# POLITECNICO DI TORINO

Facoltà di Ingegneria

Corso di Laurea Magistrale in Ingegneria Gestionale

Tesi di Laurea Magistrale


Relatore
Prof. Federico Caviggioli

Candidato
Antonio Luca Romoli

Anno accademico 2022/2023

# Indice

## Capitolo 1



## Capitolo 2



## Capitolo 3

# Capitolo 1

## Tecnologia e digitalizzazione

Il termine *tecnologia* ha origine dal greco antico, dove "techne" significa "arte, abilità manuale" e "logos" significa "parola, studio"; insieme, "techne" e "logos" formano il termine *teknologia*, che significa "studio delle arti o delle abilità".

Come suggerisce la sua etimologia, il concetto di "tecnologia" ha subito un'evoluzione nel corso dei secoli: nell'antichità, la tecnologia era associata alla produzione di beni materiali, come la ceramica, il tessuto e le armi, e si basava principalmente sull'esperienza e sull'abilità pratica dei mestieri. Durante il Rinascimento, la tecnologia è diventata un campo di studio a sé stante, con la scoperta di nuove tecniche di produzione e l'introduzione di macchine e strumenti innovativi. Nel XIX secolo, con la rivoluzione industriale, la tecnologia è diventata un fattore trainante della crescita economica e dello sviluppo sociale.
Nel XX secolo, con la diffusione dell'elettricità, della radio e della televisione, la tecnologia ha avuto un impatto profondo sulla vita quotidiana delle persone. Negli ultimi decenni, l'avvento dell'informatica e delle tecnologie digitali ha cambiato radicalmente il modo in cui le persone lavorano, comunicano e si svagano.
Oggi, con il termine tecnologia ci si riferisce alla conoscenza, alle competenze e alle attrezzature, prevalentemente a sfondo informatico, utilizzate per creare, progettare, sviluppare, implementare e utilizzare soluzioni tecniche per risolvere problemi o soddisfare le esigenze dell'uomo.
È la forza motrice dell'innovazione e del progresso in moltissime aree, tra cui la salute, l'energia, l'ambiente, l'agricoltura, l'industria, la comunicazione e l'intrattenimento. La tecnologia sta anche trasformando l'industria manifatturiera, con la diffusione della robotica, dell'automazione e dell'Internet delle cose, che stanno ridefinendo i processi produttivi e la catena di approvvigionamento.

Lo sviluppo tecnologico ha avuto un impatto profondo e trasformativo sul mondo in cui viviamo, talmente ampio che risulta anche difficile da quantificare. Soprattutto negli ultimi anni ha avuto un andamento di crescita esponenziale dovuto a diversi fattori interconnessi tra di loro come l'innovazione nella scienza e nell'ingegneria, la creazione e la disponibilità di nuovi materiali, la crescita della potenza di elaborazione dei computer, la capacità di storage dei dati, il *network effect*[1], gli investimenti in R&D e molto altro ancora, portando effetti di crescita economica, creazione di nuove e numerose opportunità, migliorando la qualità della vita delle persone. In particolare, ha determinato una trasformazione progressiva di tutta una serie di attività umane che vengono svolte con l'ausilio di congegni sempre più sofisticati. Basti pensare all'impatto che l'Internet of Things[2] (IoT) ha avuto sulla vita delle persone.

[1] La crescente adozione di una tecnologia può creare un effetto a rete, in cui l'utilità di una tecnologia aumenta con l'aumento del numero di utenti che la utilizzano.
[2] L'Internet of Things (IoT) descrive la rete di oggetti fisici, ossia le "things", che hanno sensori, software e altre tecnologie integrate allo scopo di connettere e scambiare dati con altri dispositivi e sistemi su Internet; ad esempio, nelle *smart house*, in cui tutto il sistema "casa" è collegato ed automatizzato, ed è in grado quindi di migliorare la sicurezza e le funzionalità della propria abitazione e degli elettrodomestici utilizzati; una casa completamente automatizzata che l'utente è in grado di gestire semplicemente attraverso l'utilizzo del proprio smartphone.

Risulta evidente quindi, che nel momento storico in cui viviamo, le scoperte scientifiche e le invenzioni hanno scatenato un effetto sorprendente e trainante dell'evoluzione umana: dalla prima rivoluzione industriale (1750) segnata dall'adozione di macchine a vapore, alla seconda (1870) innescata dall'utilizzo del motore a scoppio e dell'elettricità, alla terza rivoluzione industriale (1950) legata all'introduzione dell'elettronica e dell'informatica nei processi produttivi. In particolare, quest'ultima conosciuta anche come "rivoluzione digitale" ha determinato un processo di trasformazione di informazioni analogiche in informazioni digitali (cioè informazioni utilizzabili dai computer) rendendo i dati più facilmente accessibili, gestibili e trasportabili.
È intuitivo che una *feature* del genere determini un impatto significativo sulla vita di un individuo, poiché ha reso possibile la creazione di nuovi servizi e prodotti senza precedenti. Alcuni esempi possono essere:
- internet banking
- e-commerce
- utilizzo di piattaforme online per l'erogazione di corsi di formazione
- utilizzo di piattaforme online per lo streaming di musica, film, gaming

Anche in ambito professionale, la digitalizzazione sta cambiando il modo in cui le aziende, sia pubbliche che private gestiscono i loro dati, migliorando l'efficienza e la velocità delle operazioni (anche grazie agli elaboratori sempre più performanti di cui si dispone), offrendo ai lavoratori nuove e numerose possibilità come l'utilizzo di
- software per la gestione delle attività e dei progetti
- software per la comunicazione tra colleghi
- machine learning
- accesso a registri elettronici
ecc.

E queste possibilità vanno di giorno in giorno moltiplicandosi grazie ai continui investimenti in campo di: internet of things, big data, cloud computing, robotica collaborativa, realtà aumentata e virtuale, stampa 3D, veicoli autonomi, nanotecnologia e biotecnologia, intelligenza artificiale etc.
Infatti, con queste nuove tecnologie e il repentino sviluppo dell'Internet of Things, il mondo reale si connette al mondo virtuale, in modo che tutti abbiano la possibilità (a patto che ci sia una connessione) di interagire con qualsiasi computer o più in generale sistema informatico. È un mondo in cui oggetti fisici e persone, così come dati e ambienti virtuali, interagiscono tra loro nello spazio e nel tempo. Questi oggetti possono ottenere e scambiare informazioni da diverse località geografiche in maniera eterogenea, generando, nel loro insieme, enormi quantità di dati, una vera e propria "data explosion".

Per cui, se da un lato lo sviluppo di tecnologie come il cloud, l'IoT, l'intelligenza artificiale e l'aumentare delle interconnessioni del mondo digitale offrono vantaggi sostanziosi in termini di efficienza e produttività, dall'altro lato vengono sviluppati metodi sempre più all'avanguardia per compiere attività non del tutto etiche: il fatto che ogni dispositivo contenga un'enorme quantità di dati e che ognuno di sia interconnesso con gli altri, rende irrimediabilmente tutto il sistema decisamente fragile: nel momento in cui anche solo uno dei dispositivi interconnessi non abbia sistemi di sicurezza di protezione dati adeguati, ogni informazione sensibile corre un grande rischio di diventare oggetto di cybercrimini, argomento che verrà specificato più approfonditamente in

Mediante l'elaborazione a basso costo, il cloud, i Big Data, gli analytics e le tecnologie mobile, gli elementi fisici possono condividere e raccogliere i dati con un intervento umano minimo. In questo mondo iperconnesso, i sistemi digitali possono registrare, monitorare e regolare ogni interazione tra gli oggetti connessi. Il mondo fisico incontra e coopera con il mondo digitale.

seguito.
In un contesto del genere, le questioni di cybersecurity diventano sempre più importanti per prevenire e limitare rischi che possono causare danni considerevoli. Questo argomento è diventato anche un pilastro fondamentale nello sviluppo della tecnologia di protezione, non solo per la sicurezza informatica, ma anche per tutti gli altri aspetti e settori dell'attività umana.

# Il cyberspazio

L'utilizzo di nuove tecnologie dell'informazione e della comunicazione presume un'interazione frequente con quello che viene identificato come ***cyberspazio***, termine che ha origine dalla parola greca "kyber" che vuol dire "navigare" e che non vuole identificare una dimensione oscura e incontrollabile dello spazio, bensì come un luogo effettivamente navigabile e gestibile. A plasmare questo termine così ricco di fascino fu lo scrittore canadese di fantascienza William Gibson nel 1984, nel suo romanzo *Neuromante*, in cui racconta di uno spazio digitale "navigabile da persone di realtà diverse che comunicano tra loro all'interno di un mondo computerizzato fatto di reti digitali". Più approfonditamente lo descrive come

"*Un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici...Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano...*".
(William Gibson, 1984)

Un tentativo di definizione più moderno potrebbe essere:

"*Il Cyberspace è un dominio globale e dinamico (soggetto a un cambiamento continuo) caratterizzato dall'uso combinato di uno spettro elettronico ed elettromagnetico, con lo scopo di creare, immagazzinare, modificare, scambiare, condividere ed estrarre, utilizzare, eliminare informazioni, gestire e compromettere beni fisici*".

In altre parole, questo mondo di reti digitali e computer è un nuovo fronte culturale ed economico, un mondo in cui multinazionali, corporazioni e pirati informatici si scontrano per conquistare dati e informazioni. Un vero e proprio nuovo "campo di battaglia" virtuale (il cosiddetto quinto dominio, dopo aria, terra, mare e spazio). È rappresentato da un ambiente virtuale che permette di accedere a tutte le informazioni raccolte nel database, permettendone lo scambio tra più utenti.
Come immaginava Gibson, il cyberspazio oggi è definito come un ambiente costituito da un'infrastruttura computerizzata, inclusi software, hardware, utenti, big data e tutte le interrelazioni che esistono tra loro. In particolare, l'Internet of Things, le reti di comunicazione e tutti quei dispositivi connessi caratterizzati da infinito e immaterialità fanno parte di questo ambiente.
Tuttora questi processi si realizzano e si moltiplicano in modo smisurato attraverso l'uso di internet che, da mezzo di interazione e condivisione, è diventato il centro operativo di gran parte delle operazioni politiche, sociali, economiche e commerciali.

L'accessibilità a basso costo e la sua pervasività rendono il cyberspazio il luogo ideale per la proliferazione (oltre che di cose belle) di minacce e attività criminali, come virus, clonazione di carte di credito, modifica di smart-card televisive e telefoniche, pornografia, cyberterrorismo, ecc…
Tutte queste attività vengono definite *cyber crime* e si distinguono dalle classiche attività criminali

poiché la vittima non riesce e/o non può percepire l'attacco fisicamente poiché la maggior parte di esse vengono realizzate nel *dark web*, la parte oscura di internet.

Per capire meglio questo concetto abbiamo bisogno di fare un po' di chiarezza sui vari tipi di web esistenti.
Per comprendere in modo più intuitivo, immaginiamo Internet come una grande città: come ogni metropoli, contiene spazi pubblici aperti a tutti, quali strade, viali e parchi, che troviamo sulla mappa e che sono facilmente accessibili a chiunque. Nel mondo di internet, questi spazi pubblici sono conosciuti come *surface web* ed è il luogo che ospita pagine web, applicazioni web e altri elementi che sono hostate in un server web e sono disponibili ad essere visualizzate e ricercate dai vari browser. Possono contenere documenti, file multimediali e altro che chiunque può trovare usando un motore di ricerca e visualizzare senza pagare, registrarsi o installare un software speciale.

Come in una grande di città le aree pubbliche sono solamente una piccola parte di essa ed allo stesso modo, nel web, questa parte superficiale comprende solamente circa il 4% dei contenuti a cui è realmente possibile avere accesso; infatti, oltre a queste aree pubbliche, esistono in città anche zone private le quali, per potervi accedere, richiedono un pass, un biglietto o un invito (come ad esempio case, club privati, cinema, ecc…) e che per l'appunto, non possono essere rappresentate su una mappa proprio perché private (su Maps non possiamo vedere l'interno di una casa di una persona X poiché essendo privata non è aperta al pubblico e quindi non vi si può accedere liberamente). In egual modo, anche il web presenta posti molto simili, angoli che i vari motori di ricerca come Google, Bing, ecc.… non hanno la possibilità di cercare o visitare, proprio perché presentano delle limitazioni (che possono essere ad esempio un abbonamento, una password o qualunque altro tipo di limitazione che non permetta ad un motore di ricerca di trovarlo). Proprio come una macchina di Google Street View non può entrare in un cortile privato, i bot di ricerca non possono imbattersi in contenuti senza link. Complessivamente, tali luoghi che non possono essere trovati ma ai quali vi si può comunque accedere, sono conosciuti come *deep web,* il quale viene spesso affiancato erroneamente a comportamenti criminosi o illegali: la maggior parte del deep web, infatti, è costituita da pagine web e documenti innocui, persino utili, che la maggior parte di noi usa e non c'è nulla di sbagliato se sono off-limit per gli estranei. Il termine deep web serve semplicemente per circoscrivere tutti quei contenuti per i quali non esistono link dal web visibile o di superficie. Un bot di ricerca semplicemente non sa che tali contenuti esistono; trova nuove pagine seguendo i link dalle pagine che ha già indicizzato.

Tornando alla nostra città, soprattutto nelle metropoli, esistono altri tipi di luoghi, loschi, bassifondi, covi, scelti per l'appunto per la loro mancanza di traffico e per la loro segretezza, luoghi ideali per nascondere attività non del tutto legali. Anche nel web esiste un posto simile ed è identificato con il nome di *dark web* ed è proprio il luogo in cui si verificano gli attacchi cyber. Questo dark web è composto dalle famose dark net, reti di accesso limitato i cui nodi (server, computer, router) sono invisibili non solo ai motori di ricerca ma, poiché sfruttano protocolli non standard per trasferire dati, anche alla maggior parte dei browser: né un collegamento diretto né una password permetteranno ad un utente normale di entrare. Gli strumenti utilizzabili per entrare in queste reti sono dei veri e propri protocolli di connessioni, predisposti per garantire la navigazione attraverso una rete parallela quasi impossibile da tracciare.

# Cos’è la cybersecurity?

Nel contesto altamente informatizzato in cui ci troviamo, nel quale siamo altamente dipendenti dalle tecnologie moderne e dove quest’ultime sono interconnesse, risulta evidente che i pericoli non sono pochi, e la sicurezza della privacy o più in generale la protezione dei dati sensibili del singolo individuo o dell’impresa che sia, sono questioni molto spigolose e che hanno sviluppato necessità anch’esse “informatizzate”: la cybersecurity è una di queste. Ma cos’è la cybersecurity?

Nel gennaio 2008 il presidente degli Stati Uniti d’America emana una direttiva presidenziale per la sicurezza nazionale (NSPD-54/HSPD-23), nella quale si definisce con il termine cybersecurity

“*Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation*”

Il termine cybersecurity (o in italiano cyber sicurezza) è l’insieme dei mezzi, delle tecnologie e delle procedure utili a proteggere i sistemi informatici in termini di disponibilità, riservatezza e integrità dei dati e degli asset informatici da minacce dannose come attacchi informatici e furto di dati. È spesso utilizzato come sinonimo di *Information Security* ma in realtà si tratta di una sottoclasse della Sicurezza Informatica.
La cybersecurity si focalizza, quindi, sugli aspetti legati alla sicurezza delle informazioni e pone l’accento sulle capacità di resilienza, robustezza e reattività che una tecnologia deve possedere per far fronte agli attacchi informatici che possono colpire chiunque (singoli individui, imprese private, enti pubblici e organizzazioni governative)

La sicurezza informativa si applica a vari contesti, dal business al mobile computing, e può essere suddivisa in diverse categorie.

