Politecnico di Torino

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

Tesi di Laurea Magistrale

Analisi della Cyber Security: Rischi, Costi e Strategie di Protezione per le Aziende

Relatore:
Prof.ssa Laura Abrardi

Candidato:
Aurora Savastano
Numero di matricola: S314347

Anno Accademico 2024/2025

Indice

Indice delle figure

Introduzione

La cybersecurity è una delle principali preoccupazioni per le imprese, sia pubbliche che private, in un mondo sempre più digitalizzato. Le minacce informatiche sono in continua evoluzione, e il costo delle violazioni della sicurezza può essere devastante, sia dal punto di vista economico che reputazionale. Vediamo i costi e i rischi legati alla cybersecurity per le imprese, analizzando separatamente il contesto pubblico e privato.

Con l'aumento della digitalizzazione, le imprese dipendono sempre più dalla tecnologia, rendendo fondamentale l'implementazione della cybersecurity per proteggere i dati e le reti da potenziali attacchi informatici e accessi non autorizzati.

I costi legati alla cybersecurity possono essere suddivisi in costi diretti e costi indiretti, e variano in base alla dimensione dell'impresa, alla sua esposizione a rischi e alla strategia di sicurezza adottata.

I costi diretti includono ad esempio: software di sicurezza, formazione del personale, servizi di consulenza e auditing sistemi di backup e disaster recovery, assicurazioni per la cybersecurity.

I costi indiretti sono meno visibili ma spesso più gravi come ad esempio: interruzione delle operazioni, recupero dei dati e ripristino, perdita di clienti e danni reputazionali, sanzioni legali e normative.

In base ad uno studio svolto da Accenture (2020), i costi globali degli attacchi informatici sono aumentati a 6 trilioni di dollari all'anno e sono destinati a crescere. Mentre, secondo il Cost of a Data Breach Report di IBM (2022), il costo medio di una violazione dei dati a livello globale era di circa 4,35 milioni di dollari, con un aumento rispetto agli anni precedenti.

È più complesso calcolare il costo per investire in cybersecurity all'interno di un'azienda in quanto dipende dalle dimensioni dell'impresa, dal settore e dalle misure di sicurezza adottate.

I principali rischi che può causare un attacco informatico sono: furto di dati sensibili, interruzione della supply chain, attacchi agli impianti produttivi, interferenze politiche e

cyber-attacchi, interruzione dei servizi pubblici essenziali, sovraesposizione al rischio legale e vulnerabilità dei dispositivi IoT.

Il presente elaborato di tesi si suddivide in quattro capitoli ed analizza ognuna di queste dimensioni ponendo l'accento proprio sui costi e sui rischi che si riconducono al settore pubblico e a quello privato.

Capitolo I: La Cyber Security

1.1 Distinzione delle definizioni di "Sicurezza delle Informazioni" e "Cyber Security"

Nel contesto della crescente importanza della “Sicurezza delle Informazioni” e della Cyber Security”, diventa fondamentale individuare le similarità e le diversità tra questi due concetti. I ricercatori, per comprendere il significato e l’applicazione di queste due nozioni, mettono in evidenza le loro differenze sostanziali. (A. G. G., 2024)[1]

La “Sicurezza delle Informazioni” si riferisce alla tutela delle informazioni e dei dati dagli accessi non autorizzati, garantendo riservatezza, integrità e disponibilità.

La “Cyber Security”, invece, si concentra sulla protezione dei sistemi informatici, delle reti e dei programmi dagli attacchi digitali e difende i sistemi informativi da attacchi come hacking, virus, malware ecc.

Tuttavia, per una regolamentazione giuridica efficace è fondamentale distinguere chiaramente questi due concetti, di conseguenza è necessario armonizzare la terminologia per sviluppare standard che permettano di costruire definizioni chiare e univoche. Un'analisi della letteratura esistente mostra che diversi ricercatori hanno proposto definizioni sia per la “Sicurezza delle Informazioni” che per la “Cyber Security”. Tutti i ricercatori considerano la Sicurezza delle Informazioni come un insieme di misure e principi volti a proteggere le informazioni e le infrastrutture da minacce interne ed esterne, sebbene con alcune differenze di interpretazione:

- **Lipkan**: Considera solo gli interessi di individui, società e Stato, sottolineando l’importanza di evitare l’uso illegittimo, la diffusione e la distorsione delle informazioni. (A. L. V., 2010)[2]
- **Tsymbaliuk**: Pone l’accento sull'importanza delle misure legali, organizzative e tecniche per la protezione dell'informazione. (S., 2015)[3]

[1] A., Goncharenko G. On the problem of defining and defining the definitions of "Information Security" and "Cyber Security", 2024
[2] A., Lipkan V., Fundamentals of National Security Of Ukraine, 2010
[3] S., Tsymbalyuk V., Cybersecurity in the National Security System of Ukraine, 2015

- **Horbenko**: Mette in risalto la resistenza dell'ambiente informativo contro minacce interne ed esterne, con l'obiettivo di tutelare i diritti dei cittadini e degli interessi nazionali. (I., 2017)[4]
- **Morozov**: Introduce il concetto di sovranità dei dati vale a dire che i dati sono soggetti alle leggi del Paese in cui sono stati generati. (P., 2018)[5]
- **Tkachenko**: Si focalizza sulla necessità di proteggere le risorse informative in ambito giuridico, sottolineando l'importanza di integrità, riservatezza e disponibilità come principi fondamentali. (V. T. I., 2015)[6]
- **Semeniuk**: Evidenzia la necessità delle relazioni informative e della prevenzione dei danni per proteggere i soggetti coinvolti da minacce sia accidentali che intenzionali. (M., 2019)[7]
- **Melnyk**: Sottolinea l'importanza di garantire il corretto funzionamento delle risorse informative a beneficio dei cittadini e dello Stato per tutelare l'infrastruttura informativa. (O., 2016)[8]

Le definizioni di Cyber Security condividono l'idea della protezione dei sistemi informativi e delle reti, ma con alcune differenze nel modo in cui viene descritta:

- **Lipkan**: Definisce la Cyber Security come l'insieme di misure per proteggere il cyberspazio da minacce interne ed esterne, garantendo integrità, riservatezza e disponibilità. (A. L. V., 2010)[9]
- **Tsymbaliuk**: Identifica nel rischio la componente fondamentale della Cyber Security, derivante dell'uso di tecnologie, processi e pratiche digitali. (S., 2015)[10]

[4] I., Gorbenko O., Information and Cybersecurity: Conceptual Principles and Pratical Aspects, 2017
[5] P., Morozov S., Strategies for ensuring information and cyber security of the state, 2018
[6] V., Tkachenko I., Cybersecurity and protection of information system, 2015
[7] M., Semenyur N., Information security in the context of modern challenges: theory and practice, 2019
[8] O., Melnyk A., Cybersecurity in public administration: theory and practice, 2016
[9] A., Lipkan V., Fundamentals of National Security Of Ukraine, 2010
[10] S., Tsymbalyuk V., Cybersecurity in the National Security System of Ukraine, 2015

