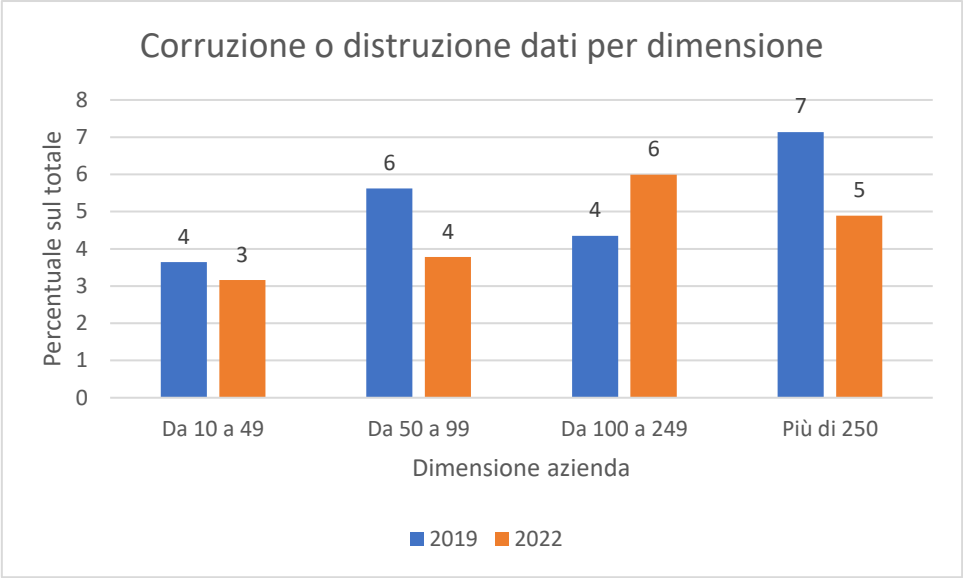

Figura 39. Variazione della percentuale di aziende che hanno subito una corruzione od distruzione di dati per dimensione 2019vs2022

Differentemente dall'analisi per settore, l'analisi per dimensione presenta dei dati molto più variabili. Nel 2019 la statistica presenta una tendenza a crescere con la dimensione aziendale, con un valore fuori scala per le aziende con dipendenti tra i 100 ed i 249, leggermente più basso della linea di tendenza. In modo opposto si visualizzano i dati del 2022 che generalmente presentano una diminuzione percentuale rispetto al precedente anno di analisi, con l'eccezione della stessa dimensione prima citata che invece presenta un aumento. Come per la divisione per settore, i valori generali non sono elevati come per il precedente indicatore e presentano una generale diminuzione tra i due anni. Il motivo, oltre all'ampio utilizzo di sistemi di backup, può essere ricercato nella necessità delle imprese di non perdere dati sensibili; infatti, il pagamento del "riscatto" normalmente richiesto dagli aggressori per il riottenimento dei dati rubati può in molti casi essere la soluzione economicamente più vantaggiosa, soprattutto per le grandi aziende, nelle quali la non continuità del business porta ad elevati costi solitamente maggiori del riscatto stesso.

L'ultimo indicatore in analisi fa riferimento alla divulgazione di dati riservati a seguito di un'intrusione da parte di un aggressore esterno.