- **Sicurezza di rete**: consiste nella difesa delle reti informatiche dalle azioni di malintenzionati, che si tratti di attacchi mirati o di malware opportunistico.
- **Sicurezza delle applicazioni**: ha lo scopo di proteggere software e dispositivi da eventuali minacce. Un'applicazione compromessa può consentire l'accesso ai dati che dovrebbe proteggere.
- **Sicurezza delle informazioni**: protegge l'integrità e la privacy di qualunque dato.
- **Sicurezza operativa**: è basata su processi e decisioni per la gestione e la protezione degli asset di dati. Comprende tutte le autorizzazioni utilizzate dagli utenti per accedere a una rete e le procedure che determinano come e dove possono essere memorizzati o condivisi i dati.
- **Disaster recovery e business continuity**: si tratta di strategie con le quali l'azienda reagisce ad un incidente di Cybersecurity. Le policy di disaster recovery indicano le procedure da utilizzare per ripristinare le operazioni e le informazioni dell'azienda, in modo da tornare alla stessa capacità operativa che presentava prima dell'evento. La business continuity è il piano adottato dall'azienda nel tentativo di operare senza determinate risorse.
- **Formazione degli utenti finali**: riguarda uno degli aspetti più importanti della Cybersecurity: le persone. Chiunque non rispetti le procedure di sicurezza rischia di introdurre accidentalmente un virus in un sistema altrimenti sicuro. Insegnare agli utenti a eliminare gli allegati e-mail sospetti, a non inserire unità USB non identificate e ad adottare altri accorgimenti importanti è essenziale per la sicurezza di qualunque azienda.

La maggior parte delle violazioni, imputabili a criminali malintenzionati, colpisce attività di ogni tipo, dai servizi medici ai rivenditori agli enti pubblici. Alcuni di questi settori sono particolarmente interessanti per i cybercriminali, che raccolgono dati medici e finanziari, ma tutte le aziende connesse in rete possono essere colpite da violazioni dei dati, spionaggio aziendale o attacchi ai clienti e a dimostrarlo sono i dati del Rapporto Clusit 2021 sulla sicurezza ICT in Italia e nel mondo, redatto dall'Associazione Italiana per la Sicurezza Informatica: solo nel 2020 sono stati registrati 1.871 gli attacchi gravi di dominio pubblico, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica.
Dallo studio emerge che nell'anno della pandemia da Covid-19, l'incremento degli attacchi cyber a livello globale ha fatto registrare un +12% rispetto al 2019 e un aumento degli attacchi gravi del 66% rispetto al 2017. Tra i settori maggiormente colpiti ci sono il "Multiple Targets" (20% del totale degli attacchi), che comprende attacchi realizzati verso molteplici obiettivi spesso indifferenziati, il settore Governativo, militare, forze dell'ordine e intelligence (14% del totale degli attacchi), la sanità, (12% del totale degli attacchi), la ricerca e istruzione (11% del totale degli attacchi) e i servizi online (10% del totale degli attacchi). Inoltre, sono cresciuti gli attacchi verso Banking & Finance (8%), produttori di tecnologie hardware e software (5%) e infrastrutture critiche (4%).

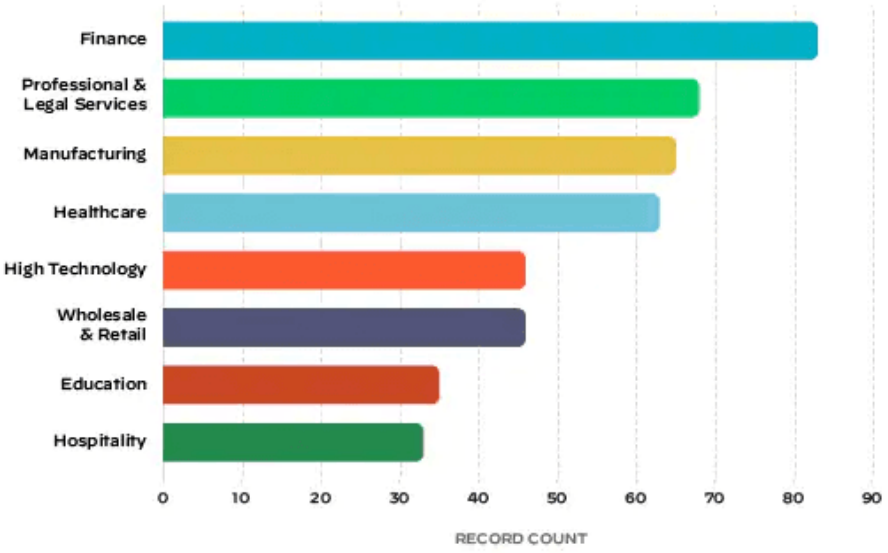



*Figura 1 - Settori più colpiti nell'anno 2021*

La sicurezza informatica è una sfida significativa e determinante, nel mondo contemporaneo, a causa della complessità dei sistemi informativi, sia in termini di utilizzo tecnologico che geopolitico ed economico. Il campo è diventato importante anche a causa della maggiore dipendenza delle attività quotidiane da sistemi informatici e Internet, nonché per la sempre maggiore diffusione di dispositivi "intelligenti" (smart) come telefoni, televisori e i vari dispositivi che costituiscono l'Internet delle cose (IoT) come ad esempio apparecchi medicali, auto, elettrodomestici e chissà che altro.

# Cyber crime e tipologie di attacchi informatici

A livello globale, le minacce informatiche continuano a evolversi rapidamente e il numero di data breach[3] aumenta ogni anno. Da un report di RiskBased Security emerge che, solo nel 2019, ben 7,9 miliardi di record sono stati esposti a data breach, più del doppio (112%) del numero dei record esposti nel 2018.

Nonostante i professionisti della sicurezza informatica lavorino duramente per colmare le lacune della sicurezza, gli aggressori sono sempre alla ricerca di nuovi modi per sfuggire all'attenzione dell'IT, aggirare le misure di difesa e sfruttare le debolezze emergenti. Le più recenti minacce alla sicurezza informatica stanno dando un nuovo senso alle minacce "conosciute", sfruttando gli ambienti per il lavoro da casa, gli strumenti di accesso remoto ed i nuovi servizi cloud.
Esistono tre tipologie di minacce principali

Il **Cyber crime** rappresenta tutte le attività illegali compiute nel cyber spazio, per interessi personali o a scopo di lucro, da parte di singoli individui o da organizzazioni criminali, il cui scopo primario è generalmente quello del raggiungimento di un profitto economico. Alcune delle attività illegali più utilizzate e conosciute sono le truffe telematiche, le frodi bancarie su Web o sulla rete mobile, e il ransomware ovvero la richiesta di un riscatto per restituire all'utente l'accesso ai propri dati che hanno subito un processo di crittografia totale da parte del virus informatico, rendendo impossibile l'accesso e il recupero delle informazioni memorizzate da parte della vittima dell'attacco. Soprattutto quest'ultimo in periodi recenti, si è candidato per diventare una delle tipologie di attacco preferite dai cyber criminali. Gli autori del ransomware contattano l'utente e, in cambio di denaro, forniscono il codice di sblocco e recupero dei propri dati.

Per **Cyber attivismo** si intende una nuova forma di resistenza "culturale e politica" portata avanti dalla comunità hacker. Questo tipo di attività è animata da motivi di natura sociopolitica o per finalità di protesta su particolari e specifiche tematiche socialmente rilevanti. Gli strumenti di attacco più utilizzati, in questo caso, sono il Distributed Denial of Service (DDoS), la raccolta illecita di dati personali (mediante attacchi di tipo APT) e diffusione di dati e di informazioni riservate (i c.d. Data breach e Data leaks). Appartiene al cyber attivismo anche l'attività di defacing ovvero l'intrusione non autorizzata nel sito web con modifica dei contenuti del sito.

Il **Cyber spionaggio**, invece, riguarda generalmente operazioni di intelligence che hanno come scopo primario quello di guadagnare l'accesso a informazioni riservate, sensibili e strategiche. È una forma di minaccia che si caratterizza per ampiezza e intensità variabili. Solitamente, precede le altre forme di cyber crime con intensità crescente e le accompagna sistematicamente, rendendo difficile stabilire una chiara distinzione tra queste categorie, e determinando, in ogni caso, danni finanziari o di reputazione – sia agli Stati colpiti che alle aziende - tali da causarne la potenziale esclusione dal mercato. Tra le operazioni che conducono le Nazioni nel cyberspace, le attività di spionaggio occupano senza dubbio un posto di rilievo. Le attività più frequenti vanno dalla raccolta di informazioni aziendali segrete, alle intercettazioni di comunicazioni telefoniche o telematiche, comunicazioni, messaggi, social network, ecc., Lo spionaggio naturalmente non nasce con l'avvento del mondo cyber ma è una pratica a cui ricorrono tutti i governi, da sempre, poiché è evidente l'interesse di qualunque Stato di poter disporre in anticipo di informazioni riservate su altre nazioni. L'informazione è potere e lo spionaggio costituisce uno degli strumenti più efficaci per ottenere vantaggi politici, militari ed economici nei confronti di Paesi ostili o anche amici o alleati, in periodi di pace così come in tempo di guerra. Un Governo può arrivare a supportare o a non ostacolare attività

[3] violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

illecite di cyber spionaggio nei confronti di industrie o aziende straniere, finalizzato alla sottrazione di segreti industriali o progetti tecnologicamente all'avanguardia e ciò allo scopo evidente di aumentare la competitività delle aziende nazionali a danno delle altre.

La **cyber warfare** è una vera guerra cibernetica e comprende tutte le attività ostili di cyber crime praticate da uno Stato nei confronti di un altro attraverso il cyber space. Appare, pertanto, evidente l'evoluzione che ha compiuto la minaccia cyber in questi ultimi anni, passando da tentativi imperfetti, condotti da una minoranza di esperti informatici, ad una forma coordinata di guerra tecnologica, supportata da Nazioni che la utilizzano come strumento strategico irrinunciabile per la competizione mondiale. Si realizza con il danneggiamento di sistemi informatici militari o industriali, di infrastrutture che assicurano la fornitura di servizi essenziali tipo l'energia elettrica, gas, acqua, servizi di telecomunicazioni, ecc. La terminologia utilizzata riporta direttamente alla natura dell'attacco; infatti, distinguere tra cyber warfare e cyber crime significa richiamare automaticamente un diverso aspetto (militare o criminale), un differente obiettivo perseguito (vantaggi strategici o obiettivi monetari) e una diversa tipologia di agente (eserciti nazionali o organizzazioni criminali).

Devono infine menzionarsi le attività illegali rientranti nel **cyber terrorismo** che include alcuni dei concetti sopra esposti, ma che ha proprie caratteristiche e connotazioni. infatti, il terrorismo digitale ha alcuni importanti vantaggi rispetto al terrorismo "tradizionale" come l'anonimità, economicità e la distanza fisica dall'obiettivo, la cui ininfluenza, non può rappresentare un ostacolo al successo dell'attacco né un effetto deterrente per l'esecutore dell'attacco. Una chiara definizione di cyber-terrorismo è stata data dall'US National Infrastructure Protection Center (NIPC), come

"A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda".

Le principali attività e le specifiche tecniche di attacco poste in essere dalle comunità criminali sono elencate nella seguente tabella:

| Tipologia di attacco | Descrizione |
|---|---|
| **Virus** | Malware che una volta attivato è in grado di replicarsi e infettare sistemi operativi, file e singoli documenti |
| **Worm** | Malware auto-replicabile in grado di auto-propagarsi e infettare tutti i sistemi connessi su una stessa rete |
| **Phishing Spear-phishing** | Malware contenuto in e-mail che sembrano provenire da soggetti conosciuti e che rubano password e informazioni finanziarie |
| **Attacco brute force** | Attacco capace di "craccare" le password generando ad altissima velocità tutte le possibili combinazioni di chiavi per aprire file protetti |
| **Cross-site scripting (XSS)** | Inclusione di codice html all'interno di una pagina web per effettuare operazioni malevoli quali prelievo di cookies privati |
| **SQL injection** | Tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che vengano eseguiti |
| **Trojan** | Malware impiegato per effettuare intercettazioni, rubare informazioni sensibili ed effettuare operazioni sui sistemi |

| | |
|---|---|
| **Vulnerabilità 0 Day** | Vulnerabilità di applicazioni non ancora divulgate o per le quali non è ancora stata distribuita una patch |
| **Exploit** | Esecuzione di codice malevolo che sfrutta una o più vulnerabilità con lo scopo di acquisire privilegi amministrativi |
| **Keylogger** | Strumento in grado di intercettare, in forma nascosta, le digitazioni effettuate sulla tastiera del dispositivo |
| **DDoS** | Attacco mirato a rendere indisponibile un servizio mediante un sovraccarico di richieste verso il sistema target |
| **APT (Advanced Persistent Threat)** | Attacco di difficile identificazione finalizzato a guadagnare punti di accesso a una rete per un lungo periodo di tempo |
| **Botnet** | Rete di computer "zombie" infettati da un malware e controllati in via remota e nascosta da un attaccante |
| **Spam** | Comunicazioni indesiderate e ripetute da parte di mittenti sconosciuti usati anche per diffondere malware |

*Tabella 1 - Tipologie principali di attacchi*

Il cybercrime è notevolmente aumentato negli ultimi anni ed è in continua crescita, giungendo a diventare la terza attività criminale per impatto sul prodotto interno lordo mondiale (0,8%) dietro solo alla corruzione governativa (1,2 %) e al traffico di droga (0,89%) (Hale, 2018) poiché per via delle sue caratteristiche intrinseche che lo rendono di fatto uno strumento super efficace per i cyber criminali poiché non presenta (quasi) nessun fattore avverso: è una forma di reato gratificante, facilmente attuabile e con scarse probabilità di cattura.

Le ragioni della crescita di questo tipo di crimine sono le seguenti (Lewis, 2018):

• adozione rapida di nuove tecnologie da parte dei criminali informatici;

forma di reato facilmente attuabile e con scarse probabilità di cattura;

• aumento del numero di nuovi utenti online (provenienti da paesi a basso reddito con debole sicurezza informatica);

• maggior facilità nel commettere crimini informatici, con la crescita del cyber crime come servizio;

• numero sempre più crescente di "centri" di criminalità informatica che ora includono Brasile, India, Corea del Nord e Vietnam;

• crescente sofisticazione finanziaria tra gli alti livelli di criminalità informatica che, rende la monetizzazione più semplice.

La monetizzazione dei dati rubati infatti è sempre stato uno dei problemi più grandi da risolvere e mai come negli ultimi anni lo è sempre meno, a causa dei miglioramenti nel mercato nero e grazie all'uso delle valute digitali. All'interno del dark web vengono offerti in gran quantità numeri di carte di credito e informazioni di identificazione personale (PII) utilizzando una serie complessa di transazioni che coinvolgono broker e altri intermediari, in tal modo il furto finanziario viene in seguito trasferito sui conti bancari dei criminali attraverso transazioni destinate a mascherare e confondere. Tale facilità sussiste in relazione alle scarse misure di protezione adottate dalla maggior parte degli utenti, anche quelle più elementari, inoltre numerosi prodotti tecnologici non sono dotati di difese adeguate. Al contrario, i criminali informatici utilizzano una tecnologia avanzata finalizzata a identificare gli obiettivi, creano e consegnano automaticamente software e monetizzano ciò che è stato rubato.

# Episodi principali di attacchi cyber

Uno degli episodi più importanti di hackeraggio è stato il **WannaCry ransomware attack** del 2017. Questo attacco ha colpito oltre 200,000 computer in 150 paesi, bloccando i dati degli utenti e chiedendo un riscatto in bitcoin per il loro rilascio. Le vittime includevano aziende, governi e organizzazioni sanitarie, causando danni per milioni di dollari. È stato scoperto che l'attacco è stato effettuato utilizzando una vulnerabilità nei sistemi Microsoft Windows, che era stata precedentemente sfruttata dalla NSA americana. Questo episodio ha evidenziato la gravità dei pericoli della cyber-sicurezza e la necessità di sviluppare e mantenere sistemi di sicurezza più robusti

Un altro episodio importante di hackeraggio è stato l'attacco **SolarWinds del 2020**. Questo attacco è stato effettuato da un gruppo di hacker sofisticato e ha colpito oltre 18.000 clienti di SolarWinds, un'azienda che fornisce software di monitoraggio delle prestazioni IT. Gli hacker sono riusciti ad inserire un malware all'interno del software di SolarWinds, che ha permesso loro di accedere ai sistemi IT delle vittime e ai loro dati sensibili. Questo attacco ha avuto un impatto significativo su molte organizzazioni governative e private, tra cui il dipartimento di Stato degli Stati Uniti, il Dipartimento della Difesa e le agenzie di intelligence. Questo episodio ha evidenziato la necessità di aumentare la sicurezza delle supply chain tecnologiche e di migliorare la capacità di rilevare e rispondere a questo tipo di attacchi sofisticati.