- **Horbenko**: Afferma che la Cyber Security è la capacità dei sistemi e delle reti di resistere alle minacce informatiche, garantendo il funzionamento continuo delle tecnologie e proteggendo i dati dall'accesso non autorizzato. (I., 2017)[11]
- **Morozov**: Definisce la Cyber Security come la protezione del cyberspazio e delle infrastrutture critiche dagli attacchi informatici. (P., 2018)[12]
- **Tkachenko**: Descrive la Cyber Security come un processo di gestione dei rischi digitali, che comprende identificazione, analisi e neutralizzazione delle minacce informatiche per garantire stabilità operativa. (V. T. I., 2015)[13]
- **Semeniuk**: Considera la Cyber Security come un insieme di azioni e procedure per un utilizzo sicuro del cyberspazio, evitando l'accesso non autorizzato, la divulgazione e la distruzione delle informazioni digitali. (M., 2019)[14]
- **Melnyk**: Introduce il concetto di Cyber Security come un complesso di politiche, procedure e tecnologie per proteggere dati elettronici e sistemi da accessi non autorizzati, danni e perdite. (O., 2016)[15]

Le definizioni di "Sicurezza dell'informazione" e "Cyber Security" sono strettamente interconnesse, ma ognuna ha il proprio focus. La "Sicurezza dell'informazione" riguarda la protezione di tutte le informazioni, indipendentemente dalla loro forma che siano elettroniche, cartacee o verbali. La "Sicurezza dell'informazione" garantisce tre componenti chiave: la riservatezza, l'integrità e la disponibilità delle informazioni. La riservatezza protegge le informazioni rendendole disponibili solo per coloro che ne hanno il diritto. L'integrità garantisce che le informazioni siano precise e complete, e certifica che vengano modificate solo da persone autorizzate. La disponibilità, infine, garantisce un accesso tempestivo e affidabile alle informazioni per coloro che ne hanno diritto. La sicurezza dell'informazione abbraccia un'ampia gamma di misure e approcci, includendo

[11] I., Gorbenko O., Information and Cybersecurity: Conceptual Principles and Pratical Aspects, 2017
[12] P., Morozov S., Strategies for ensuring information and cyber security of the state, 2018
[13] V., Tkachenko I., Cybersecurity and protection of information system, 2015
[14] M., Semenyur N., Information security in the context of modern challenges: theory and practice, 2019
[15] O., Melnyk A., Cybersecurity in public administration: theory and practice, 2016

politiche, processi e fattori umani per proteggere le risorse informative da minacce interne ed esterne. (V. Z. O., 2021)[16]

D'altro canto, la "Cyber Security" rappresenta un ramo specifico della sicurezza dell'informazione, orientato alla protezione dei sistemi informatici, delle reti e dei software dalle minacce digitali. Questo settore si articola in tre componenti principali: la protezione dell'infrastruttura di rete, la protezione dei dati e la risposta agli incidenti. La protezione dell'infrastruttura di rete è fondamentale per difendersi da attacchi che potrebbero compromettere la rete, mentre la protezione dei dati è essenziale per tutelare le informazioni da accessi non autorizzati e furti. La risposta agli incidenti, infine, si riferisce alla capacità di rispondere efficacemente agli incidenti che possono compromettere la sicurezza dei sistemi. La sicurezza informatica include difese tecniche come firewall, software antivirus e sistemi di rilevamento delle intrusioni, nonché misure per prevenire attacchi informatici, criminalità informatica e altre attività dannose nel cyberspazio.

Pertanto, mentre la sicurezza dell'informazione copre un ampio spettro di misure per proteggere tutte le forme di informazioni, la sicurezza informatica si concentra specificamente sulla protezione dei sistemi digitali contro le minacce informatiche. Entrambi i campi sono essenziali e lavorano in sinergia per garantire una protezione completa delle risorse informative. (V. C. G., 2020)[17]

1.2 Introduzione alla Cyber Security

La Cyber Security è diventata una componente fondamentale per le aziende nell'era digitale. Il crescente utilizzo della tecnologia per la gestione dei dati sensibili, delle attività aziendali e dell'innovazione espone maggiornamente le organizzazioni agli attacchi online. La sicurezza informatica definisce i processi e le normative nate per arrestare l'accesso non autorizzato, gli attacchi informatici ed il furto di dati, alle reti ed ai sistemi informativi.

[16] V., Zakharova O., Information Security: Textbook, 2021
[17] V., Chernenko G., Cybersecurity: modern threats and protection, 2020

1.2.1 Principali minacce informatiche affrontate dalle aziende

Nell'era digitale, le aziende affrontano una vasta gamma di minacce informatiche che possono compromettere le operazioni, mettere a rischio dati riservati e causare perdite finanziarie. È fondamentale che le aziende comprendano queste minacce per implementare misure di sicurezza efficaci e proteggere i propri asset. Di seguito sono elencate alcune delle minacce informatiche più comuni che le aziende devono affrontare:

Attacchi di phishing: Il phishing è una tra le minacce informatiche più comuni ed efficaci contro le aziende. Gli hacker ingannano le persone per ottenere dati attraverso l'uso di email, SMS o siti web falsi. Dopo aver ottenuto questi dati, gli aggressori possono rubare informazioni, lanciare ulteriori attacchi o ottenere accesso non autorizzato ai sistemi aziendali. È difficile per il personale distinguere i messaggi legittimi dagli attacchi perchè sembrano veritieri.

Malware: Il malware rappresenta uno dei programmi più distruttivi in grado di danneggiare un sistema informatico. Con il termine malware si fa riferimento a varie tipologie di software tra cui worm, trojan, spyware e virus. Il malware può infiltrarsi nella rete di un'azienda rubando dati, interferendo con le funzioni di sistema o fornendo agli hacker accesso remoto al sistema, attraverso vari canali, come siti web compromessi, download di software infetti e allegati di posta elettronica.

Ransomware: Il ransomware è una forma di malware che limita l'accesso del dispositivo che "infetta", fino al pagamento di un riscatto da parte della vittima. Un attacco ransomware può avere effetti devastanti, tra cui perdite finanziarie significative, interruzioni delle operazioni aziendali e danni alla reputazione. La doppia estorsione combina il furto e la crittografia de dati perchè l'hacker chiede il pagamento sia per sbloccare le informazioni che per evitare la loro divulgazione.[18]

Minacce interne: Le minacce interne si riferiscono ad un dipendente, un appaltatore o un partner commerciale, che utilizza il suo accesso autorizzato alle risorse di un'organizzazione per danneggiare le informazioni, le reti ed i sistemi aziendali.[19] Si

[18] https://www.checkpoint.com/it/cyber-hub/ransomware/what-is-double-extortion-ransomware/
[19] https://www.fortinet.com/it/resources/cyberglossary/insider-threats#:~:text=In%20genere%2C%20una%20minaccia%20interna,le%20reti%20e%20i%20sistemi%20aziendali.

tratta di rischi più difficili da identificare e contrastare poichè provengono dall'interno dell'azienda. Le minacce interne possono includere il furto di dati, il sabotaggio o la divulgazione involontaria di informazioni riservate a causa di negligenza o ignoranza.