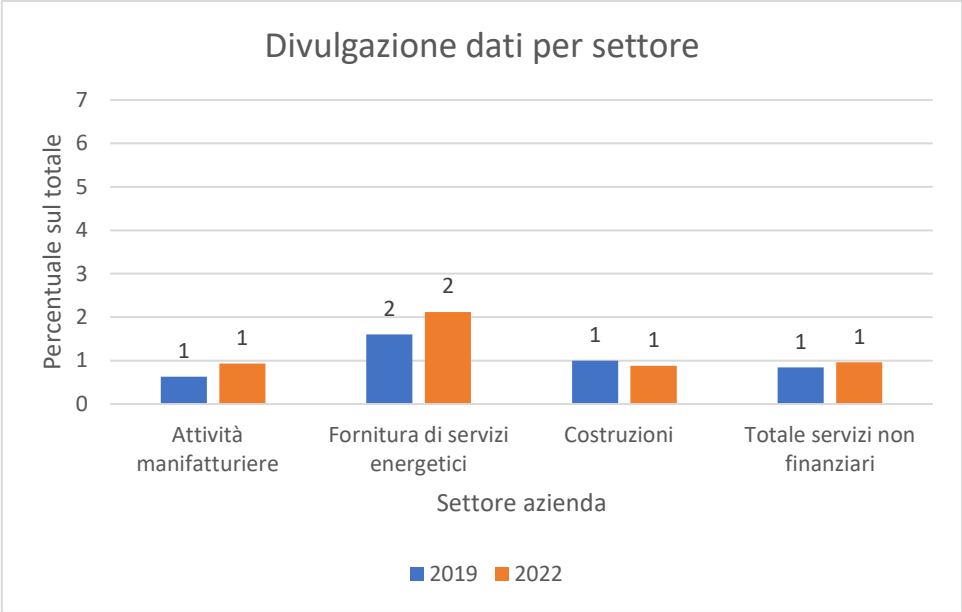

Figura 40. Variazione della percentuale di aziende che hanno subito una divulgazione di dati sensibili per settore 2019vs2022

Nel grafico sopra riportato sono indicate le percentuali di aziende, divise per settore, che hanno subito negli anni di analisi una intrusione che ha causato la divulgazione di dati riservati. Il confronto tra i valori del 2019 e del 2022 non porta a notevoli differenze, i valori infatti si assestano ad un valore compreso tra l'1% ed il 2% sul totale in tutti i settori, percentuali decisamente inferiori a quelle analizzate precedentemente. Il motivo può essere ricercato nella bassa incidenza di attacchi in aziende di piccole e medie dimensioni, unito all'implementazione generale di pratiche di valutazione del rischio. La differenza della percentuale dei fornitori di servizi energetici può essere ricercata nel valore dei dati stessi che essi raccolgono, in primo luogo indirizzo ed età dei propri clienti. Questi dati possono essere successivamente rivenduti ad ulteriori malintenzionati con lo scopo di possibili truffe future.

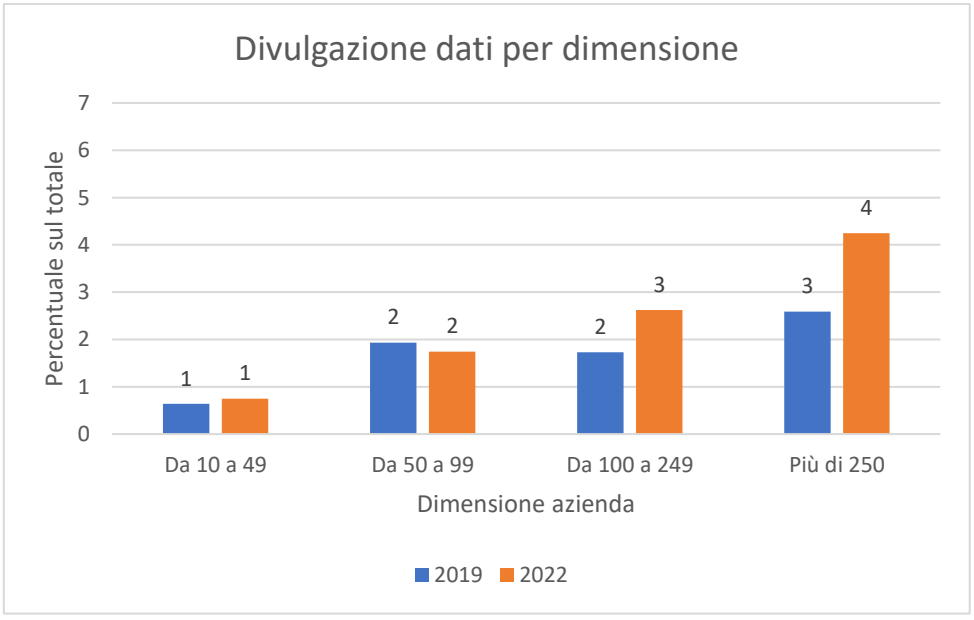

Figura 41. Variazione della percentuale di aziende che hanno subito una divulgazione di dati sensibili per dimensione 2019vs2022

Diversamente dai dati raccolti per settore, la divisione per dimensione evidenzia delle differenze molto più marcate. In primo luogo, nonostante anche in questo caso le differenze tra i due anni in analisi non siano estremamente elevate, è chiaramente percepibile un incremento delle percentuali per le medio-grandi aziende, con un aumento medio di un punto percentuale. Inoltre, è chiaramente individuabile una differenza basata sulla dimensione aziendale, in linea con i precedenti indicatori. Nonostante le grandi aziende presentino sistemi di sicurezza più elaborati, come individuato nell'analisi sui sistemi di protezione fatta precedentemente, i dati di una grande azienda sono molto più appetibili sul mercato di quelli di una piccola azienda, a parità di settore. La mole di dati di una azienda con meno di 50 dipendenti, difficilmente può presentare un qualche valore economico per il potenziale aggressore, ed allo stesso modo, più è piccola l'azienda e meno è incentivata a pagare una cifra per evitare la loro divulgazione.