Un altro episodio di hackeraggio significativo è stato l'attacco alle centrali **nucleari iraniane nel 2010**, noto come Stuxnet. Questo attacco è stato effettuato utilizzando un worm informatico che ha infettato i sistemi di controllo industriale delle centrali nucleari iraniane, causando danni ai loro processi di produzione di energia. Questo attacco è stato condotto da un gruppo di attori sofisticati e ha rappresentato una delle prime volte in cui un attacco informatico è stato utilizzato per causare danni fisici a un sistema. Stuxnet ha anche dimostrato la vulnerabilità dei sistemi di controllo industriale e ha sollevato preoccupazioni sulla sicurezza delle infrastrutture critiche. Questo episodio ha reso evidente la necessità di sviluppare sistemi di sicurezza informatica più robusti per proteggere contro questo tipo di attacchi.

**L'Operazione Shady Rat** è stata una delle più grandi campagne di hacking di massa condotte su larga scala e che ha colpito organizzazioni in tutto il mondo. Il nome "Shady Rat" fa riferimento alla specie di topi (rat in inglese) usata come metafora per descrivere gli hacker che hanno effettuato l'attacco. La campagna è stata scoperta nel 2011 da McAfee, una società di sicurezza informatica, che ha identificato una serie di intrusioni informatiche che hanno colpito organizzazioni di tutto il mondo, tra cui governi, organizzazioni non governative, aziende e università. Gli attacchi erano mirati e hanno utilizzato tecniche avanzate di phishing e di intrusione per infiltrarsi nei sistemi delle vittime e rubare informazioni sensibili. Tra le informazioni rubate c'erano dati sulle relazioni commerciali, informazioni sulle transazioni finanziarie, informazioni sulle operazioni militari e sulla ricerca e sviluppo.
Non è stato reso noto chi fosse responsabile dell'attacco, ma molte fonti sostengono che l'Operazione Shady Rat potrebbe essere stata condotta da un gruppo di hacker basato in Asia. L'Operazione Shady Rat ha messo in evidenza la necessità di una maggiore attenzione alla sicurezza informatica a livello globale e ha dimostrato che anche le organizzazioni più grandi e ben protette possono essere vulnerabili a intrusioni informatiche sofisticate.

# Capitolo 2

## Mercato globale della Cybersecurity

Il mercato della cybersecurity è in rapida crescita e rappresenta un settore in forte evoluzione. La crescente quantità di dati sensibili e la diffusione di attacchi informatici stanno spingendo le aziende e i governi a investire sempre di più in soluzioni di sicurezza informatica.

Si prevede che le dimensioni del mercato globale della sicurezza informatica cresceranno fino a raggiungere i 345,4 miliardi di dollari entro il 2026.

Difatti, la crescente consapevolezza delle minacce informatiche sta portando l'industria della Cybersecurity ad attirare sempre più investimenti, con un aumento delle fusioni e acquisizioni e del finanziamento di venture capital.

In un'era all'insegna della digitalizzazione, in cui tutto si connette, la sicurezza informatica appare sempre più una un'esigenza e un'urgenza.

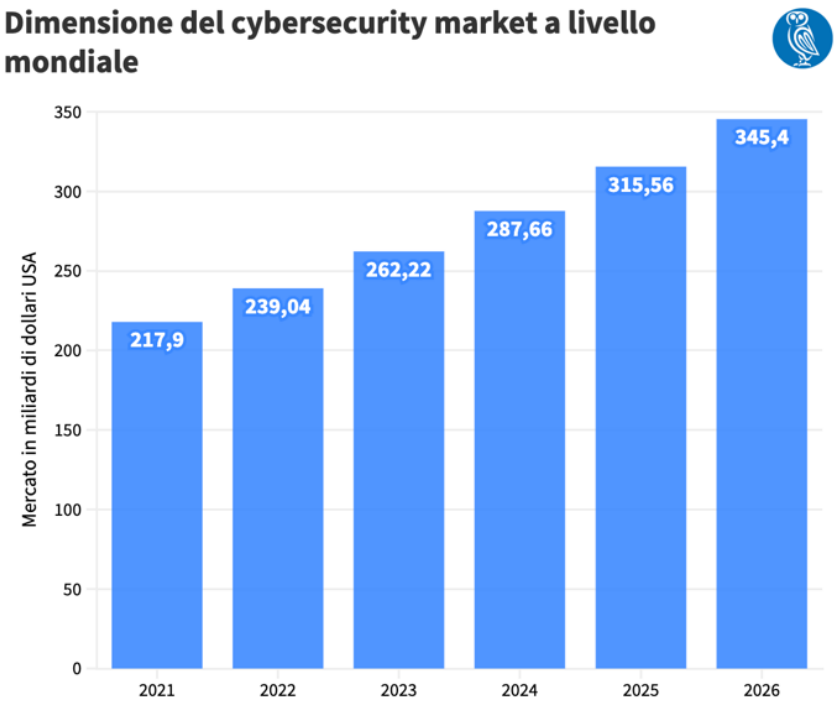
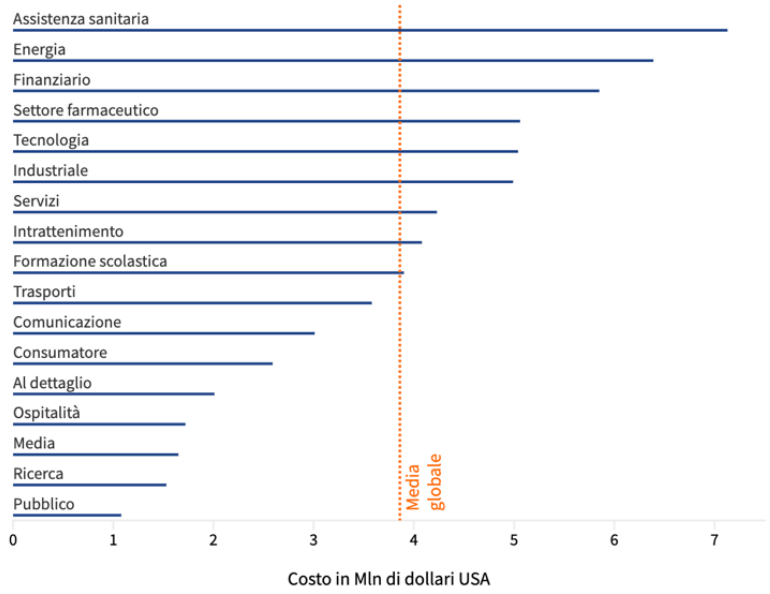



*Figura 2 - Dimensione del mercato*

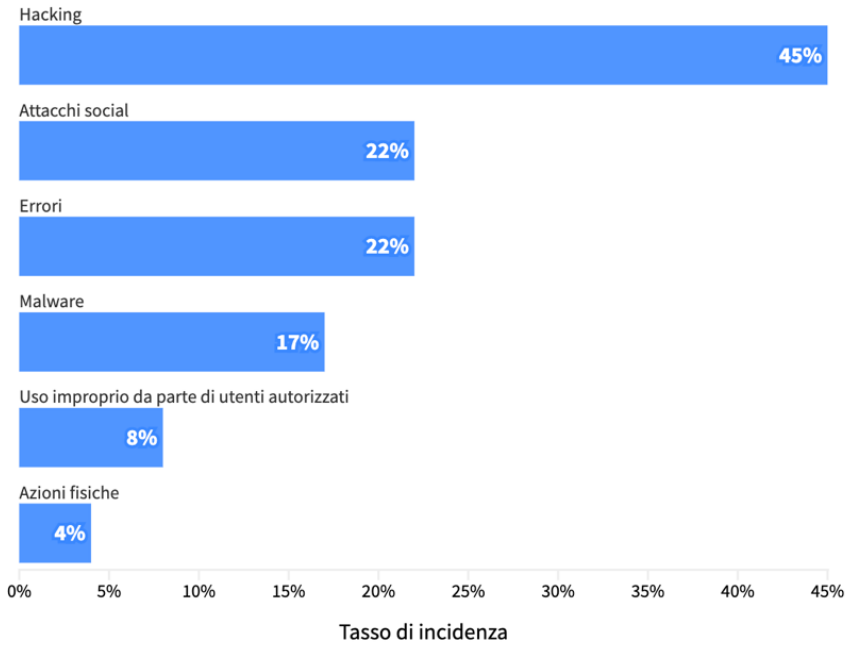
Secondo un'indagine per settore condotta da Statista, nel 2020 il costo medio di una violazione dei dati nel comparto sanitario ammontava a 7,13 milioni di dollari, contro un costo medio globale di una violazione di 3,86 milioni di dollari. Seguono il settore energetico (6,39 Mln) e il ramo finanziario (5,85 Mln). Le violazioni dei dati nel settore pubblico si sono classificate all'ultimo posto, con un costo medio di 1,08 milioni di dollari.




Fonte: Statista, Ponemon Institute • Dati da agosto 2019 ad aprile 2020; 524 organizzazioni

*Figura 3 - Costo medio violazioni nel mondo*

Varie risultano essere anche le tipologie di violazioni dei dati. In particolare, nel 2019 il 45% delle violazioni dei dati globali ha riguardato l'hacking. Attacchi social ed errori conquistano invece un pareggio al secondo posto (22%). È altresì doveroso precisare che la maggior parte delle violazioni è stata perpetrata da attori esterni.

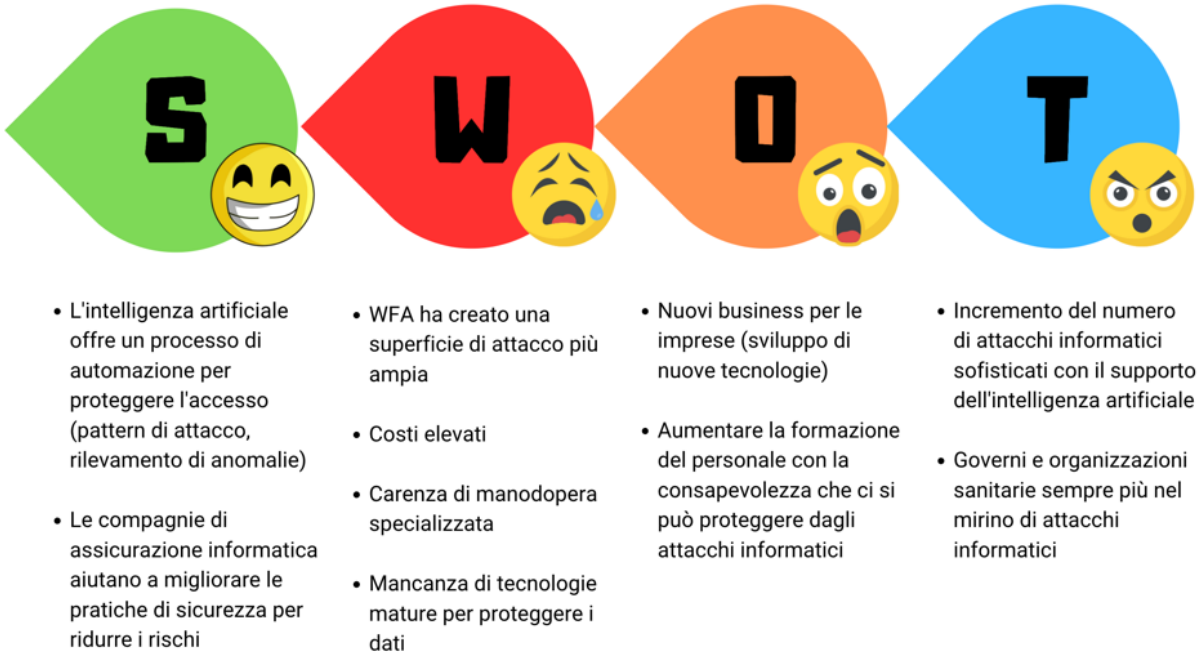



Fonte: Statista • Dati 2019

*Figura 4 - Azioni più comuni nelle violazioni di dati*

## Analisi del settore della Cybersecurity

Per comprendere meglio quanto sia importante per le aziende proteggersi dagli attacchi informatici è importante andare ad effettuare un'Analisi SWOT (Strengths, Weaknesses, Opportunities, Threats):




### Punti di forza (*Strengths*)

Nel 2022, l'innovazione nella sicurezza informatica ha rafforzato il mercato e offerto soluzioni affidabili per aziende e organizzazioni.
I modelli di rilevamento potenziati dall'apprendimento automatico sono ora necessari per efficaci difese della sicurezza informatica.
I modelli di rilevamento basati su ML sono ampiamente utilizzati nell'identificazione e prevenzione del malware (Endpoint Protection Detection & Response systems), nella prevenzione delle intrusioni di rete (Network Detection & Response tools) e nell'analisi del comportamento degli utenti; possono, inoltre, ottimizzare i flussi di lavoro dei team di sicurezza informatica.
Sul lato Identity and Access Management (IAM), le tecnologie biometriche hanno ottenuto l'accettazione e sono diventate ampiamente utilizzate. Questa tecnologia riconosce gli utenti in base alle loro caratteristiche biologiche, come impronte digitali, riconoscimento facciale e analisi comportamentale. Si tratta di progressi significativi che aiutano a proteggere le risorse delle organizzazioni.
A causa del crescente numero di attacchi informatici, le compagnie assicurative hanno colto l'opportunità di avviare e offrire polizze assicurative informatiche. Sebbene l'assicurazione informatica non fornisca di per sé mitigazioni tecniche, tali polizze possono ridurre al minimo l'impatto finanziario in caso di attacchi informatici o fughe di dati. Inoltre, i clienti devono soddisfare determinati requisiti tecnici per acquisire una polizza assicurativa e le compagnie assicurative forniscono indicazioni alle organizzazioni, il che porta a una migliore postura di sicurezza e all'uso delle migliori pratiche nella sicurezza informatica.

### Debolezze (*Weaknesses*)

Il COVID-19 ha cambiato la realtà quotidiana di molti lavoratori, portando alla democratizzazione del concetto di "Work From Anywhere" (WFA). La protezione delle apparecchiature di dipendenti al di fuori dell'ufficio è una sfida per i team di sicurezza informatica.

Errori umani, reti e sistemi vulnerabili, così come la mancanza di formazione, contribuiscono ad aumentare la superficie di attacco.

Tuttavia, ci sono alcune opzioni per massimizzare la protezione, come l'uso di VPN. Purtroppo, tali soluzioni non sono gratuite e quindi portano le aziende ad affrontare crescenti costi di sicurezza informatica.

Inoltre, l'implementazione di soluzioni è difficile per le organizzazioni a causa della carenza di professionisti della sicurezza informatica in tutto il mondo. Alcuni massicci attacchi informatici si sono verificati a causa dell'insufficienza delle risorse tecniche e umane disponibili per implementare e mantenere l'infrastruttura di sicurezza e rispondere agli incidenti di sicurezza. Ciò ha costretto alcune aziende a cercare personale qualificato nelle più disparate località del mondo.

### Opportunità (*Opportunities*)

Il crescente utilizzo di tecnologie emergenti come IoT e cloud computing sta aumentando la domanda di soluzioni di sicurezza informatica, aprendo nuove opportunità di business per le imprese.

Zero Trust Architecture (ZTA) è un concetto che è stato istanziato in molti prodotti. Non esiste un singolo prodotto che fornisca ZTA completo, ma sono disponibili molti prodotti che possono consentire alle organizzazioni di assemblare solide difese che incorporano ZTA.

Anche nel settore IAM, le soluzioni di autenticazione senza password possono ridurre il rischio di phishing e compromissione delle credenziali migliorando al contempo l'esperienza dell'utente. Questa soluzione sta iniziando a essere sempre più ampiamente accettata poiché le password tradizionali fanno fatica a rispondere a un panorama delle minacce in rapida evoluzione.

Infine, le soluzioni SASE (Secure Access Service Edge) mirano a consolidare prodotti e servizi di sicurezza e networking per aiutare le organizzazioni ad affrontare le sfide del WFA e della connettività delle strutture remote.

Gli attacchi di phishing sono diffusi e sempre più difficili da distinguere dalle comunicazioni legittime. Gli aggressori utilizzano le informazioni pubblicamente disponibili per creare con cura messaggi che sembrano autentici. Alcune organizzazioni utilizzano parole in codice antiquate che vengono condivise solo di persona e che possono essere successivamente utilizzate per autenticare ordini sospetti.

### Minacce (*Threats*)

Gli attacchi informatici stanno diventando sempre più sofisticati e complessi, rappresentando una minaccia per le soluzioni di sicurezza informatica esistenti.

In particolare, sia i Governi che le organizzazioni sanitarie sono ormai vittime di un numero sempre crescente di attacchi informatici.