Distributed Denial of Service (DDoS) Attacks: Lo scopo di un attacco DDoS (Distributed Denial of Service) è rallentare gravemente o impedire del tutto al traffico leggitimo di raggiungere la sua destinazione, sovraccaricando il sito web o i servizi online di un'azienda con una quantità eccessiva di traffico, rendendoli inaccessibili agli utenti autorizzati.[20] Per difendersi dagli attacchi DDoS, le aziende possono adottare diverse strategie, tra cui l'uso di reti specifiche di distribuzione dei contenuti (CDN).

Advanced Persistent Threats (APT): Gli APT sono una tipologia di attacchi mirati e duraturi, eseguiti da avversari altamente qualificati e ben finanziati, come Stati nazionali o organizzazioni criminali che cercano di infiltrarsi nella rete di un'azienda. [21]

Attacchi alla Supply Chain: Gli attacchi alla supply chain prendono di mira un fornitore o collaboratori esterni per ottenere l'accesso in un'azienda target. L'inserimento di malware nell'intera catena di fornitura può portare ad un attacco alla supply chain del software, dell'hardware e del firmware. [22]

Ingegneria sociale: Gli attacchi di ingegneria sociale manipolano le persone inducendole a condividere informazioni riservate; mentre a livello aziendale questi attacchi possono portare a perdite finanziarie. L'ingegneria sociale sfrutta tratti psicologici umani come l'errore e la debolezza umana. Le tattiche più comuni utilizzate includono il pretesto (fingere di essere qualcun altro), incutere paura o un senso di urgenza, fare leva sull'avidità, fare appello al buon cuore o alla curiosità. [23] (SSMLG Gudimetla Naga Venkata, 2024)[24]

[20] https://www.akamai.com/it/glossary/what-is-ddos
[21] https://www.cybersecurity360.it/nuove-minacce/minacce-apt-cosa-sono-le-advanced-persistent-threat-come-funzionano-e-come-difendersi/
[22] https://www.keepersecurity.com/it_IT/threats/supply-chain-attack.html
[23] https://www.ibm.com/it-it/topics/social-engineering#:~:text=Gli%20attacchi%20di%20ingegneria%20sociale,che%20compromettono%20la%20loro%20sicurezza
[24] SSMLG Gudimetla Naga Venkata, Abhishake Reddy Onteddu, RamMohan Reddy Kundavaram, Arun Kumar Sandu, Cyber Security in business management, 2024

1.3 Analisi dei principali incidenti cyber noti a livello globale dal 2019 al primo semestre 2024

Nel primo semestre del 2024 si sono verificati numerosi incidenti di sicurezza informatica di rilevanza globale, analizzati confrontando i dati raccolti nei cinque anni precedenti. Il rapporto redatto dal Clusit (Clusit, 2024)[25], si basa sull'analisi di incidenti cyber noti [26], andati a buon fine e di particolare gravità, che hanno avuto impatti significativi in termini economici, tecnologici, legali, reputazionali sulle Organizzazioni vittima degli stessi.

Nel periodo tra gennaio 2019 e giugno 2024 si sono registrati un totale di 12.495 incidenti e nel primo semestre 2024 è stato registrato il numero più alto mai rilevato prima ossia 1.637 eventi. Dal 2019, l'andamento è sempre stato crescente e solo raramente si sono osservate inversioni di tendenza come nel secondo semestre del 2021 e del 2023. Gli incidenti dell'ultimo semestre rappresentano il 13% del totale dal 2019 e segnano un aumento del 23% rispetto al semestre precedente.

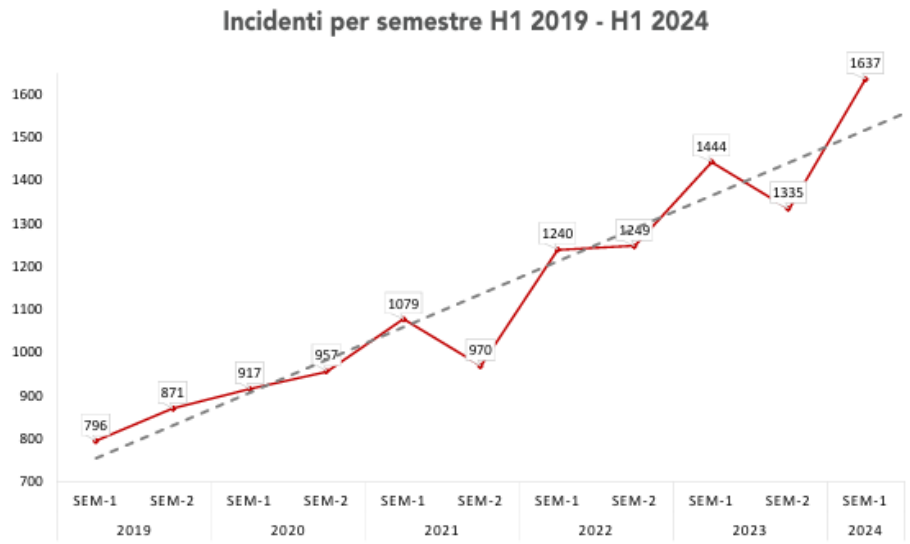

Figura 1: Andamento degli incidenti cyber nel periodo 2019 - H1 2024

[25] Clusit, Rapporto Clusit 2024 primo semestre 2024, https://clusit.it/wp-content/uploads/area_stampa/2024/Rapporto_Clusit_2024_primo_semestre.pdf

[26] G. Faggioli, M. Andreolini, A. Apruzzese, L. Bechelli, G. Butti, S. Castelluccio, G. Cesarone, L. Chiantore, M. Cicognini, G. Dragoni, I. Gabrielli, C. Gatti, P. Girdinio, P. Giudice, C. Giustozzi, A. Greco, L. Ivaldi, M. Leoncini, F.M.R. Livelli, Rapport Clusit, 2024

Conseguentemente, anche la media mensile degli incidenti cyber (Fig. 2) è aumentata considerevolmente, raggiungendo quota 273, più del doppio di quanto avveniva il I semestre 2019.

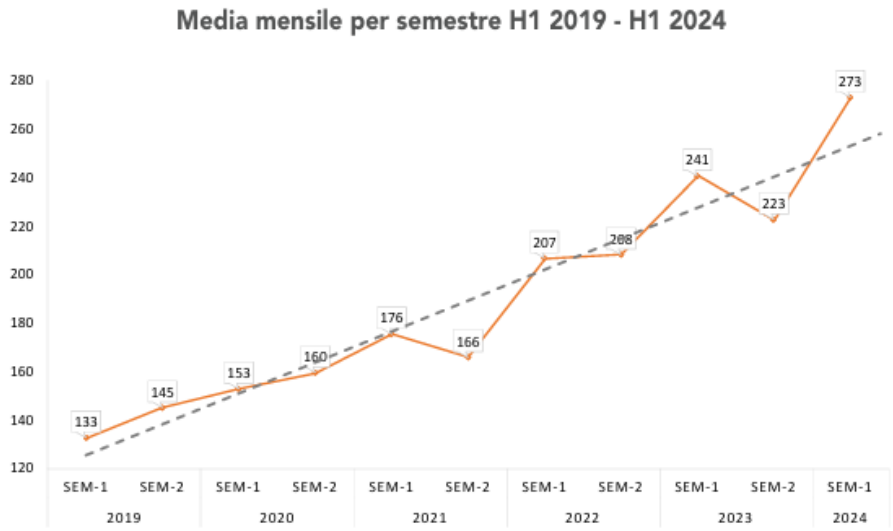

Figura 2: Andamento delle medie mensili nel periodo 2019 - H1 2024

L'aumento del numero di incidenti è principalmente dovuto alla crescita del cybercrime, che rappresenta l'88% del totale, con un incremento di oltre 23 punti rispetto al primo semestre del 2023. Questo dimostra come il cybercrime attiri sempre più l'attenzione della criminalità organizzata, che sfrutta modelli "as-a-Service" per coinvolgere anche soggetti non specializzati in attività cyber. In calo, invece, gli attacchi di tipo espionage, che scendono di oltre due punti percentuali rispetto al 2023, confermando una tendenza

già osservata l'anno precedente. Anche l'hacktivism, dopo un picco di crescita nel 2023, torna in flessione di circa tre punti percentuali, raggiungendo il 6% del totale.