Per questa serie di ragioni, unite a quelle precedentemente esposte per gli altri indicatori, vi è una tendenza delle grandi aziende a cadere vittima di intrusioni esterne, nonostante l'aumento di sistemi di protezione come l'utilizzo di dati biometrici e le VPN. Per questo motivo, l'implementazione di pratiche di valutazione del rischio e di test per la sicurezza risultano essere in forte crescita in questa tipologia di aziende molto più che in quelle di dimensione ridotta, risultano essere i metodi più efficaci per la difesa contro aggressori esterni.

4.7 Analisi delle Assicurazioni

Al termine delle analisi relative all'incidenza degli attacchi, si analizzano le risposte alla domanda della sezione *Q4* riguardante la sottoscrizione a servizi di assicurazioni sulla sicurezza informatica nell'azienda. È infatti importante verificare il cambiamento della percentuale di utilizzatori comparandolo alla variazione del quantitativo di aziende colpite da una qualsiasi tipologia di attacco.

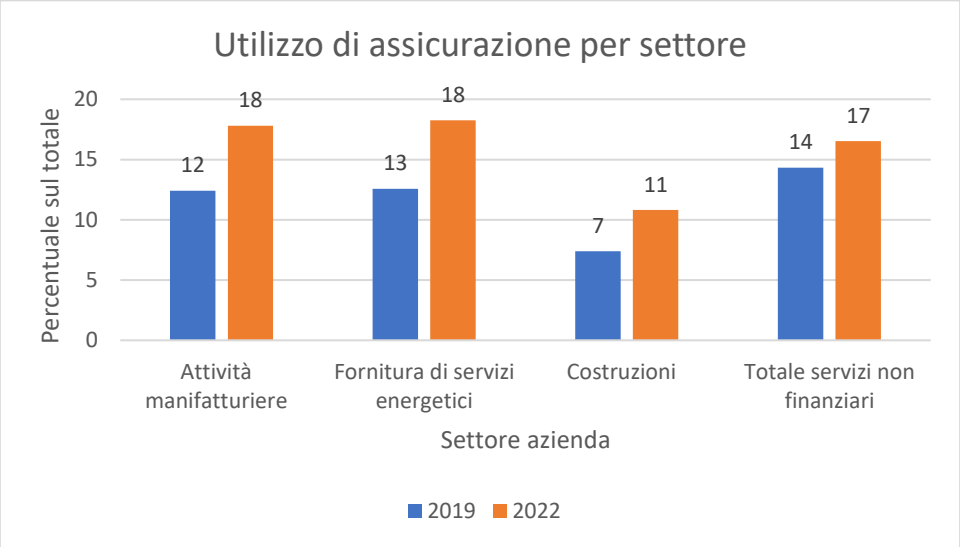

Figura 42. Variazione della percentuale di aziende che hanno fatto uso di assicurazioni contro incidenti di sicurezza informatica per settore 2019vs2022

Il grafico sopra riportato individua la percentuale di aziende, divise per settore, che nel 2019 e nel 2022 hanno usufruito di questa tipologia di assicurazione. Si nota immediatamente come per tutte le tipologie di settore si presenti un aumento percentuale di sottoscrittori, in particolare per le attività manifatturiere e per quelle di fornitura di servizi energetici. Queste due categorie, nonostante non presentino rilevanti incrementi per quanto riguarda attacchi che hanno portato a corruzione o distruzione di dati nei due anni in analisi, sono gli stessi che maggiormente hanno subito un incremento di attacchi per gli altri due indicatori, in particolare, indisponibilità di servizi ICT per le attività manifatturiere e divulgazione di dati sensibili per quelle di fornitura di servizi energetici. I fornitori di servizi non finanziari non presentano invece un

incremento rilevante, ma ciò può essere dovuto al già elevato valore nel 2019. È inoltre importante rilevare come queste percentuali siano in linea con quelle relative all'indisponibilità di servizi ICT, segno che sia presente una correlazione diretta tra l'aver subito questa tipologia di attacco e l'aver sottoscritto una assicurazione a riguardo.