Risulta molto utile dare anche uno sguardo, per effettuare un'analisi più completa, a quella che risulta essere la competitività all'interno del settore della Cybersecurity.
A tal proposito ci serviamo del *Modello delle 5 Forze di Porter*:


### Concorrenza Interna (*Rivalry*)

L'intensità della concorrenza nel mercato della cybersecurity è elevata. Ci sono poche grandi imprese che detengono una quota significativa del mercato, tra cui Symantec, McAfee, TrendMicro, Kaspersky e NortonLifeLock. Tuttavia, ci sono anche molte imprese più piccole e start-up innovative che offrono soluzioni di sicurezza informatica. Inoltre, la concorrenza è intensificata dalla continua evoluzione tecnologica, che richiede alle imprese di mantenere il passo con i cambiamenti del mercato per rimanere competitive.

### Minaccia dei Nuovi Entranti (*New Entrants*)

La minaccia di nuovi entranti nel mercato della cybersecurity è moderatamente bassa. La creazione di una nuova impresa di sicurezza informatica richiede un'elevata specializzazione tecnica, una conoscenza approfondita del settore e notevoli investimenti in R&D. Inoltre, l'alto livello di consolidamento del mercato, con poche grandi imprese che detengono una quota di mercato significativa, rende difficile l'ingresso di nuovi player.

### Servizi Sostituti (*Substitutes*)

La minaccia di prodotti o servizi sostitutivi nel mercato della cybersecurity è moderatamente alta. Le soluzioni di sicurezza informatica sono essenziali per proteggere le informazioni e i dati sensibili, tuttavia, l'evoluzione tecnologica potrebbe portare alla creazione di nuove soluzioni che offrono una maggiore sicurezza e un costo inferiore.

### Potere contrattuale dei Clienti (Buyers)

Il potere contrattuale dei clienti nel mercato della cybersecurity è elevato. Le imprese di sicurezza informatica dipendono dai clienti per acquistare i loro prodotti e servizi. I clienti, a loro volta, possono scegliere tra una vasta gamma di fornitori di soluzioni di sicurezza informatica, il che può esercitare una pressione sui prezzi e sulle condizioni di contratto.

### Potere contrattuale dei Fornitori (*Suppliers*)

Il potere contrattuale dei fornitori nel mercato della cybersecurity è moderato. Le aziende di sicurezza informatica dipendono da fornitori di tecnologia, di servizi di cloud computing e di componenti hardware, ma questi fornitori hanno molte alternative tra cui scegliere. Inoltre, le grandi imprese di sicurezza informatica possono sviluppare soluzioni in-house, riducendo la dipendenza dai fornitori.

## Mercato italiano della Cybersecurity

Il mercato della cyber security in Italia è in crescita, ma ancora relativamente piccolo rispetto ad altri paesi europei come Germania, Regno Unito e Francia.

In Italia, tra il 2015 e il 2020, la dimensione del mercato della cybersecurity è passata da 728,2 milioni a 1.238,5 milioni di euro. Queste cifre rispecchiano lo sviluppo nei settori dell'hardware e software di sicurezza, consulenza, formazione, integrazione di sistemi, MSS e servizi cloud.

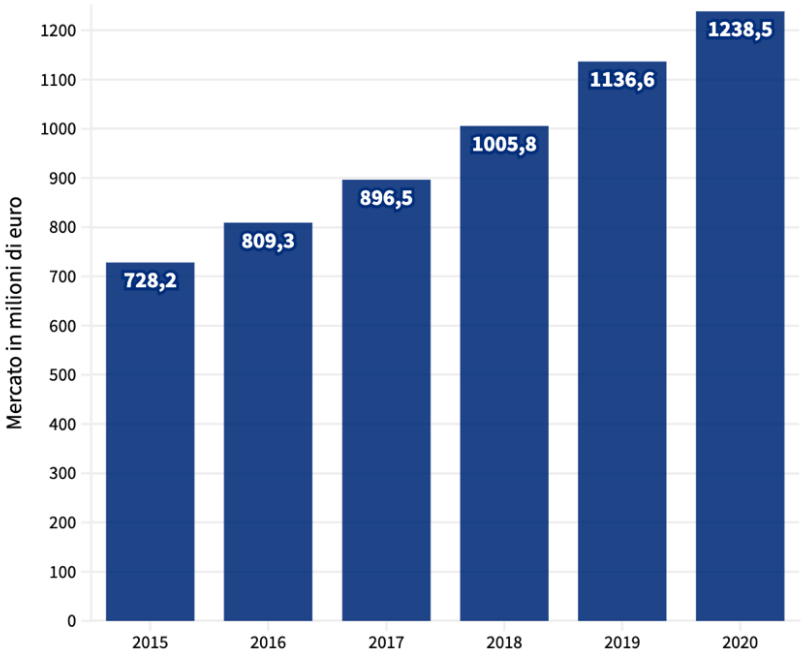



*Figura 5 - Dimensione del mercato italiano*

Oltre a ciò, secondo gli ultimi dati disponibili, il 22,73% delle aziende con 10-50 dipendenti, con 251-1000 dipendenti e con 1001-5000 dipendenti hanno subito più di dieci attacchi informatici in un anno. Tuttavia, la questione riguarda anche le realtà più piccole. Infatti, circa il 23% delle aziende con meno di 10 dipendenti ha subito almeno una volta un attacco informatico.

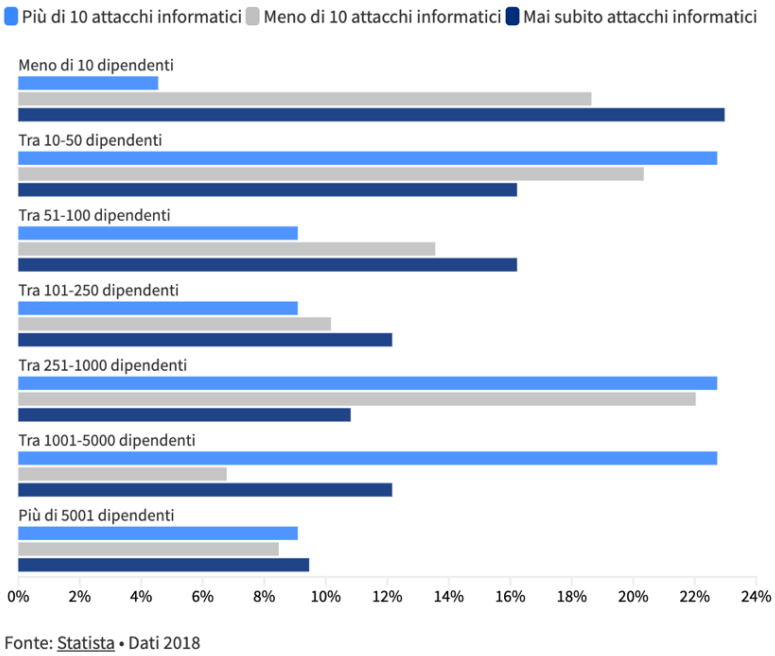



*Figura 6 - Numero attacchi informatici nelle imprese italiane*

Assodata non solo l'esistenza, ma anche la pericolosità della questione, un'indagine svolta da Statista, sulla quota di aziende ed enti che hanno una copertura assicurativa contro i rischi ICT ha svelato che circa il 35% degli intervistati non ha alcuna assicurazione, il 17,5% non sa cosa fare o ignora la questione, il 17,5% ha pianificato di assicurarsi in futuro, mentre il 30% è già coperto. Il fatto che più della metà del campione intervistato non sia assicurato o ignori il problema della cybersecurity e che solamente il 30% sia protetto non solo è allarmante, ma è anche indice della scarsa informazione circa il tema.

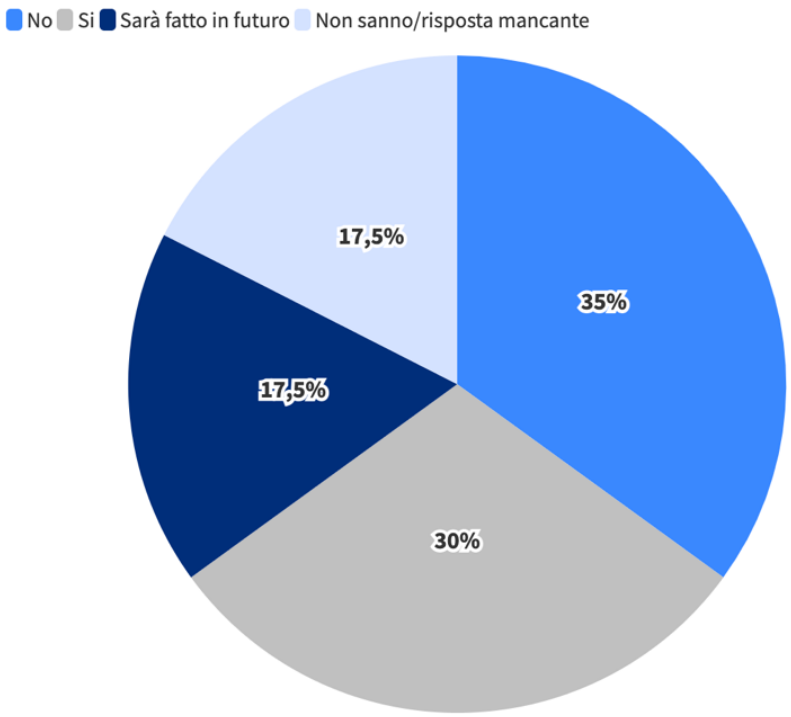



*Figura 7 - Imprese con coperture assicurative contro i rischi ICT*

Alla luce dell'analisi dei dati riportati, si dimostra giustificata e anzi, forse non ancora sufficiente, la crescita del mercato della cybersecurity.
La consapevolezza dell'importanza della sicurezza informatica sta aumentando in Italia nonostante sia un contesto nuovo, dinamico e in continuo aggiornamento. Sarà un mercato da esplorare e sicuramente redditizio per le imprese, sebbene lontano dal punto di massima espansione.

## Aspettative nel 2023

Non possiamo prevedere il futuro, ma una certezza rimane: il numero di attacchi informatici continuerà ad aumentare nel 2023. Anche i costi degli attacchi informatici aumenteranno a causa di diversi fattori: inflazione mondiale, crisi energetica, conflitti geopolitici ed espansione delle organizzazioni. D'altra parte, le crisi a volte possono essere viste come opportunità, portando i fornitori di sicurezza a innovare per fornire prodotti e servizi migliori. Inoltre, le organizzazioni richiederanno soluzioni nuove e più potenti per affrontare gli attacchi informatici e ridurre i rischi.

In primo luogo, ci sarà una maggiore attenzione alle tecnologie di rilevamento e prevenzione delle minacce. Le aziende potranno avvalersi di tecnologie avanzate come l'analisi dei comportamenti, l'intelligenza artificiale e l'apprendimento automatico per rilevare e prevenire le minacce in modo tempestivo. Queste tecnologie saranno fondamentali per proteggere le reti aziendali dai cyber attacchi.
Inoltre, le aziende inizieranno a fare investimenti significativi nella gestione dei dati. Ciò comprenderà l'implementazione di una forte strategia di gestione dei dati che preveda la crittografia, la conservazione e l'archiviazione sicure, nonché l'utilizzo di tecnologie avanzate come la blockchain.
Infine, vedremo l'adozione di una cultura della sicurezza informatica che incoraggi la consapevolezza dei rischi e la responsabilizzazione dei dipendenti. Ciò comprenderà anche la formazione dei dipendenti su come riconoscere e affrontare le minacce informatiche e come prevenire gli incidenti di sicurezza.
In conclusione, la cybersecurity sarà una componente fondamentale delle strategie aziendali nel 2023. Le aziende dovranno prendere il controllo dei loro dati e adottare le tecnologie più avanzate per garantire una protezione adeguata. Inoltre, dovranno adottare una cultura della sicurezza informatica che incoraggi la consapevolezza dei rischi e la responsabilizzazione dei dipendenti".

# Capitolo 3

## Premessa

Per l'analisi del settore di mercato della cybersecurity in Italia si è scelto di andare a considerare solo ed esclusivamente quelle società che operano entro i confini del territorio italiano (escludendo quindi tutti i player internazionali) e che abbiano sede legale in Italia.
Inizialmente, per quanto concerne la raccolta dei dati, si è utilizzato il portale AIDA che attraverso lo sfruttamento di alcuni filtri ha permesso di individuare le aziende che hanno un ruolo attivo nel mercato di riferimento e successivamente, tramite l'analisi dei bilanci che la piattaforma ha fornito, si è riusciti a condurre un'indagine a tutto tondo.
È importante sottolineare però che l'analisi è stata condotta dal punto di vista di un *outsider* poiché è per l'appunto basata solamente sui bilanci pubblici civilistici, sprovvista quindi della possibilità di accesso alle informazioni interne alle aziende stesse.

La fase iniziale dell'analisi prevede una riclassificazione di alcuni dei documenti che compongono il bilancio (Stato Patrimoniale e Conto Economico) in modo da poterlo scomporre e riaggregare nelle modalità più congeniali all'analisi in atto.

Nello specifico, l'esplorazione dello SP ha comportato 3 diversi tipi di riclassificazione:
- riclassificazione per natura che ha l'obiettivo di aggrega le voci di Stato Patrimoniale in reali e finanziarie per quanto riguarda l'attivo e in patrimonio netto, debiti e fondi per quanto riguarda il passivo.
- riclassificazione per destinazione nella quale si aggregano le voci dell'attivo e del passivo secondo la durata, distinguendo quindi le voci a breve termine da quelle a lungo termine
- riclassificazione per tipologia di attività svolta che invece aggrega le attività in operative e finanziarie, mentre le passività in operative circolanti e finanziarie.

Diversamente, per quanto riguarda il Conto Economico, è stato possibile solamente procedere con un solo tipo di riclassificazione, quella al valore aggiunto nella quale il profitto sarà ripartito tra diverse aree gestionali, quella operativa e quella finanziaria. Non verranno trattate le altre due tipologie di riclassificazione (al margine del venduto e al costo del venduto) poiché come detto in precedenza, ricoprendo il ruolo di analisti esterni, non si ha la possibilità di derivare la totalità dei dati necessari dal bilancio civilistico per condurre un'analisi di questo tipo.

Una volta completata questa fase si è passati al calcolo degli indici di bilancio e all'analisi economico-finanziaria del settore.

Durante l'analisi sono state assunte alcune approssimazioni a causa della tipologia dei dati forniti da AIDA: i bilanci forniti dal database presentano solamente degli aggregati delle voci dei bilanci, senza quindi andare a specificare la natura o la tipologia della voce.
In particolare, nel caso della riclassificazione del CE si è resa necessaria la deduzione di alcune voci che nel bilancio civilistico fanno parte del "COSTO TOTALE DI PRODUZIONE" e che in una riclassificazione vengono scomposte andando ad alimentare impieghi diversi. Ad esempio, per quanto riguarda le voci "accantonamenti" e "variazioni materie prime" per i motivi sopra elencati si è reso necessario aggregarle e approssimarle considerando il tutto come "accantonamenti". Questo perché sicuramente le aziende che presentano un ebitda negativo avranno avuto una variazione

positiva di consumo di materie prime che nel caso specifico sarebbero andate a gonfiare l'ebitda (data la loro applicazione cronologicamente precedente a quella degli accantonamenti) e che avrebbero restituito un valore molto diverso e di conseguenza degli indici molto diversi.

Altre approssimazioni riguardano la natura dei debiti e dei crediti: non è stato specificato se si trattasse di debiti commerciali, finanziari o tributari e di crediti a breve o lungo termine, sempre per i motivi sopra citati.
Inoltre, si è scelto di considerare solamente quelle aziende che presentassero a seguito delle riclassificazioni varie un EBITDA positivo o che quanto meno non sia influenzato troppo negativamente dalla mancata specificazione delle macro-voci.

## Scelta del campione

Le aziende fornite dal database AIDA sono state individuate inizialmente utilizzando le *keywords* "cybersecurity" e "sicurezza informatica" per il periodo di tempo che va dal 2017 al 2021. Il risultato di questa ricerca ha prodotto un elenco di 339 imprese. Non tutte però sono state prese in considerazione nello svolgimento dell'analisi poiché non presentavano le caratteristiche adeguate a essere annoverate come operanti nel settore target: infatti molte di esse, come ad esempio "BLUE REPLY S.R.L." o "MAUDEN S.R.L.", generano la quasi totalità dei propri profitti attraverso attività come commercio all'ingrosso di computer, apparecchiature informatiche periferiche e di software o installazione di impianti elettronici, o ancora come fabbricazione di apparecchi elettromedicali, attività in qualche modo legate all'ambito informatico, ma distanti dal più specifico mercato della cybersecurity.