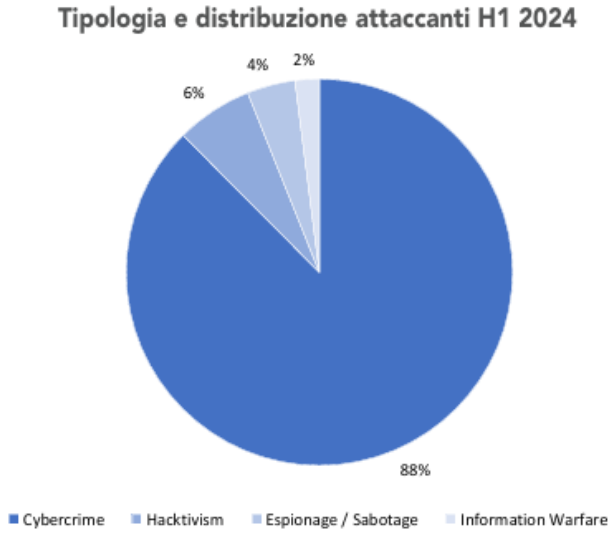

Figura 3: La distribuzione percentuale degli attacchi nel primo semestre 2024

Nel primo semestre del 2024, gli incidenti come Espionage/ Sabotage e Information Warfare sembrano in calo, nonostante l'intensificarsi di conflitti già dal 2023.

Il settore più colpito dagli attacchi continua ad essere l'Healthcare con il 18% degli incidenti registrati, in aumento quasi del 4% rispetto al 2023. Nei primi sei mesi del 2024 si sono verificati 296 attacchi in questo settore, appena 100 in meno rispetto all'intero 2023 e un valore quasi pari a quello del 2022 (304 attacchi).

È la seconda volta dal 2019 che una singola categoria (Healthcare) supera gli incidenti classificati come Multiple Target, che tuttavia continuano a crescere. Il settore Governativo/Militare/Law Enforcement mantiene la terza posizione con il 13% degli incidenti, con un calo di 1 punto percentuale rispetto al 2023. Il settore Finance/Insurance è al quarto posto con l'8% e registra un calo di oltre tre punti percentuali rispetto all'anno 2023. I settori ICT ed Education rimangono stabili rispettivamente al 7% e al 6%, con il primo che mostra una leggera flessione, probabilmente grazie a una maggiore maturità e pressione regolatoria in termini di sicurezza. Il settore Manufacturing, che rappresenta oltre il 5% degli incidenti, conserva la sua posizione in classifica, nonostante sia più colpito in termini assoluti. Il comparto News/Multimedia registra la crescita più significativa, passando dall'ottavo al dodicesimo posto rispetto al 2023. Anche Organizations, Wholesale/Retail ed Energy/Utilities mostrano aumenti preoccupanti, con

il numero di incidenti nel primo semestre del 2024 che supera in alcuni casi il 70% dell'intero anno precedente.

Figura 4: Distribuzione della tiplogia di vittime nel H1 2024

L'analisi della distribuzione geografica delle vittime riflette i cambiamenti nella digitalizzazione e nella normativa sulla cybersecurity a livello globale. Nel primo semestre del 2024, il continente americano resta la regione più colpita con il 41% degli incidenti, sebbene in calo del 3% rispetto al 2023. L'Europa segue con il 29%, con un aumento del 6% rispetto al 2023, rappresentando circa un terzo degli incidenti mondiali. In valore assoluto, i 469 incidenti registrati in Europa nel primo semestre del 2024 corrispondono al 75% del totale del 2023, suggerendo che a fine anno il continente rappresenterà la seconda area più colpita. L'Asia si attesta all'8%, un valore influenzato dalla limitata presenza di normative che obbligano alla notifica degli incidenti. Il 17% degli attacchi ha coinvolto località multiple, mentre Oceania (4%) e Africa (1%) rimangono marginali, sebbene in crescita.

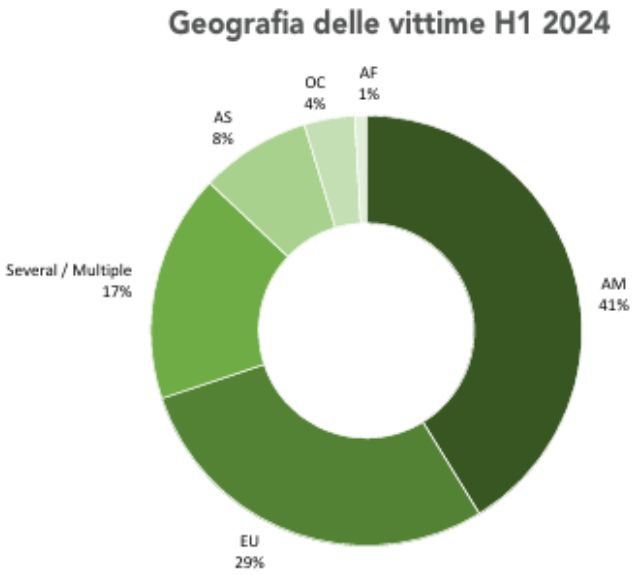

Figura 5: Distribuzione geografica delle vittime in percentuale nel H1 2024

L'analisi delle strategie utilizzate dai cybercriminali permette di comprendere le cause dell'aumento significativo delle minacce rivolte alle nostre aziende e istituzioni. Il malware è la tecnica di attacco più utilizzata, infatti oltre un terzo degli incidenti registrati si riferiscono a questo tipo di minaccia, sebbene ci sia stato un calo dal 36% nel 2023 al 34% nel primo semestre del 2024. Il ransomware si conferma la minaccia principale, grazie all'elevato profitto che offre agli aggressori, spesso organizzati in schemi di affiliazione. Gli attacchi che sfruttano la vulnerabilità restano la seconda tecnica più usata (14%), ma in calo di quattro punti percentuali. Il phishing è stabile all'8%, mentre DDoS e attacchi con tecniche multiple scendono dell'1%. Gli attacchi basati su Identity Theft crescono dell'1%, con un aumento preoccupante in termini assoluti in quanto nel primo semestre del 2024 sono stati registrati più incidenti di questo tipo rispetto a tutto il 2023. Per circa un incidente su quattro (26%) non è possibile determinare la tecnica utilizzata, un dato in aumento di 5% rispetto al 2023.