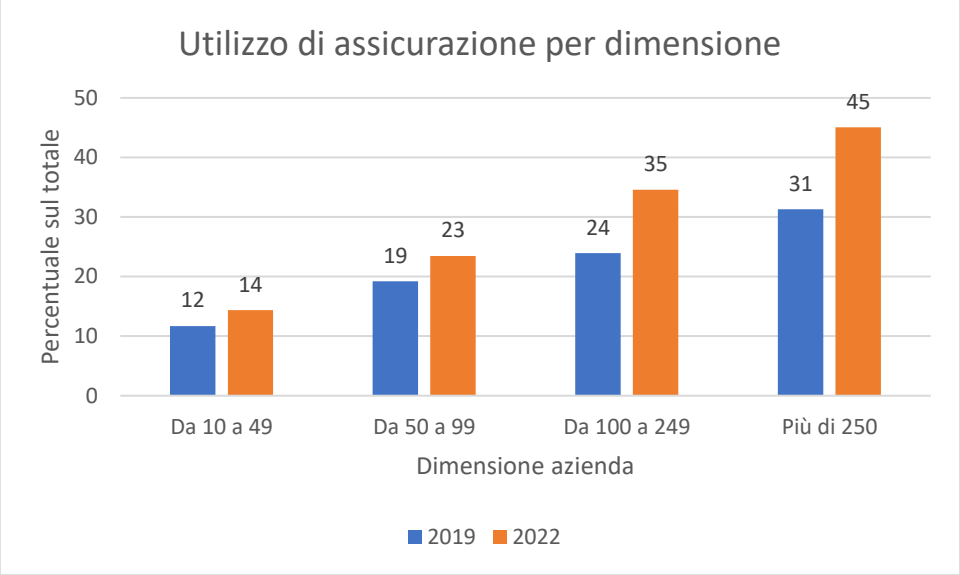

Figura 43. Variazione della percentuale di aziende che hanno fatto uso di assicurazioni contro incidenti di sicurezza informatica per dimensione 2019vs2022

Nell'analizzare la variazione relativa alla dimensione aziendale, si osserva un trend di incremento percentuale direttamente proporzionale alla grandezza dell'impresa. Questo fenomeno non sorprende, dato che le grandi aziende, avendo maggiore visibilità e una più ampia disponibilità di dati, tendono naturalmente a essere bersagli più attraenti per gli attacchi esterni. Nonostante l'intensificazione degli sforzi nell'aggiornamento dei sistemi di sicurezza, le grandi imprese continuano a registrare un aumento degli attacchi nel tempo, spiegando così il parallelo incremento delle grandi aziende che optano per assicurazioni specifiche per mitigare i rischi associati a tali attacchi.

Per le aziende con un numero di dipendenti compreso tra 100 e 250, nel 2019 circa un quarto di esse aveva stipulato polizze assicurative, una cifra che è cresciuta a più di un terzo in soli tre anni. In modo simile, tra le aziende con più di 250 dipendenti, la proporzione di quelle assicurate è aumentata dal 31% nel 2019 al 45% nel 2022.

Questo aumento dell'adozione di assicurazioni riflette una crescente consapevolezza delle sfide poste dalla sicurezza informatica. Nonostante gli avanzamenti significativi nei sistemi di protezione, l'escalation degli attacchi evidenzia una realtà inevitabile: il rischio di incursioni dannose è sempre presente. Di conseguenza, oltre a implementare misure di sicurezza avanzate, per le aziende diventa essenziale disporre di un ulteriore strato di protezione contro le perdite economiche potenziali. L'assicurazione, in questo contesto, non solo offre una copertura finanziaria in caso di attacchi riusciti ma rappresenta anche un componente critico nella strategia complessiva di gestione del rischio.

Questi dati sottolineano l'importanza per le aziende di non solo investire in tecnologia e formazione per difendere i propri sistemi digitali ma anche di considerare soluzioni assicurative che possano offrire un cuscinetto finanziario contro le eventualità di sicurezza. In ultima analisi, mentre le misure preventive sono cruciali, la resilienza si costruisce anche attraverso la capacità di rispondere efficacemente alle emergenze quando queste si verificano.