Detto ciò, per la costruzione del campione di riferimento si è preferito scegliere solamente quelle aziende la cui maggior parte degli utili fosse prodotta da attività strettamente collegate a servizi puramente di sicurezza informatica, relativi quindi alla protezione dei dati e della privacy.

A questo proposito, il driver per la selezione delle imprese è stato quello della classificazione ATECO, una combinazione alfanumerica che identifica le attività economiche.
In particolare, si è scelto di considerare solamente le aziende che rispondessero ai seguenti codici:

- ATECO 62.01.00 - Produzione di software non connesso all'edizione

- ATECO 62.02.00 - Consulenza nel settore delle tecnologie dell'informatica

- ATECO 63.11.30 - Hosting e fornitura di servizi applicativi (ASP)

In più sono state prese in considerazione solamente le imprese che presentassero un valore dell'attivo disponibile maggiore di 1000 euro e un valore maggiore di 0 per quanto concerne le voci di Produzione Lorda, Patrimonio Netto e Capitale Sociale, in modo da capire la popolazione di imprese che effettivamente operano nel panorama italiano.

Questo screening ha prodotto un elenco di 123 aziende attive nel settore, nel periodo di tempo che intercorre tra il 2017 e il 2021; l'arco temporale scelto è quindi abbastanza ampio per poter comprendere l'andamento e l'evoluzione dei principali driver dell'analisi e abbastanza recente da poter rappresentare in modo affidabile la situazione economica in cui versa il settore.
Non tutte le imprese presentano dei bilanci completi nel quinquennio, chi per motivi di nascita recente chi per cause di fallimento o liquidazione. Per ovviare a questo inconveniente, sono state considerate solamente le imprese che presentassero per almeno 4 anni bilanci completi.

Da questo punto in poi il campione utilizzato sarà quello formato dalle imprese che rispettano i vincoli precedenti.

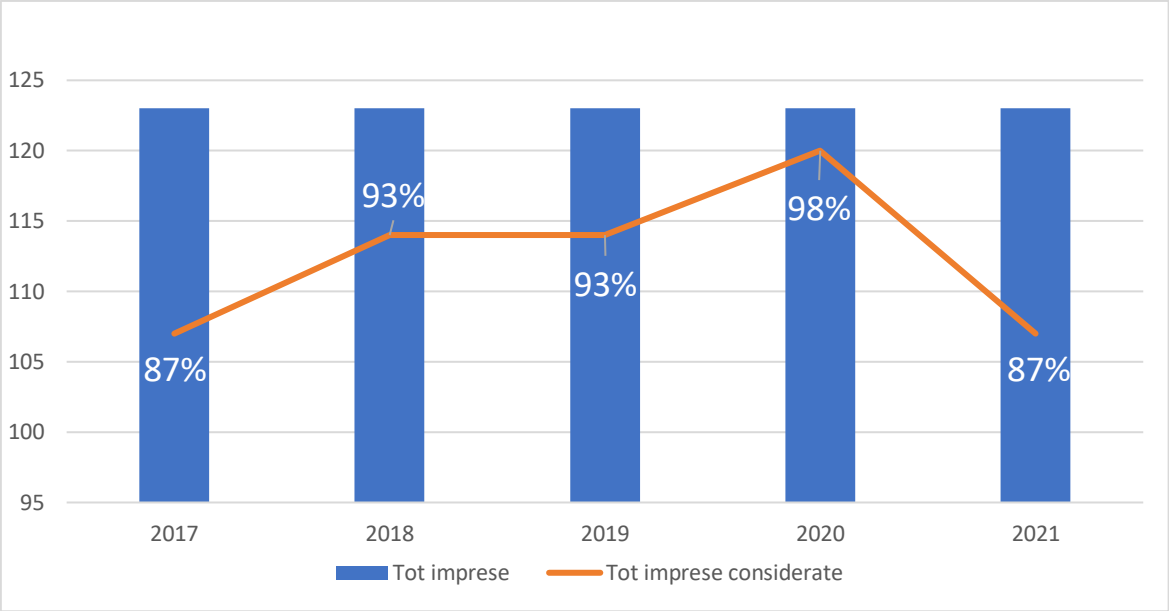



*Figura 8 - Totale imprese considerate anno per anno*

Per quanto riguarda la dimensione delle aziende considerate, la tabella X riporta i dati relativi al il numero di aziende che rientrano nella rispettiva classificazione in termini di fatturato.
Nello specifico:

- la microimpresa registra fatturati massimi di 2 M€
- la piccola impresa registra fatturati massimi di 10 M€
- la media impresa registra fatturati massimi di 50 M€
- la grande impresa registra fatturati di oltre 50 M€.

| | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| Micro | 77 | 69 | 59 | 54 | 59 |
| Piccola | 36 | 42 | 48 | 53 | 48 |
| Media | 9 | 9 | 13 | 14 | 13 |
| Grande | 1 | 3 | 3 | 2 | 3 |

*Tabella 2 - Numero di imprese per dimensione*

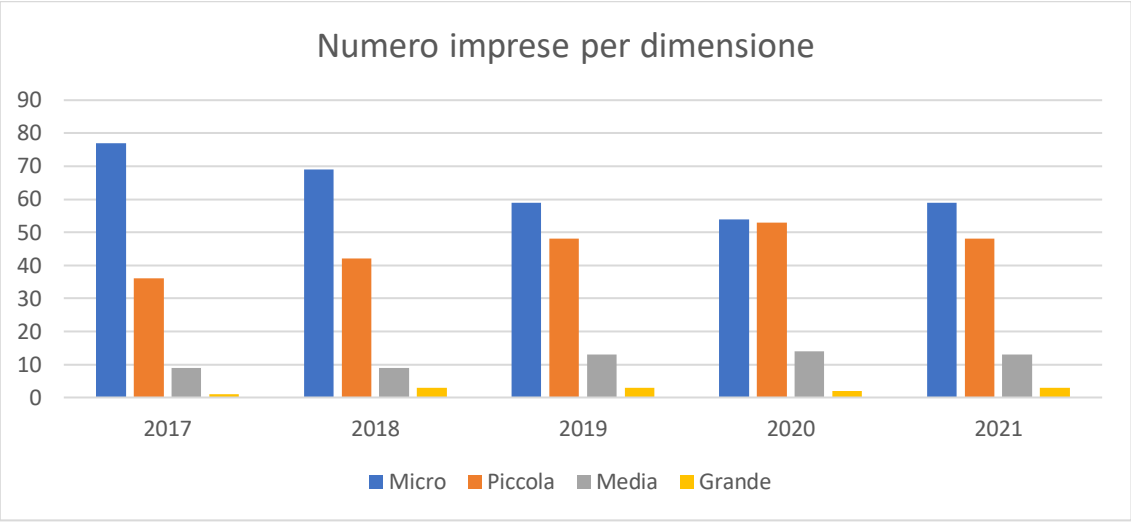



*Figura 9 - Numero imprese per dimensione*

Alla luce dei dati considerati è possibile affermare che il panorama italiano è composto da una maggioranza da micro e piccole imprese ma che i fatturati maggiori sono prodotti per lo più dalle piccole e medie imprese, anche se negli anni recenti, anche la grande impresa ha raggiunto gli stessi livelli di fatturato, arrivando nel 2021 ad occupare la seconda posizione come la tipologia di impresa che produce più fatturato nonostante il numero decisamente esiguo nei confronti delle altre tipologie.

| | Micro | Piccola | Media | Grande |
|---|---|---|---|---|
| 2017 | 60882 | 142637 | 185091 | 56879 |
| 2018 | 66415 | 185195 | 169775 | 172994 |
| 2019 | 59495 | 195347 | 228971 | 186789 |
| 2020 | 60593 | 212608 | 287285 | 147204 |
| 2021 | 55388 | 199617 | 266803 | 241837 |

*Tabella 3 - Fatturato prodotto per tipologia di impresa*

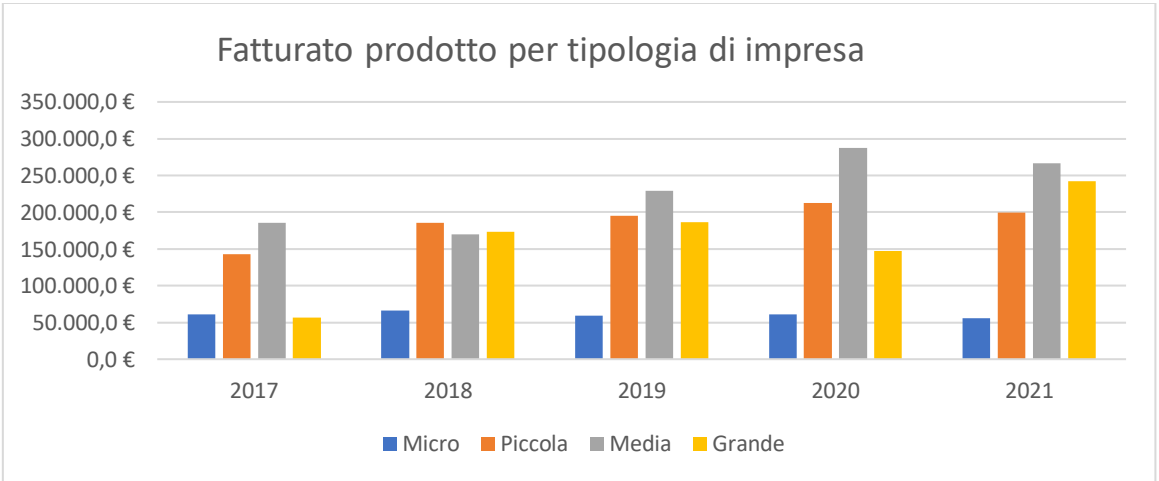



*Figura 10 - Fatturato per tipologia di imprese*

La distribuzione territoriale delle imprese è decisamente sproporzionata poiché la maggior parte delle aziende ha sede nel nord e centro Italia (Lombardia, Emilia, Piemonte, Lazio) mentre il sud ospita solamente il 12% del totale.

| Regione | # imprese |
|---|---|
| Abruzzo | 2 |
| Basilicata | 1 |
| Calabria | 1 |
| Campania | 7 |
| Emilia-Romagna | 12 |
| Lazio | 31 |
| Lombardia | 34 |
| Marche | 2 |
| Piemonte | 12 |
| Puglia | 2 |
| Sardegna | 2 |
| Toscana | 4 |
| Trentino-Alto Adige | 3 |
| Umbria | 2 |
| Veneto | 8 |

*Tabella 4 - Distribuzione aziende per regione*

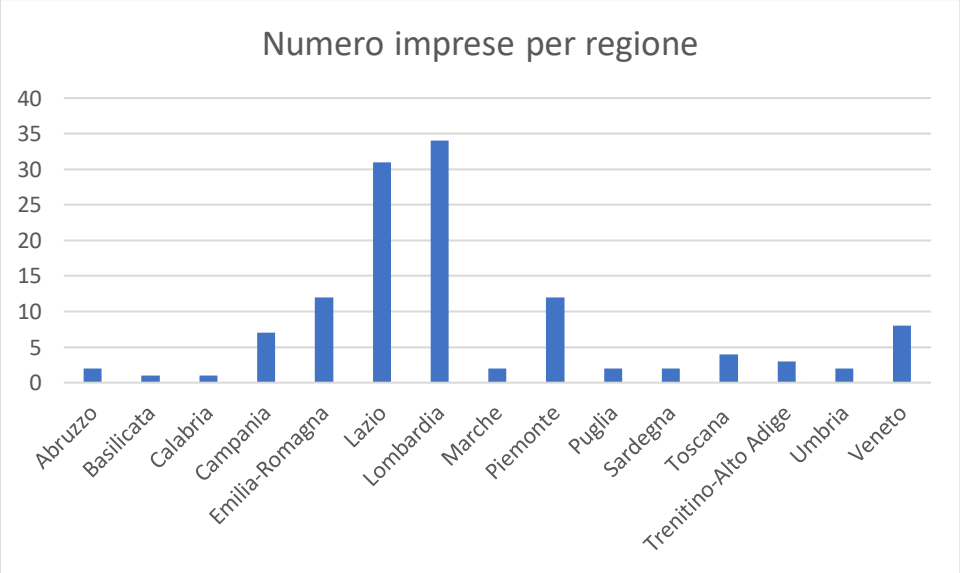



*Figura 11 - Numero imprese per regione*

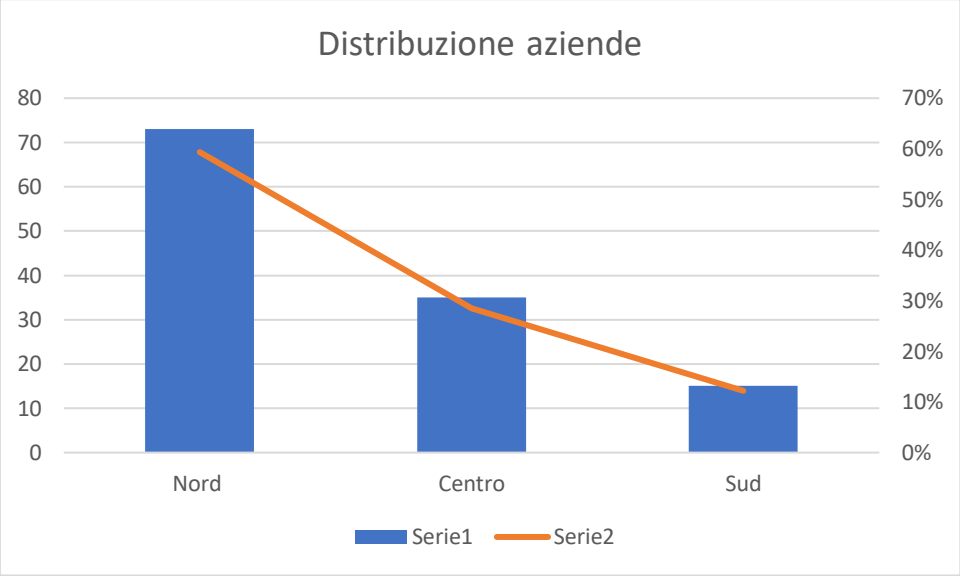



*Figura 12 - Distribuzione aziende nelle macro-aree*

# Analisi dei dati di settore

Per le successive analisi si andrà a considerare un campione di 123 aziende. Sono stati mantenuti i valori nulli sia nel 2017, sia nel 2021 per poter in ogni modo pesare anche quelle aziende di nuova costituzione (che quindi non effettuano ricavi nei primi anni successivi), e di quelle che invece falliscono e vengono liquidate. Inoltre sono stati scartati gli *outlier* ovvero quei valori anomali che si discostano significativamente dalle altre osservazioni del dataset per evitare che impattino fortemente il seguente studio restituendo una realtà distorta.

## Produzione Lorda / Fatturato

Il fatturato è una delle principali misure della performance economica di un'azienda, e quindi è un'importante variabile da considerare in un'analisi economica.

Considerato il settore della cybersecurity, si può pensare che il valore di produzione coincida con il valore di fatturato. Infatti, solitamente il valore di produzione di questo servizio è pari al fatturato o somma dei ricavi da vendite/altri ricavi, incrementato di variazioni di rimanenze di magazzino. Da questo momento in poi quindi non verrà fatta alcuna differenza tra produzione lorda e fatturato.