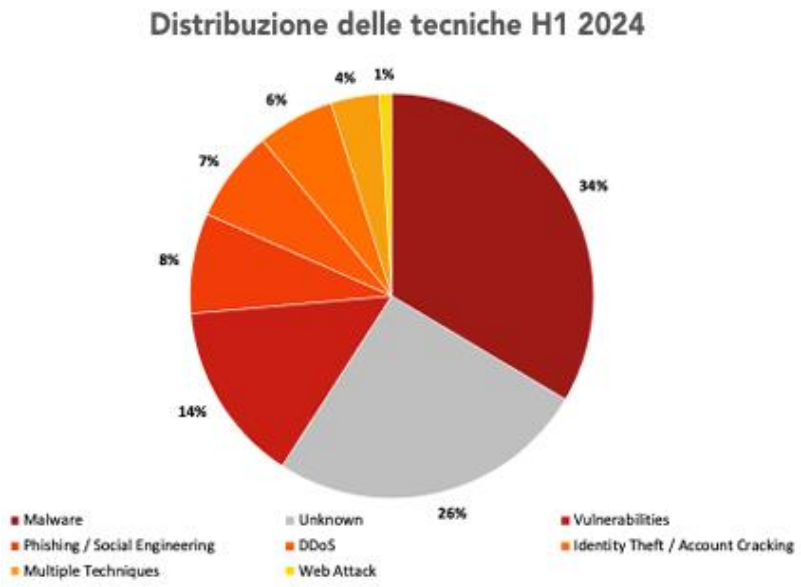

Figura 6: Distribizione delle tecniche di attacco nel H1 2024

L'analisi della gravità degli incidenti mostra che la crescita costante degli eventi critici osservata negli ultimi anni sembra essersi arrestata. Nel primo semestre del 2024, il 31% degli incidenti è stato classificato come Critical, in calo di sette punti percentuali, mentre gli eventi High sono aumentati al 50%, con un incremento di 8%. In valore assoluto, gli incidenti High nei primi sei mesi del 2024 rappresentano il 70% del totale del 2023. Complessivamente, gli incidenti con gravità elevata (Critical e High) costituiscono l'81% del totale, in aumento dell'1% rispetto al 2023. Gli incidenti a basso impatto sono ormai scomparsi dal campione analizzato, che si concentra su attacchi con gravi conseguenze per le organizzazioni a livello globale.

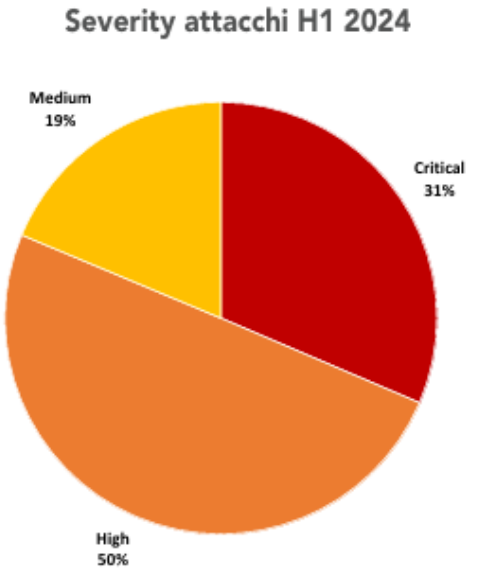

Figura 7: Distribuzione della Severity nel H1 2024

Per quanto riguarda la gravità degli attacchi in base alle tecniche utilizzate, il malware mantiene un livello critico nel 40% dei casi, mentre gli incidenti basati sullo sfruttamento di vulnerabilità vedono un calo significativo della gravità critica, passando dal 60% nel 2023 al 35% nel primo semestre del 2024. La gravità degli attacchi di phishing, DDoS e identity theft si mantiene intorno al 20%, mentre diminuisce l'impatto critico degli attacchi che sfruttano tecniche multiple (dal 50% al 40%) e dei web attack (dal 20% al 10%). Anche le tecniche sconosciute registrano una riduzione della gravità critica, dal 40% nel 2023 al 30% nel primo semestre del 2024.

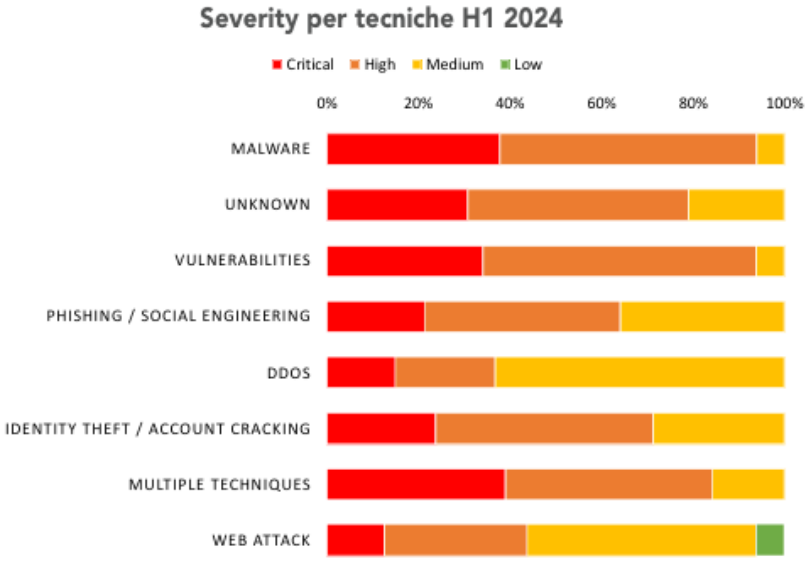

Figura 8: Distribuzione della Severity per tecniche di attacco nel H1 2024

1.4 Analisi degli incidenti cyber in Italia

In questa sezione vengono analizzati gli incidenti cyber in Italia grazie al rapporto redatto dal Clusit [27], offriamo un approfondimento sulla situazione italiana, con una panoramica degli incidenti di sicurezza avvenuti negli scorsi 6 mesi, confrontati con l'andamento dal 2019 in poi. [28]

Nel primo semestre 2024, gli incidenti noti di particolare gravità che hanno coinvolto vittime italiane sono 124. Come si evince dal grafico in Fig. 9, nel primo semestre 2024 si sono registrati lo stesso numeri di attacchi, con una leggera diminuzione, rispetto al primo semestre 2023 (132). Il dato che più deve preoccupare è quello che fa riferimento agli eventi registrati nel secondo semestre del 2023, in cui gli attacchi sono cresciuti di circa il 35% rispetto ai 6 mesi precedenti.