Conclusioni

L’analisi condotta sul livello di sicurezza informatica nelle imprese italiane ha messo in evidenza quanto la cybersecurity sia diventata un elemento fondamentale nell’attuale contesto di trasformazione digitale. Il percorso storico della cybersecurity mostra come la crescente dipendenza delle aziende dalle tecnologie digitali abbia portato allo sviluppo di sistemi di difesa sempre più complessi. Questa evoluzione è stata determinante per comprendere non solo le minacce passate, ma anche le nuove sfide che si profilano all'orizzonte. Un aspetto centrale dello studio è stato l’approfondimento delle principali tipologie di crimini informatici, tra cui phishing, ransomware e hacktivism, che continuano a rappresentare minacce di vasta portata per le imprese. La crescente sofisticazione degli attacchi e le loro motivazioni, spesso legate a guadagni finanziari, ma sempre più orientate alla destabilizzazione operativa, dimostrano la necessità di adottare misure preventive adeguate. Tuttavia, nonostante la consapevolezza crescente, molte aziende italiane faticano ancora a implementare difese efficaci contro tali minacce, e ciò contribuisce ad ampliare la loro vulnerabilità. Il contesto normativo italiano ed europeo si è dimostrato cruciale per fornire un quadro di riferimento alle imprese, incentivando l’adozione di misure di sicurezza più robuste. Tuttavia, come emerso, le sole normative non bastano: è necessaria una maggiore adesione da parte delle imprese e un impegno concreto nella loro implementazione pratica. Le riforme e le iniziative come il PNRR forniscono un supporto importante, ma la loro efficacia dipende dall’attivazione di risorse adeguate e dalla capacità delle aziende di integrare queste politiche nelle loro strategie operative.

Il nucleo centrale di questo studio si è concentrato sull'analisi del livello di cybersecurity nelle imprese italiane, grazie ai dati forniti da Istat. Il quadro che emerge non è omogeneo: se da un lato alcune imprese, soprattutto di maggiori dimensioni, stanno adottando misure di sicurezza avanzate, dall’altro molte piccole e medie imprese non sembrano investire allo stesso modo. Nonostante le differenze nell'adozione delle pratiche di sicurezza, i risultati mostrano chiaramente che, all'aumentare della dimensione aziendale, cresce in modo più che proporzionale la percentuale di aziende vittime di attacchi informatici. Questo suggerisce che, sebbene le imprese più grandi implementino un numero maggiore di misure di sicurezza, sono comunque più esposte agli attacchi da parte di agenti esterni. Le ragioni di questo fenomeno possono essere ricondotte principalmente a due fattori: i motivi e i metodi degli attacchi.

Innanzitutto, con l'espansione delle dimensioni aziendali, cresce anche la quantità di dati sensibili che queste aziende gestiscono, sia riguardo alle operazioni interne sia relativi ai propri clienti. Questo le rende obiettivi più attraenti per i cybercriminali, poiché un attacco a una grande azienda può potenzialmente generare maggiori ricompense, sia economiche che di altra natura. Tuttavia, questo aspetto da solo non è sufficiente a spiegare l'incremento degli attacchi, soprattutto considerando che, come evidenziato dall’analisi del dataset, le aziende più grandi investono anche in sistemi di sicurezza più avanzati.

Il secondo elemento cruciale da considerare riguarda i metodi utilizzati dai cybercriminali per portare a termine i loro attacchi. Come discusso nel capitolo dedicato al cybercrime, le intrusioni forzate non rappresentano più la principale tecnica per sottrarre dati sensibili. Al contrario, i criminali informatici ricorrono sempre più frequentemente a strategie più semplici, ma altrettanto efficaci, come il phishing. Nonostante i notevoli investimenti in misure di sicurezza avanzate, un attacco di phishing può facilmente compromettere l’azienda: basta che un singolo dipendente clicchi su un link dannoso presente in un’email fraudolenta, permettendo così il furto di dati riservati o l'infiltrazione di un ransomware, con conseguente blocco dei sistemi aziendali. La vulnerabilità delle grandi aziende a questo tipo di attacchi è legata al numero elevato di dipendenti che possono essere presi di mira. Con una forza lavoro più ampia, aumenta la probabilità che qualcuno cada vittima di una truffa di phishing, rendendo queste aziende particolarmente esposte a questo genere di minacce, nonostante l'adozione di sofisticati sistemi di protezione.