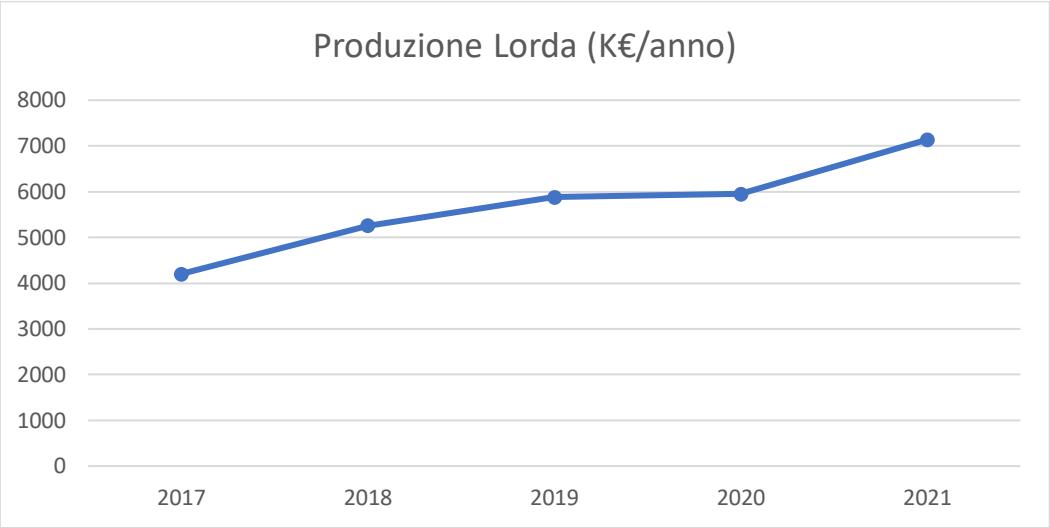



*Figura 13 - Produzione lorda*

Nel complesso si nota una crescita costante e progressiva della produzione lorda media di anno in anno con un boost nel 2021. Questo trend positivo conferma quanto asserito nel capitolo precedente: questo settore di mercato sta vivendo un periodo di salute finanziaria in cui le società che lo compongono sono in grado di generare reddito. Infatti, la produzione lorda media è praticamente raddoppiata nel giro di 5 anni, presentando un *Compound Average Growth Rate* o CAGR dell'11,17%.

| *PL* | *Media* *(k€/anno)* | *Varianza* | *Valore MAX* *(k€/anno)* | *Valore MIN* *(k€/anno)* |
|---|---|---|---|---|
| *2017* | 4202,7 | 59698075,5 | 56879,0 | 26 |
| *2018* | 5260,0 | 96519952,9 | 61607,0 | 67 |
| *2019* | 5882,5 | 115149664,1 | 72920,0 | 45 |
| *2020* | 5947,0 | 126790254,9 | 81096,0 | 507 |
| *2021* | 7136,9 | 189359860,6 | 94524,0 | 131 |

*Tabella 5 - Produzione Lorda*

Si ottengono valori di varianza elevati, quindi le dimensioni di fatturato cambiano di molto da impresa a impresa, che possono chiaramente ed evidentemente avere grandezze del tutto differenti. Considerando poi i valori di fatturato minimi e massimi, diventa evidente che si ha a che fare sia con microimprese che anche con grandi imprese.

Territorialmente parlando, la maggior parte della produzione lorda è concentrata nel nord e ne centro della penisola mentre, solamente 5,86% della PL viene prodotta nel sud Italia.

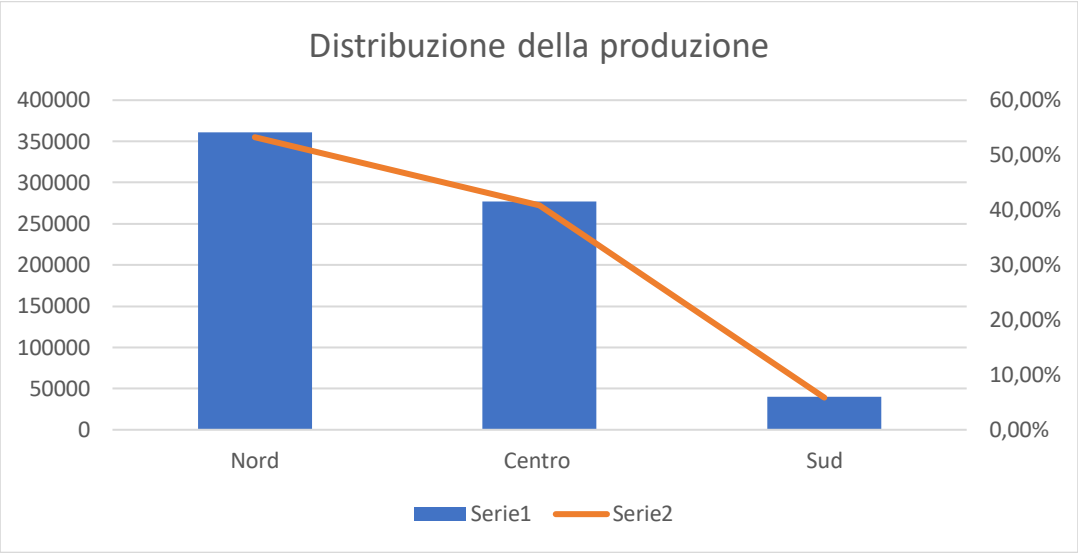



*Figura 14 - Distribuzione della produzione*

## Utile

Procedendo ad un'analisi di conto economico può essere interessante valutare quante delle aziende di questo settore, riescono ad ottenere utili positivi, e la media di questi valori.

L'utile segue lo stesso trend del fatturato presentando quindi una crescita costante e progressiva, che nel periodo di tempo considerato è riuscita quasi a raddoppiare, seguendo un tasso medio di crescita annuo del 13%. Anche da questa analisi si intuisce che il settore è capace di generare profitti, gestire i propri costi e creare valore per gli azionisti

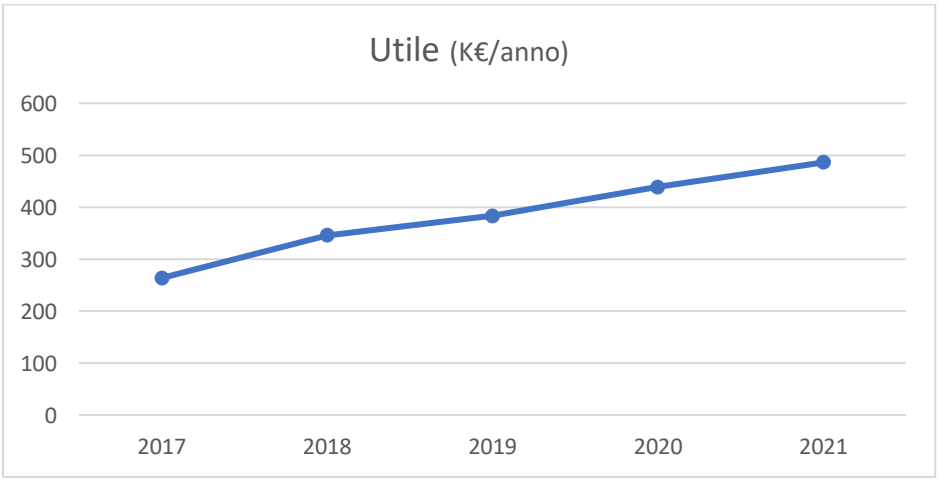



*Figura 15 - Utile*

Nel caso dell'utile, si notano varianze più piccole rispetto a quelle relative alla produzione lorda proprio perché misurano un capitale che viaggia su un ordine di grandezza minore rispetto a PL e EBITDA. Nonostante ciò, sono comunque varianze sufficientemente elevate sono molto da suggerire una grande diversità tra le aziende.

| *Utile* | *Media* *(k€/anno)* | *Varianza* | *Valore MAX* *(k€/anno)* | *Valore MIN* *(k€/anno)* |
|---|---|---|---|---|
| *2017* | 264 | 1387856 | 9221 | -3102 |
| *2018* | 346 | 2220176 | 12122 | -2192 |
| *2019* | 383 | 2448108 | 11287 | -4498 |
| *2020* | 439 | 2601554 | 11468 | -3552 |
| *2021* | 486 | 5854721 | 15143 | -13833 |

*Tabella 6 - Utile*

## EBITDA

Rimaniamo sempre in ambito Conto Economico per andare ad analizzare un altro driver particolarmente importante.
L'EBITDA o risultato operativo viene definito come valore della produzione, al netto dei costi della produzione stessa, al lordo della tassazione. Al valore della produzione, infatti, si vanno a sottrarre i costi del personale, delle materie prime e gli altri costi legati alla produzione. Rappresenta il reddito derivante dall'attività principale dell'impresa e può essere usato nel calcolo di indicatori di bilancio.

| *EBITDA* | *Media* *(k€/anno)* | *Varianza* | *Valore MAX* *(k€/anno)* | *Valore MIN* *(k€/anno)* |
|---|---|---|---|---|
| *2017* | 655 | 3470714 | 15913 | -1010 |
| *2018* | 756 | 4672834 | 17770 | -1407 |
| *2019* | 686 | 4393396 | 16331 | -1983 |
| *2020* | 916 | 6725188 | 20580 | -745 |
| *2021* | 1197 | 10158853 | 26602 | -1025 |

*Tabella 7 - EBITDA*

Spostando l'attenzione sui valor minimi registrati per l'EBITDA, Risulta evidente dalla tabella che molte imprese raggiungono risultati operativi, prima di interessi e tasse, negativi. In tutti gli anni il valore minimo è negativo. La tabella successiva mostra come molte delle imprese ogni anno registrino RO negativi

| | **Imprese con EBITDA < 0** | **% imprese su tot** |
|---|---|---|
| **2017** | 5 | 4,1% |
| **2018** | 9 | 7,3% |
| **2019** | 6 | 4,9% |
| **2020** | 10 | 8,1% |
| **2021** | 11 | 8,9% |

*Tabella 8 - Numero imprese con EBITDA negativo*

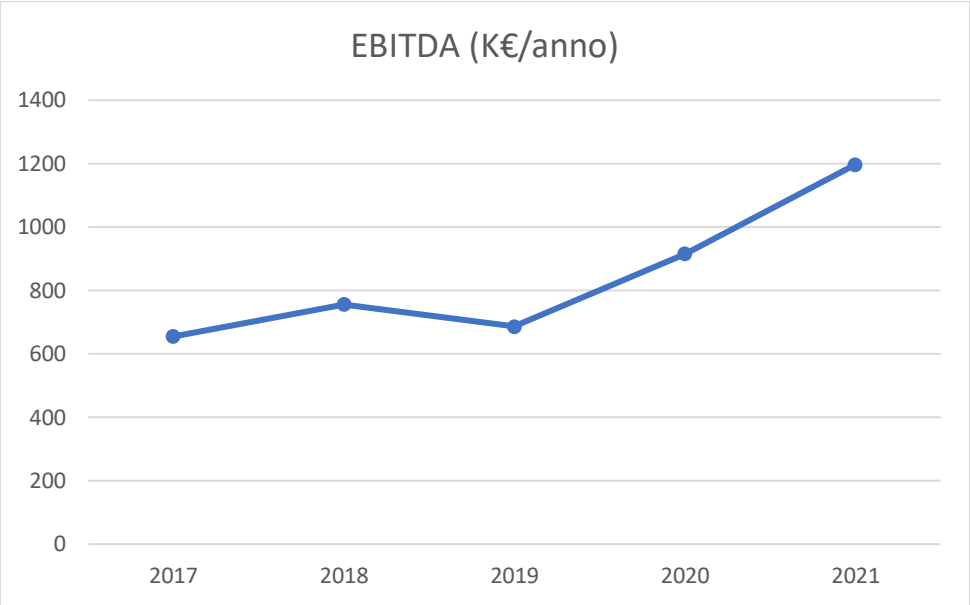



*Figura 16 - EBITDA*

Se produzione lorda e utili presentavano un trend molto simile, quello relativo all'EBITDA risulta leggermente differente, infatti nonostante abbia anch'esso un andamento decisamente crescente, presenta un leggera inflessione nell'anno 2019 decrescendo del 9,27% rispetto all'anno precedente. Tuttavia, negli anni successivi (2020 e 2021), probabilmente anche a causa della pandemia che ha dato un *boost* importante allo sviluppo delle tecnologie costringendo le imprese a doversi adattare ad un nuovo modo di lavorare, comunicare e interagire con i clienti. In questo periodo temporale infatti si è verificata una crescita repentina del 53% circa dal 2019 al 2020 e del 51% circa dal 2020 al 2021.
Globalmente, il CAGR è stato del 12,82% portando quindi anche in questo caso ad un raddoppio dell'EBITDA nel periodo di tempo considerato.

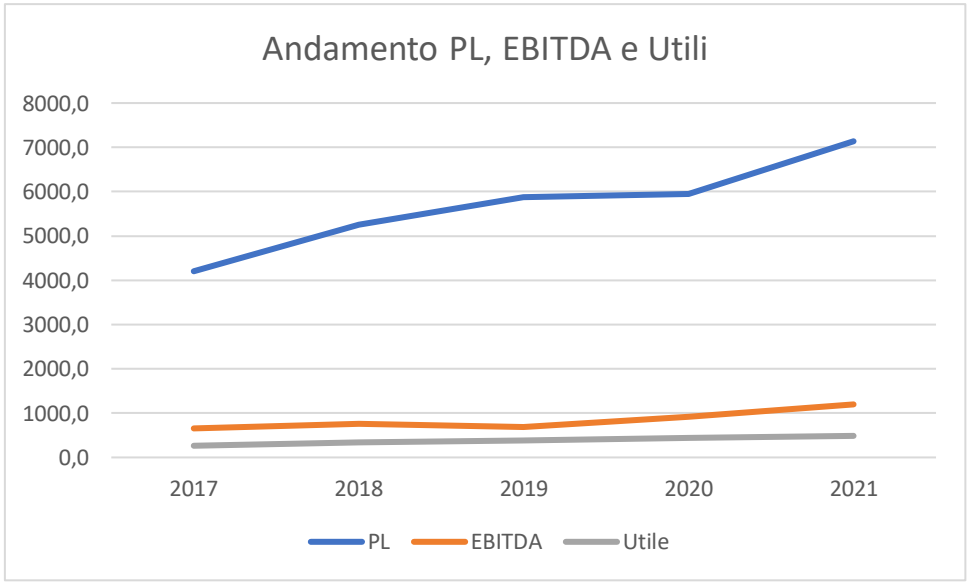



*Figura 17 - Confronto andamento PL, EBITDA e Utili*

# Indici di redditività

Gli indicatori principali sono:

- ROE (Return on Equity)
- ROS (Return on Sales)
- ROI (Return on Investment)
- ROA (Return on Asset)

## Return on Equity

Il ROE è una misura della redditività del capitale investito dagli azionisti di un'azienda e viene calcolato dividendo il reddito netto dell'azienda per il suo patrimonio netto.

$$ROE = \frac{Utile}{PN}$$

Questa misura aiuta gli investitori a valutare la capacità di un'azienda di generare profitti utilizzando il denaro investito dagli azionisti. In generale, un ROE elevato indica che l'azienda è in grado di utilizzare efficacemente il suo capitale proprio per generare profitti, mentre un ROE basso potrebbe indicare una gestione inefficiente del capitale proprio.
Generalmente questo indice viene confrontato dagli investitori con rendimenti risk-free per giudicare la validità di un investimento: infatti il ROE di un'azienda dovrebbe essere superiore ai rendimenti risk-free, poiché gli investitori richiedono un premio per il rischio che assumono investendo in azioni. Se il ROE di un'azienda fosse inferiore ai rendimenti risk-free, gli investitori potrebbero preferire di investire in titoli di Stato o altri investimenti a basso rischio.

| *ROE* | *Media* | *Varianza* | *Valore MAX* | *Valore MIN* |
|---|---|---|---|---|
| *2017* | 27,6% | 0,11 | 1,27 | -0,86 |
| *2018* | 26,4% | 0,08 | 0,99 | -0,76 |
| *2019* | 25,1% | 0,08 | 0,99 | -0,75 |
| *2020* | 23,3% | 0,13 | 1,14 | -1,05 |
| *2021* | 23,3% | 0,10 | 1,17 | -0,75 |

*Tabella 9 - ROE*

Il ROE medio del settore nel periodo di tempo considerato è ha avuto un andamento sempre decrescente, passano inizialmente dal 27, 6% al 25,1% per poi assestarsi su valori di circa del 23% negli ultimi due anni del quinquennio. Nonostante questa decrescita, il valore assunto dal Return on Equity è comunque molto positivo, infatti secondo *Zacks Investment Research, Inc* un valore ottimo di questo indice si aggira intorno al 25%.
In media quindi i risultati ottenuti sono soddisfacenti.

La presenza di valori negativi è dovuta al fatto che vi sono imprese che ottengono utili negativi ovvero perdite. Questo significa che lo squilibrio economico è così grave da andare ad erodere i mezzi propri.

La varianza è abbastanza alta soprattutto nel 2020, e lo si può notare osservando le colonne dedicate ai valori minimi e massimi; ad ogni modo ciò non sorprende poiché il campione di imprese considerato è comunque molto eterogeneo dal momento che racchiude microimprese e imprese decisamente più grandi quotate in borsa.