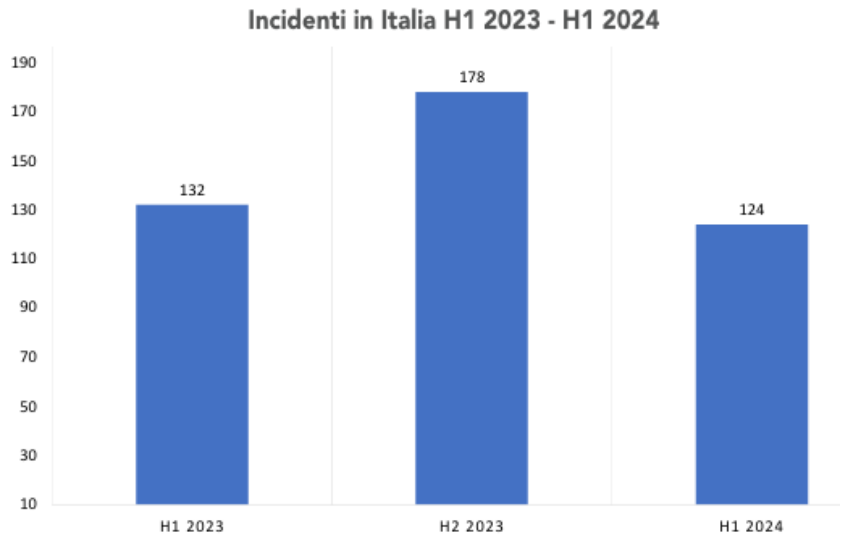

Figura 9: Distribuzione dei cyber attacchi in Italia per semestre nel periodo H1 2023 - H1 2024

Nei primi 6 mesi del 2024, gli attacchi avvenuti con successo contro le realtà del nostro Paese costituiscono il 7,6% (Fig. 10) del totale degli eventi rilevati a livello globale (1.637). Il rapporto tra il numero di incidenti avvenuti in Italia rispetto al campione complessivo globale nei primi 6 mesi del 2024 (7,6%) evidenzia una diminuzione rispetto

[27] G. Faggioli, M. Andreolini, A. Apruzzese, L. Bechelli, G. Butti, S. Castelluccio, G. Cesarone, L. Chiantore, M. Cicognini, G. Dragoni, I. Gabrielli, C. Gatti, P. Girdinio, P. Giudice, C. Giustozzi, A. Greco, L. Ivaldi, M. Leoncini, F.M.R. Livelli, Rapport Clusit, 2024

[28] https://www.newcomm.it/cyber-security/report-clusit-2024/

al primo e secondo semestre del 2024 in cui la percentuale è pari rispettivamente al 9,6% e 12,7%.

Figura 10: L'incidenza degli attacchi in Italia sul campione globale per semestre nel periodo H1 2023 - H1 2024

Per evidenziare alcune tendenze che caratterizzano il panorama degli attacchi in Italia, è utile analizzare la tipologia di attaccanti, indicativa delle finalità degli attacchi e utile per comprendere i fenomeni predominanti da monitorare (Fig. 11). In Italia, la maggioranza degli incidenti noti appartiene alla categoria Cybercrime, infatti si è registrato un aumento dal 2023 al 2024 passando rispettivamente dal 63% al 71%, con una riduzione del 17% rispetto al campione globale (88%, vedere Fig. 3).

Di conseguenza, si riduce la quota degli incidenti classificati come Hacktivism, che rappresentano il 29% del totale. Tuttavia, in Italia questi attacchi hanno un'incidenza significativamente maggiore rispetto al campione globale, dove costituiscono solo il 6% degli incidenti. Oltre un terzo (34%) degli attacchi con finalità di Hacktivism a livello mondiale ha colpito organizzazioni italiane, evidenziando una particolare vulnerabilità del Paese a iniziative di matrice politica o sociale. In Italia, a causa delle minori capacità di prevenzione e mitigazione, gli attacchi mirano alle piccole e medie imprese e alla Pubblica Amministrazione.

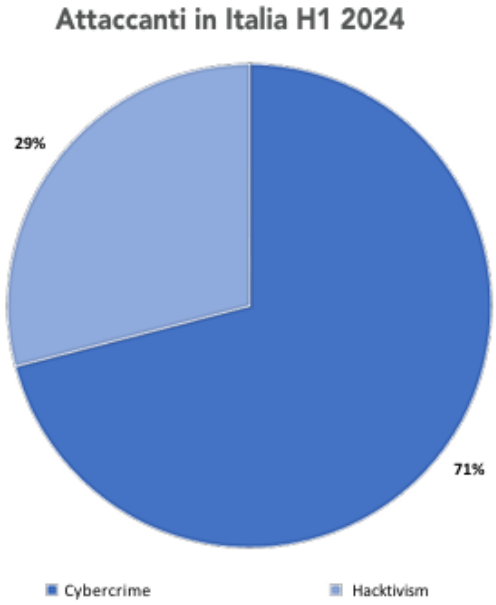

Figura 11: Attaccanti in Italia nel H1 2024

Analizzando la distribuzione delle vittime (Fig. 12), il primo semestre del 2024 mostra variazioni significative che interessano diversi settori. La categoria più colpita dagli incidenti cyber in Italia è il settore manifatturiero (19% del totale), che per la prima volta supera il settore Governativo/Militare/Law Enforcement, ora al terzo posto con l'11% degli attacchi. Questo dato può essere parzialmente attribuito alla minore incidenza dell'Hacktivism nei primi sei mesi del 2024, tuttavia bisogna considerare che nel secondo semestre 2023 gli attacchi Hacktivism sono raddoppiati, di conseguenza è affrettato qualsiasi pronostico per il 2024.

Al secondo posto si colloca la categoria Multiple Targets (13% del totale), la cui rilevanza continua a crescere, in linea con il trend globale, dove occupa una posizione analoga con il 16% degli incidenti. [29] La distribuzione degli attacchi in Italia è molto differente rispetto al campione globale, infatti a livello mondiale, nel settore manifatturiero si registrano solo il 5% degli incidenti (settima posizione), mentre in Italia oltre un quarto (28%) degli attacchi avviene ai danni di realtà manifatturiere. (Manuela Gianni, 2024)[30]

[29] https://www.newcomm.it/cyber-security/report-clusit-2024/
[30] Manuela Gianni, Paola Capoferro, Annalisa Casali, Sofia Ferrante, Le minacce informatiche più pericolose e i principali settori nel mirino, 2024, https://www.digital4.biz/executive/minacce-informatiche-piu-pericolose-settori-colpiti-italia-mondo/

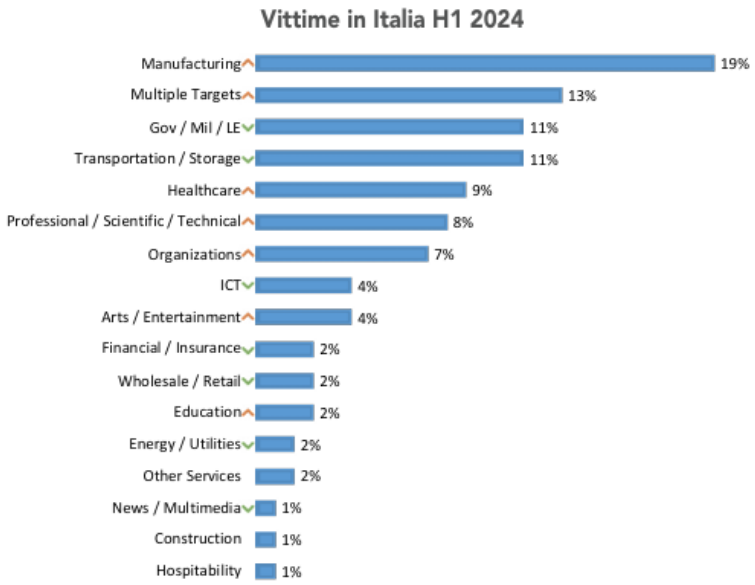

Figura 12: Distribuzione delle vittime in Italia 2024

La crescente eterogeneità dei settori colpiti evidenzia come gli attacchi informatici stiano coinvolgendo vittime in quasi tutte le aree merceologiche. Questa situazione è preoccupante perchè mostra che le misure di difesa adottate non sono all'altezza delle strategie degli attaccanti, e le vulnerabilità esistenti rendono questi obiettivi particolarmente appetibili per i cybercriminali. È una tendenza da monitorare attentamente, poiché in futuro c'è il rischio di un peggioramento, in quanto le tecniche di attacco diventano sempre più sofisticate, anche grazie all'uso dell'Intelligenza Artificiale, ed è fondamentale che anche le contromisure adottate dalle organizzazioni si evolvano di pari passo per fronteggiare adeguatamente le minacce.