Questi risultati sottolineano l'importanza di affiancare gli investimenti in sicurezza informatica a un'adeguata formazione interna, indipendentemente dalla dimensione aziendale. Strumenti come la valutazione dei rischi, i test di sicurezza e le polizze assicurative contro incidenti ICT devono essere adottati con maggiore frequenza, ma ciò non basta. È essenziale che le aziende garantiscano una formazione continua ai propri dipendenti, affinché siano consapevoli delle minacce del mondo digitale e possano contribuire attivamente alla protezione dell'organizzazione.

In conclusione, lo studio dimostra che, nonostante i progressi compiuti, le imprese italiane devono ancora compiere passi significativi per rafforzare la propria sicurezza informatica. La digitalizzazione offre immense opportunità, ma porta con sé anche sfide rilevanti. Investire in cybersecurity non è più una scelta opzionale, ma una necessità per garantire la continuità e la competitività aziendale in un mondo sempre più interconnesso. Solo un approccio integrato, che unisca tecnologie avanzate, formazione continua del personale e un solido quadro normativo, potrà ridurre l'esposizione ai rischi informatici e assicurare un futuro digitale sicuro per le imprese italiane.

Bibliografia

[1] https://csrc.nist.gov/glossary/term/cybersecurity

[2] https://csrc.nist.gov/glossary/term/cyberspace

[3] https://www.sailpoint.com/identity-library/five-types-of-cybersecurity/

[4] Abbate, J. (2000). Inventing the Internet. MIT Press

[5] https://en.wikipedia.org/wiki/Internet_protocol_suite

[6] https://en.wikipedia.org/wiki/Data_Encryption_Standard

[7] https://pandorafms.com/blog/creeper-and-reaper/

[8] https://arcticwolf.com/resources/blog/decade-of-cybercrime/

[9] https://www.cloudflare.com/it-it/learning/security/glossary/what-is-zero-trust/

[10] SurfShark. (2023). *Virtual private network (VPN) market worldwide in 2023, by country (in billion U.S. dollars)*. *Statista*. Statista Inc.. Accessed: June 30, 2024. https://www-statista-com.ezproxy.biblio.polito.it/statistics/1341916/worldwide-virtual-private-network-market-country/

[11] Security.org. (2023). *Average monthly price for virtual private networks in 2023 (in U.S. dollars)*. *Statista*. Statista Inc.. Accessed: June 30, 2024. https://www-statista-com.ezproxy.biblio.polito.it/statistics/1449514/global-vpns-monthly-price/

[12] Petee, T. A., Corzine, J., Huff-Corzine, L., Clifford, J., & Weaver, G. (2010). Defining "cyber-crime": Issues in determining the nature and scope of computer-related offenses. *Futures Working Group*, *5*, 6-11.

[13] Malik, J. K., & Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, *9*(3), 242.

[14] IC3, FBI. (2024). *Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023 (in million U.S. dollars)*. *Statista*. Statista Inc.. Accessed: July 16, 2024. https://www-statista-com.ezproxy.biblio.polito.it/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us

[15] Barracuda Networks. (2023). *Distribution of spear-phishing attacks worldwide in 2022, by type*. *Statista*. Statista Inc.. Accessed: July 17, 2024. https://www-statista-com.ezproxy.biblio.polito.it/statistics/1253262/spear-phishing-attack-trends/

[16] Barracuda Networks. (2023). 2023 spear-phishing trends

[17] https://www.ibm.com/reports/data-breach

[18] 02.04.2021 Ransomware: What It Is & What To Do About It (pdf)

[19] Fortinet. (2023) The 2023 Global Ransomware Report

[20] Fortinet. (2023) Global Threat Landscape Report

[21] https://www.chainalysis.com/blog/ransomware-2024/

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

[23] https://www.investopedia.com/terms/h/hacktivism.asp

[24] https://it.wikipedia.org/wiki/WikiLeaks

[25] Rapporto Clusit 2024 sulla sicurezza ICT in Italia

[26] Agenzia per la Cybersicurezza in Italia (2023) Relazione Annuale al Parlamento 2023

[27] https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale

[28] DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016

[29] DECRETO LEGISLATIVO 18 maggio 2018, n. 65

[30] https://www.acn.gov.it/portale/home

[31] Proofpoint. (2024). *Consequences of ransomware attacks for organizations following ransom payments worldwide in 2023*. *Statista*. Statista Inc.. Accessed: July 22, 2024. https://www-statista-com.ezproxy.biblio.polito.it/statistics/1147471/outcomes-organizations-ransom-payments-it-professionals/