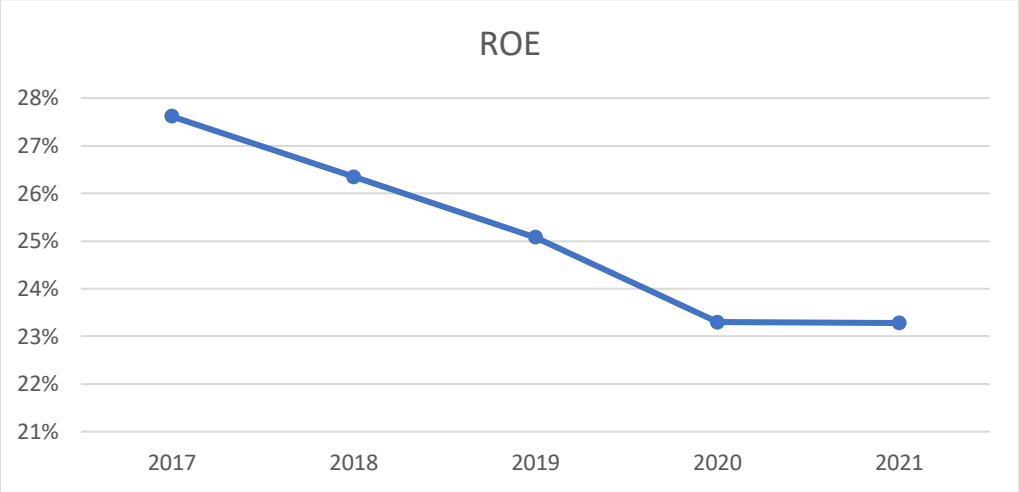



*Figura 18 - ROE*

## Return on Sales

Il ROS, o Return On Sales, è dato dal rapporto tra reddito operativo e valore di produzione lorda.

$$ROS = \frac{RO}{PL}$$

È una misura della redditività dell'azienda che rappresenta il risultato operativo che si ottiene con una unità di ricavo in rapporto alle sue entrate; in altre parole, indica quanto margine di profitto viene generato dalle vendite. Un ROS negativo significa che l'azienda non ottiene un utile con l'attività principale svolta.

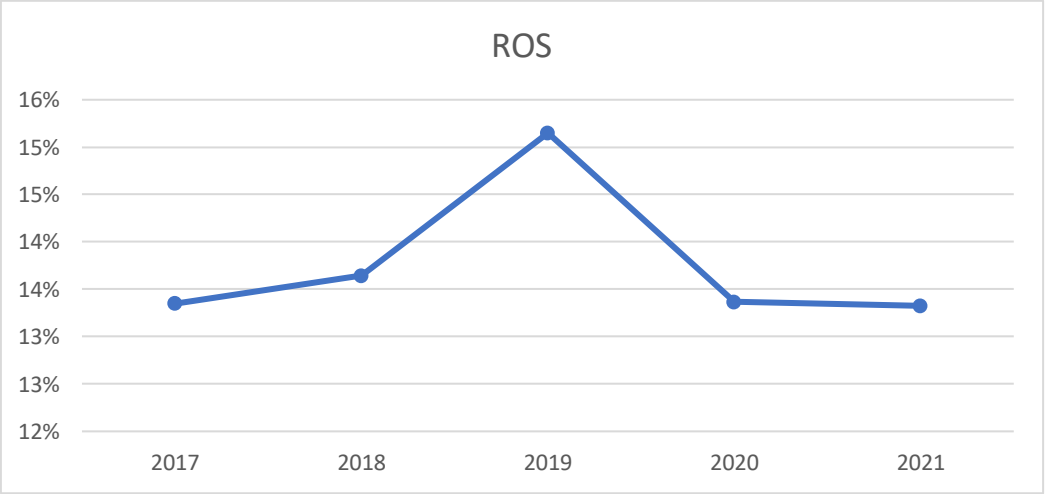



*Figura 19 - Andamento ROS*

| ROS | Media | Varianza | Valore MAX | Valore MIN |
|---|---|---|---|---|
| 2017 | 13,4% | 0,04 | 0,74 | -1,13 |
| 2018 | 13,6% | 0,02 | 0,67 | -0,57 |
| 2019 | 15,1% | 0,03 | 0,82 | -0,49 |
| 2020 | 13,4% | 0,03 | 0,68 | -1,07 |
| 2021 | 13,3% | 0,03 | 0,60 | -0,70 |

*Tabella 10 - ROS*

Il livello del ROS è decisamente positivo durante tutto il periodo di tempo considerato aggirandosi intorno al 13-14%; il 2020 è stato l'anno in cui si è assistito ad una forte impennata dell'indice aumentando di circa 2 punti percentuali rispetto agli altri anni; nonostante ciò, i livelli di ROS rimangono bene o male costanti nel quinquennio.

La varianza a differenze degli indicatori analizzati precedentemente, è decisamente minima: le diverse imprese hanno situazioni di redditività delle vendite molto simili sia che si tratti di micro, piccole, medie o grandi imprese.

## Return on Asset

Il ROA o Return on Asset, misura la quantità di reddito prodotta dall'impresa in rapporto all'attivo totale generato investito come asset. Un valore alto di questo indice sta a significare che si possiede maggiore efficienza nello sfruttamento della base patrimoniale.

Questo indicatore è ideale per misurare la profittabilità di aziende dello stesso settore, perché spiega come a parità di asset, l'impresa riesca a trarre maggiore profitto di un'altra.

$$ROA = \frac{RO}{Tot\ attivo}$$

| ROA | Media | Varianza | Valore MAX | Valore MIN |
|---|---|---|---|---|
| 2017 | 15,5% | 0,03 | 0,81 | -0,89 |
| 2018 | 14,3% | 0,05 | 0,81 | -0,93 |
| 2019 | 17,1% | 0,04 | 0,79 | -0,60 |
| 2020 | 14,7% | 0,04 | 0,82 | -0,46 |
| 2021 | 15,2% | 0,04 | 0,93 | -0,37 |

*Tabella 11 - ROA*

Guardando ai valori massimi e minimi assunti dall'indice si nota come, a differenza degli altri indici di redditività, siano sempre compresi tra 1 e -1; ciò è comprensibile trattandosi di un rapporto percentuale che presenta una varianza abbastanza contenuta. Le imprese considerate quindi versano in una situazione di ritorni sugli asset sufficientemente simile.
Nonostante ciò, l'andamento durante il periodo di tempo considerato è abbastanza altalenante subendo una piccola decrescita del 2018 e successivamente una crescita arrivando ad un picco del 17,1% nel 2019, per poi assestarsi per i due anni successivi nei pressi del 15%. Di anno in anno in fin dei conti assistiamo ad un ROA abbastanza costante, con piccole variazioni rispetto all'anno precedente.

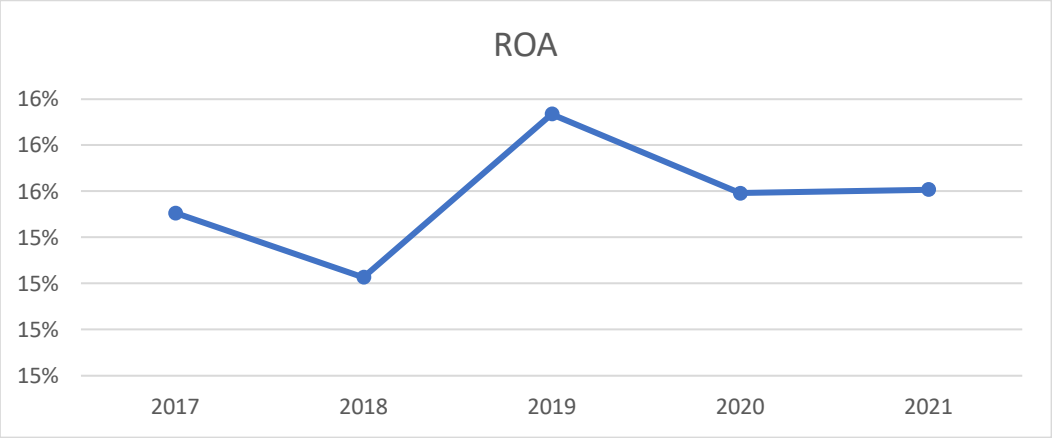



*Figura 20 - Andamento ROA*

## Return on Investment

Insieme al ROA, per identificare la redditività degli impieghi, viene considerato il ROI, o Return on Investment, che rappresenta quanto EBITDA viene generato per ogni unità di capitale operativo netto. Viene calcolato per l'appunto come reddito operativo netto diviso capitale operativo netto o investito, che a sua volta viene determinato come differenza tra debiti finanziari e attività finanziarie a cui va sommato il patrimonio netto.

$$ROI = \frac{RO}{KON}$$

Il ROI è ideale da utilizzare quando si vogliono confrontare due o più investimenti simili e serve per capire dato un livello di investimento, quanto profitto si può generare da esso.

Per il calcolo di questo indice è importante evidenziare il fatto che, come premesso all'inizio del capitolo, i bilanci delle aziende fornite da AIDA non presentano una distinzione tra le varie tipologie di debito, per cui la voce relativa ai debiti finanziari considerata in realtà comprende sia debiti commerciali che finanziari. Si è comunque deciso di calcolare e rappresentare l'indice per avere un'idea dell'andamento del ROI.

| *ROI* | *Media* | *Varianza* | *Valore MAX* | *Valore MIN* |
|---|---|---|---|---|
| *2017* | 15,7% | 0,04 | 0,81 | -0,99 |
| *2018* | 14,3% | 0,05 | 0,81 | -0,93 |
| *2019* | 17,1% | 0,04 | 0,79 | -0,60 |
| *2020* | 14,7% | 0,04 | 0,82 | -0,46 |
| *2021* | 15,2% | 0,04 | 0,93 | -0,37 |

*Tabella 12 - ROI*

Nel caso del ROI il trend individuato è molto altalenante in concordanza all'indicatore precedente, presentando aumenti e decrescite *every other year*. L'andamento durante gli anni è molto simile al ROA poiché subisce una decrescita nel 2018 arrivando a toccare il valore minimo per rispetto ai 5

anni (14,3%), per poi subire un aumento repentino fino ad arrivare ad un picco di 17,1% nell'anno successivo.

Il livello generale è più alto del ROS, infatti il ritorni sugli investimenti si aggirano tra il 15% e il 17%; anche in questo caso indicatore molto positivo che indica un'ottima salute del settore ed una varianza minima tra le imprese a campione

Valori massimi e minimi sono compresi tra 1 e -1, conseguenza diretta del fatto che anche nel caso del Return on Investment sono stati registrate varianze moderate, per cui si intuisce che in media le imprese presentano una situazione abbastanza simile.

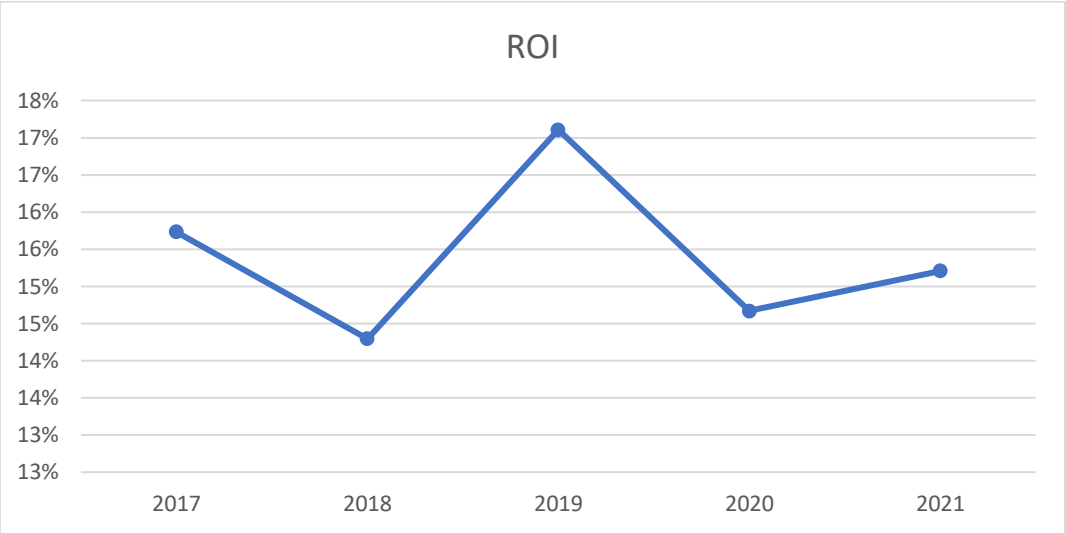



*Figura 21 - Andamento ROI*

Un ROI alto spesso è sintomo di preferenza di capitale di debito piuttosto che di capitale proprio; questo succede poiché il capitale di debito è meno costoso da utilizzare, per cui è preferibile e ha come conseguenza un ROI alto. Tuttavia, l'ottenimento di un ROI negativo è giustificato dal fatto che l'investimento per risultare profittevole necessita di diversi anni e deve essere considerato in un orizzonte temporale lungo e non breve.

## Current Ratio e Acid Test

Il Current Ratio (o rapporto corrente) è una misura della capacità di un'azienda di far fronte ai propri obblighi a breve termine con le sue attività correnti. In altre parole, il Current Ratio indica la capacità di un'azienda di soddisfare i propri impegni di pagamento a breve termine, come debiti a fornitori, prestiti a breve termine o altre passività.

$$CR = \frac{AC}{PC}$$

Il Current Ratio viene calcolato dividendo le attività correnti dell'azienda (cioè le attività che possono essere convertite in contanti entro un anno) per le passività correnti (cioè le passività che devono essere saldate entro un anno)

| CR | Media | Varianza | Valore MAX | Valore MIN |
|---|---|---|---|---|
| 2017 | 1,6 | 1,4 | 7,3 | 0,2 |
| 2018 | 1,7 | 1,9 | 9,2 | 0,4 |
| 2019 | 1,7 | 2,2 | 10,1 | 0,5 |
| 2020 | 1,8 | 1,9 | 7,9 | 0,2 |
| 2021 | 1,9 | 3,2 | 11,4 | 0,2 |

*Tabella 13 - Current Ratio*

Un Current Ratio superiore a 1 indica che l'azienda ha abbastanza attività correnti per coprire le sue passività correnti. In generale, un Current Ratio più alto indica una maggiore liquidità e una maggiore capacità dell'azienda di far fronte ai propri obblighi di pagamento a breve termine. Tuttavia, un Current Ratio troppo alto potrebbe indicare che l'azienda non sta utilizzando le sue risorse in modo efficiente e potrebbe avere eccessive riserve di liquidità.

Allo stesso modo, L'Acid Test o Quick Ratio è una misura della liquidità di un'azienda molto simile al Current Ratio, infatti viene calcolata come

$$AT = \frac{AC - MG}{PC}$$

dove per MG si intendono le rimanenze di magazzino.