Proseguendo nell'analisi, si evidenziano ulteriori settori presi di mira, tra cui Transportation/Storage (11%), Healthcare (9%), Professional/Scientific/Technical (8%) e Organizations (7%). Seguono i comparti ICT e Arts/Entertainment (entrambi al 4%) e Financial/Insurance (poco sopra il 2%). Nel primo semestre 2024, il settore Healthcare ha registrato un numero di incidenti pari a quelli dell'intero 2023, con un incremento dell'83% rispetto al primo semestre 2023, confermando una tendenza preoccupante che si riscontra anche a livello globale.

Rispetto ai primi sei mesi del 2023, le categorie Government e Finance/Insurance, grazie alla loro resilienza superiore alla media, registrano una diminuzione, con un calo rispettivamente dell'11% e del 6,7%. (Manuela Gianni, 2024)[31]

Il malware, come evidenziato dalla Figura 13, registra il 51% degli eventi con un aumento del 20% rispetto al primo semestre 2023, occupando in Italia il primo posto, diventando la tecnica dominante e preferita dai cybercriminali. Questo strumento, risulta spesso difficile da rilevare e offre molteplici opzioni per compromettere i sistemi, aumentando la possibilità di successo e monetizzazione, come nel caso degli attacchi ransomware. [32]

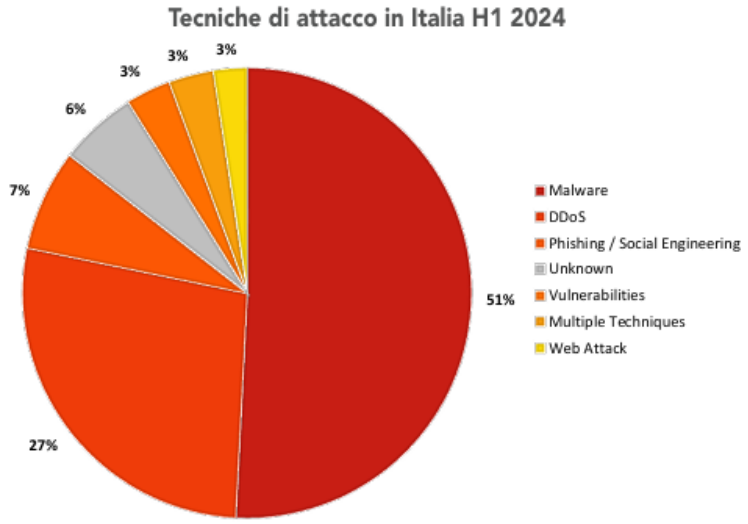

Figura 13: Tecniche di attacco in Italia H1 2024

Gli incidenti DDoS rappresentano il 27% dei casi, con una percentuale più alta rispetto alla media globale (7%), infatti questa è la tecnica di attacco più utilizzata dagli hacktivist per interrompere i servizi di un'organizzazione e sensibilizzare il pubblico sulla loro causa. (Clusit, 2024)[33] Le tecniche di Phishing/Social Engineering, che sfruttano la vulnerabilità del fattore umano, si trovano al terzo posto con il 7%. Sebbene questi attacchi siano in lieve calo, continuano a rappresentare una minaccia significativa per le

[31] Manuela Gianni, Paola Capoferro, Annalisa Casali, Sofia Ferrante, Le minacce informatiche più pericolose e i principali settori nel mirino, 2024, https://www.digital4.biz/executive/minacce-informatiche-piu-pericolose-settori-colpiti-italia-mondo/
[32] https://www.newcomm.it/cyber-security/report-clusit-2024/
[33] Clusit, Rapporto Clusit 2024 primo semestre, 2024, https://clusit.it/wp-content/uploads/area_stampa/2024/Rapporto_Clusit_2024_primo_semestre.pdf

organizzazioni, sia in Italia che a livello internazionale, evidenziando la necessità di potenziare e rendere più efficaci le campagne di sensibilizzazione e formazione per i dipendenti.[34] Gli incidenti della categoria "Unknown" diminuiscono in modo significativo, passando dal 18% nel primo semestre del 2023 al 6%, grazie alle normative che impongono l'obbligo di segnalazione di alcune tipologie di incidenti. (Clusit, 2024) Gli incidenti legati allo sfruttamento di vulnerabilità restano decisamente inferiori a quelli registrati a livello globale (3% rispetto al 14% nel campione complessivo), mentre gli incidenti legati a Multiple Techniques e Web Attacks si attestano anch'essi al 3%. [35]

Per quanto riguarda la severity degli incidenti, i dati italiani (Fig. 14) si distaccano parzialmente da quelli globali. (Giusti, 2024) [36]

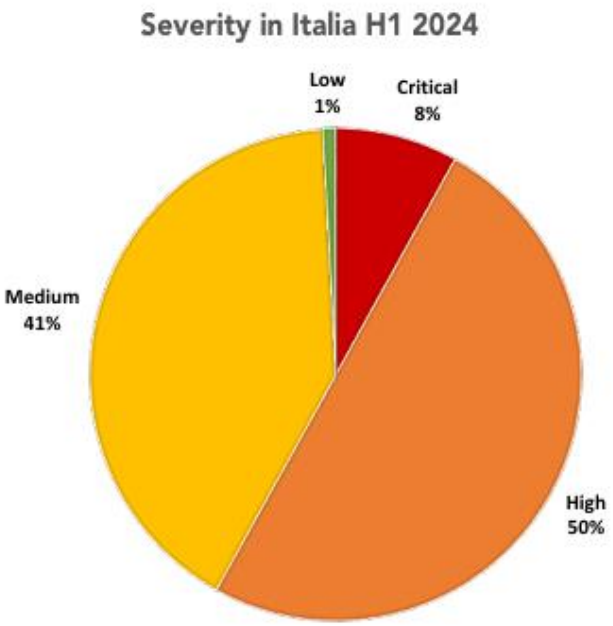

Figura 14: Severity degli attacchi in Italia H1 2024

La categoria "High" è in linea con quella globale (50% degli incidenti), mentre la categoria "Critical" è notevolmente più bassa in Italia (8% rispetto al 31%), e la categoria "Medium" è invece molto più alta (41% contro il 19%). Gli incidenti a basso impatto sono trascurabili in Italia (1%). Complessivamente, il dato suggerisce una tendenza positiva:

[34] https://www.newcomm.it/cyber-security/report-clusit-2024/
[35] https://www.newcomm.it/cyber-security/report-clusit-2024/
[36] https://gdprzerosanzioni.it/news-gdpr-news-privacy/attacchi-informatici-in-italia-aumentati-del-65/

come già osservato nel 2023, gli attacchi che causano danni critici sono meno frequenti in Italia rispetto al resto del mondo, e anche se gli incidenti di impatto medio sono più numerosi, i danni che comportano sono più contenuti.