Date le caratteristiche del settore, CR e AT hanno valori molto simili proprio perché le rimanenze hanno assumono valori veramente esigui. Di conseguenza i due indici presentano lo stesso andamento: AT si trova ad un livello leggermente inferiore rispetto a CR proprio a causa delle rimanenze di magazzino che sono state sottratte dalle attività correnti.

| AT | Media | Varianza | Valore MAX | Valore MIN |
|---|---|---|---|---|
| 2017 | 1,6 | 1,4 | 7,3 | 0,2 |
| 2018 | 1,7 | 1,9 | 9,2 | 0,4 |
| 2019 | 1,7 | 2,2 | 10,1 | 0,5 |
| 2020 | 1,7 | 1,9 | 7,9 | 0,2 |
| 2021 | 1,8 | 3,3 | 11,4 | 0,2 |

*Tabella 14 - Acid Test*

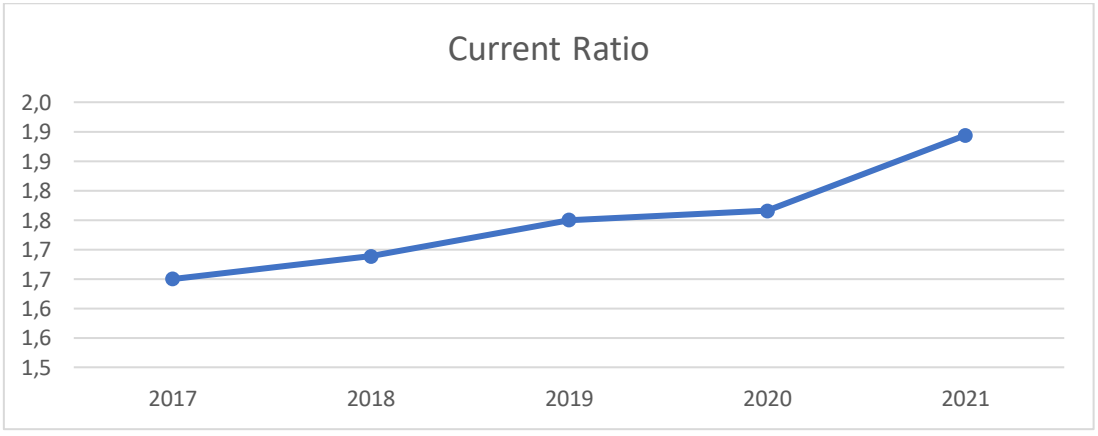



*Figura 22 - Andamento Current Ratio*

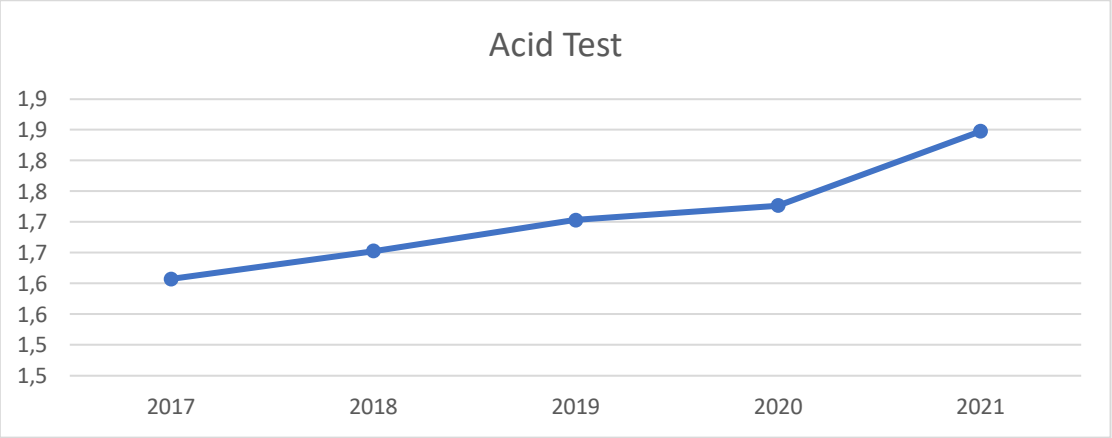



*Figura 23 - Andamento Acid Test*

## Leva finanziaria

Il *leverage book value* è un indicatore finanziario che misura l'effetto della leva finanziaria sul patrimonio netto di un'azienda. Esso viene calcolato dividendo il debito totale dell'azienda per il suo patrimonio netto.

$$LBV = \frac{D}{PN}$$

È uno degli indici principali per studiare la struttura finanziaria di un'impresa o in questo caso di un settore di mercato, in modo da capire in che proporzione le imprese sono finanziate da fonti interne e fonti esterne. Nonostante andrebbe calcolata come il rapporto tra i debiti finanziari e l'equity, nello sviluppo delle analisi del caso, sempre per i motivi precedentemente indicati, è stata determinata non facendo alcuna distinzione tra la tipologia dei debiti, considerandoli quindi in toto. Il risultato è un livello di LBV mediamente più elevato rispetto alla normalità, che però ci permette di poter analizzare il tipo di trend dell'indice nel periodo di tempo considerato.

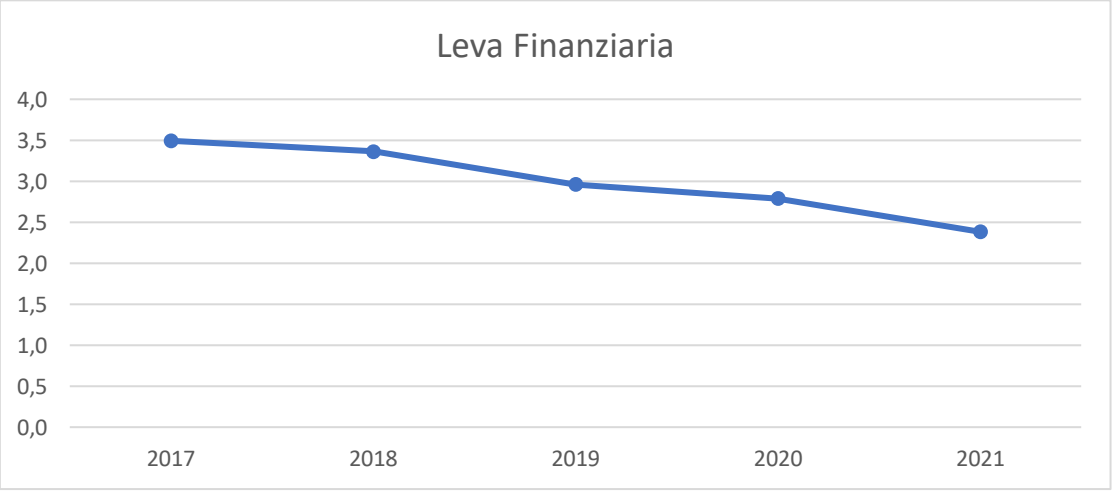



*Figura 24 - Andamento leva finanziaria*

L’andamento dell’indice è in costante decrescita passando da un’inziale 3,5 nel 2017 ad un 2,4 del 2021, risultato dovuto soprattutto ad una diminuzione media graduale del debito totale. In ogni anno però mediamente il rapporto va oltre l’unità (D/PN=1); ciò sta quindi a significare che le imprese preferiscono adoperare capitale di debito rispetto al capitale proprio dal momento in cui quest’ultimo risulta più costoso (*pecking order*).

I valori di varianza sono molto grandi durante tutti gli anni, quindi avremo aziende con una leva talmente esposta da poter fallire, e altre che invece godono di ottima solidità. Questa considerazione è evidente se si osservano i valori di minimo e massimo.

| *LBV* | *Media* | *Varianza* | *Valore MAX* | *Valore MIN* |
|---|---|---|---|---|
| *2017* | 3,5 | 14,5 | 18,3 | -7,2 |
| *2018* | 3,4 | 12,1 | 14,3 | -3,6 |
| *2019* | 3,0 | 9,9 | 15,8 | -3,8 |
| *2020* | 2,8 | 12,9 | 16,0 | -9,0 |
| *2021* | 2,4 | 18,9 | 19,4 | -13,5 |

*Tabella 15 - Leva finanziaria*

# Concentrazione del mercato

Andando a calcolare l'indice di Herfindhal-Hirschman HH, possiamo ricavare importanti informazioni sulla concentrazione del mercato. Sfruttiamo quindi la relazione tra questo indice e la quota di mercato *si* posseduta da ogni impresa per andare a ricavare queste informazioni.
Data la mancanza della voce fatturato nei bilanci forniti da AIDA, basiamo il calcolo della quota di mercato sul totale della produzione.
Fatto ciò, calcoliamo la l'indice HH attraverso la formula

$$HH = \sum_{1}^{i} Hi$$

con
$Hi = si^2$

Per il calcolo dell'indice, sono state considerate solamente le imprese che avessero uno quota di mercato sufficientemente grande; sono state quindi scartate quelle imprese con un livello di fatturato esiguo, che non avrebbero quindi inciso in modo sostanziale sul calcolo finale.
Le aziende individuate sono le seguenti e si dividono il mercato come indicato in figura 25:
- INFOCERT
- BLUE REPLY
- ATLANTICA DIGITAL
- NOVANEXT
- NAMIRIAL
- CREDEMTEL
- AXIANS BRAND ID
- ACTALIS
- MEAD INFORMATICA
- TELECONSYS
- PRISMI
- CITEL GROUP
- L F IMPIANTI

L'indice viene calcolato come media degli ultimi 5 anni in modo da comprendere i livelli di concentrazione sui quali si aggira questo mercato

| **Società** | **Produzione** (k€/anno) | ***si*** | ***Hi*** | ***HH*** |
|---|---|---|---|---|
| INFOCERT | 73405,2 | 20,5% | 0,0419 | 0,1241 |
| BLUE REPLY | 62807,5 | 17,5% | 0,0307 | |
| ATLANTICA DIGITAL | 48431,8 | 13,5% | 0,0182 | |
| NOVANEXT | 31910,1 | 8,9% | 0,0079 | |
| NAMIRIAL | 37339,8 | 10,4% | 0,0108 | |
| CREDEMTEL | 25773,0 | 7,2% | 0,0052 | |
| AXIANS BRAND ID | 16360,9 | 4,6% | 0,0021 | |
| ACTALIS | 16085,5 | 4,5% | 0,0020 | |
| MEAD INFO | 13627,0 | 3,8% | 0,0014 | |
| TELECONSYS | 10995,8 | 3,1% | 0,0009 | |
| PRISMI | 14615,4 | 4,1% | 0,0017 | |
| CITEL GROUP | 9960,4 | 2,8% | 0,0008 | |
| L F IMPIANTI | 6904,2 | 1,9% | 0,0004 | |

*Tabella 16 - Calcolo indice HH*

Sapendo che l'intervallo di valori che l'indice di Herfindhal-Hirschman può assumere va da 0 a 1, un valore di HH di 0,118 sta proprio ad indicare una concentrazione del mercato assolutamente bassa in cui le singole imprese presentano quote altrettanto striminzite.

Dall'analisi dell'indice di Herfindhal-Hirschman emerge che questo mercato (o almeno quello conteso nel panorama italiano) risulta poco concentrato. Le motivazioni sono varie.
Una prima motivazione è sicuramente legata alla numerosità e alle modalità di scelta del campione; infatti, quest'ultimo è formato solamente da 13 società che sono state prelevate da una popolazione circa 10 volte più grande: è intuitivo quindi dedurre che la maggior parte della popolazione è formata maggiormente, come abbiamo visto anche nel capitolo precedente, da micro e piccole imprese (fatturato minore di 2M€ per le prime e minore di 10€ per le ultime). Questo suggerisce quindi che in un mercato formato prevalentemente da tante piccole imprese, nessuna di esse riesce ad imporsi sulle altre e ad accaparrarsi la parte di mercato più ampia in modo da ricoprire una posizione di leader.

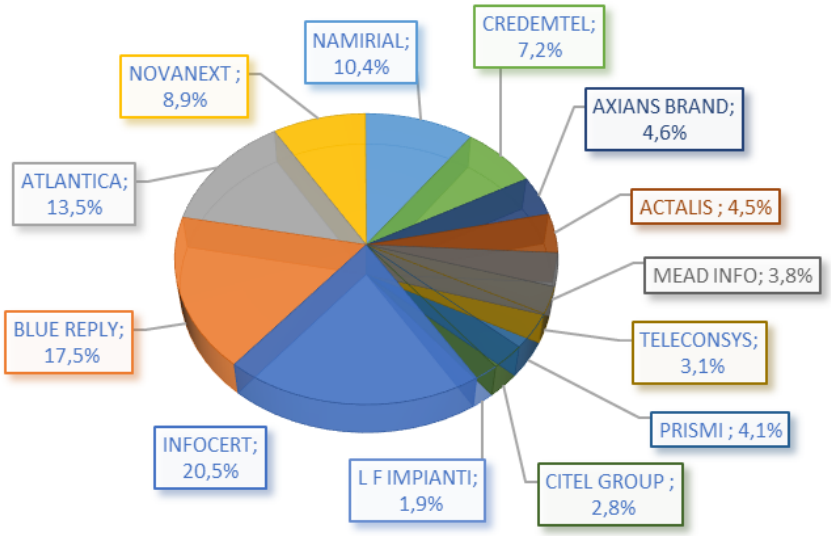



*Figura 25 - Divisione del mercato*

Infatti, ad esclusione di Infocert e Blue Reply che sono le due imprese più grandi in termini di fatturato e produzione, dallo studio dell'indice è ben visibile che nessuna delle altre società ha abbastanza potere di mercato da influenzare i prezzi o le quantità di produzione proprio a causa delle caratteristiche intrinseche dello stesso (gran numero di concorrenti che offrono prodotti o servizi simili). In questo tipo di mercato, i produttori devono competere tra loro per attrarre i consumatori offrendo prezzi competitivi, prodotti di alta qualità e servizi migliori.
Inoltre, l'ingresso nel mercato è relativamente facile poiché ci sono poche barriere all'entrata per i nuovi concorrenti, poiché i servizi offerti non necessitano di grossi investimenti iniziali che renderebbero sconveniente l'ingresso nel mercato: la maggior parte dei servizi offerti, sfrutta software e architetture che è possibile affittare e prendere in prestito, come una specie di leasing. Infatti, tutto il settore è subordinato ai grandi colossi come Google, Amazon e Microsoft che offrono le loro infrastrutture permettendo ai player di usufruire delle capacità di storage e gestione di dati senza la necessità di dover tirare su la propria infrastruttura *on-premise*.
Date queste caratteristiche, è intuitivo che un gran numero di aziende riescano facilmente entrare nel mercato e competere.

# Conclusioni

Dopo aver analizzato il settore di mercato della cybersecurity, emerge con chiarezza che la sicurezza informatica rappresenta una sfida sempre più rilevante per le aziende, le organizzazioni e le istituzioni di ogni genere. La crescente dipendenza dalle tecnologie informatiche, infatti, espone a rischi e minacce che possono compromettere la privacy, la sicurezza e la stabilità di un'organizzazione.
I principali attori del settore, come le società di sicurezza informatica e i fornitori di tecnologie, stanno investendo ingenti risorse per migliorare la loro offerta di servizi e prodotti e rispondere alle crescenti esigenze dei clienti. La necessità di proteggere i dati e le informazioni sensibili, infatti, richiede una continua innovazione tecnologica e una costante formazione del personale specializzato.

Le conclusioni che emergono da questa analisi sono che il settore di business relativo alla cybersecurity è in salute ed in forte espansione: a seguito dell'analisi dei principali indici economici e finanziari relativi al settore di mercato della cybersecurity, emerge con chiarezza che la sicurezza informatica rappresenta un'opportunità di business in continua crescita.
La crescente dipendenza dalle tecnologie informatiche e l'aumento delle minacce informatiche hanno portato molte organizzazioni a investire in soluzioni di sicurezza informatica sempre più sofisticate e avanzate.

L'analisi degli indici economici del settore dimostra una crescita costante del mercato della cybersecurity, che si traduce in un aumento altrettanto costante della produzione e delle entrate delle società di sicurezza informatica e dei fornitori di tecnologie. Inoltre, si osserva una crescente specializzazione dei fornitori di servizi di sicurezza informatica, che offrono soluzioni personalizzate per specifici settori e applicazioni.

Gli indici economici mostrano anche che il settore della cybersecurity rappresenta un'opportunità di lavoro in continua crescita, con una forte domanda di professionisti altamente qualificati e specializzati. In particolare, la richiesta di esperti in sicurezza informatica, analisti di dati e specialisti in tecnologie di sicurezza è in costante crescita.

Tuttavia, la crescita del mercato della cybersecurity comporta anche nuove sfide, come la concorrenza tra i fornitori di servizi di sicurezza informatica, la necessità di costante innovazione tecnologica e la complessità crescente delle minacce informatiche. Inoltre, il costo delle soluzioni di sicurezza informatica può rappresentare un ostacolo per le organizzazioni meno abbienti.

In conclusione, gli indici economici relativi al settore della cybersecurity dimostrano che questa è un'area di business in continua crescita, con grandi opportunità di sviluppo. Detto ciò, sarà però importante continuare a monitorare l'evoluzione del settore, investire in innovazione e formazione, e collaborare con altre organizzazioni per garantire una protezione efficace e affidabile dei dati e delle informazioni sensibili.

# Sitografia


Cysea - Cyber Security Academy - Cyberspace Cyberspazio, la definizione Storica e Moderna
https://cysea.it/2020/09/02/cyberspazio-definizione-storica-moderna/

Darknet, dark web, deep web e surface web | Blog ufficiale di Kaspersky
https://www.kaspersky.it/blog/deep-web-dark-web-darknet-surface-web-difference/23836/

https://aida.bvdinfo.com

Statista - The Statistics Portal for Market Data, Market Research and Market Studies

Sicurezza delle informazioni. Cos'è e come funziona la Cyber Security (namirial.it)
https://focus.namirial.it/cyber-security/

Cos'è la Cybersecurity? (kaspersky.it)
https://www.kaspersky.it/resource-center/definitions/what-is-cyber-security

Zacks Investment Research: Stock Research, Analysis, & Recommendations
https://www.zacks.com/