Rispetto al 2023, si rileva una ulteriore diminuzione della categoria "Critical", che passa dal 20% nel primo semestre 2023 al 13% nel campione complessivo dell'anno e all'8% nei primi sei mesi del 2024, confermando una tendenza in calo che prosegue dal 2022. Al contrario, gli incidenti con severity "Alta" aumentano del 7%, passando al 43% nel 2023, mentre le altre categorie mostrano un andamento stabile.

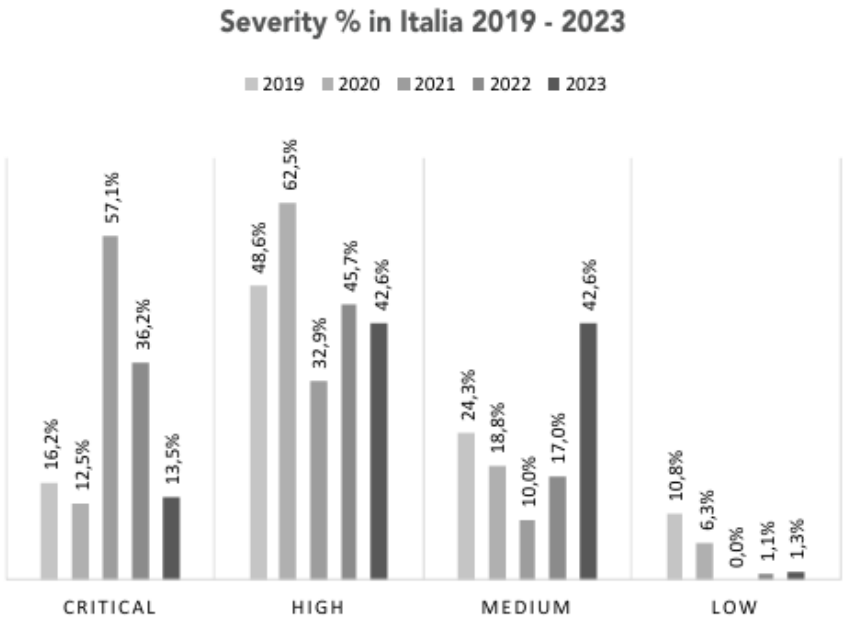

Figura 15: Severity degli incidenti in Italia nel periodo 2019 – 2023

È importante considerare queste tendenze nel contesto globale, ricordando che gli incidenti italiani costituiscono il 7,6% del campione mondiale. (Comitel, 2023)[37] I dati suggeriscono che in Italia una serie di attacchi, potenzialmente meno gravi, non vengono prevenuti o mitigati, rispetto ad altri Paesi, raggiungendo gravità Medium o addirittura High, posizionando il nostro Paese in una posizione più alta nel ranking internazionale. (G. Faggioli, 2024)[38]

[37] Comitel, Rapporto Clusit 2023, 2023, https://www.comitel.net/blog/rapporto-clusit-2023-italia-sotto-assedio/

[38] G. Faggioli, M. Andreolini, A. Apruzzese, L. Bechelli, G. Butti, S. Castelluccio, G. Cesarone, L. Chiantore, M. Cicognini, G. Dragoni, I. Gabrielli, C. Gatti, P. Girdinio, P. Giudice, C. Giustozzi, A. Greco, L. Ivaldi, M. Leoncini, F.M.R. Livelli, Rapport Clusit, 2024

1.5 Prospetto economico sulla Cyber Security a livello globale e nazionale

Negli ultimi anni, gli investimenti nelle soluzioni di sicurezza informatica sono cresciuti notevolmente per affrontare le sempre più numerose minacce nel cyberspazio. Si prevede che il mercato della sicurezza informatica continuerà ad espandersi in modo significativo, con un incremento dei ricavi che dovrebbe raggiungere i 203 miliardi di dollari USA a livello globale entro il 2025. Tra i vari segmenti del mercato, i servizi di sicurezza saranno i principali protagonisti, con un volume di mercato previsto di 103,1 miliardi di dollari USA nel 2025. Inoltre, si prevede che il mercato crescerà a un tasso annuo composto (CAGR) del 7,58% dal 2025 al 2029, arrivando a un volume complessivo di 271,9 miliardi di dollari USA entro il 2029.

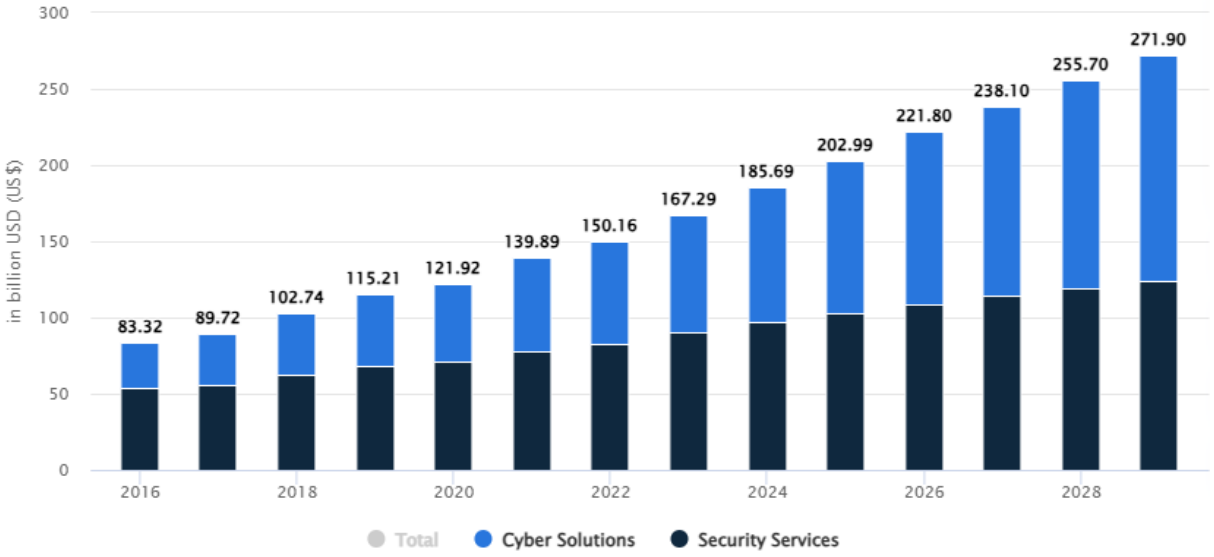

Figura 16: Ricavi del mercato della sicurezza informatica a livello mondiale 2016 - 2029

I crescenti investimenti sono giustificati dal fatto che, a partire dal 2016, gli attacchi informatici registrati sono aumentati, seguendo un trend in crescita fino al 2021, per poi stabilizzarsi negli ultimi anni, come illustrato nella Figura 17.

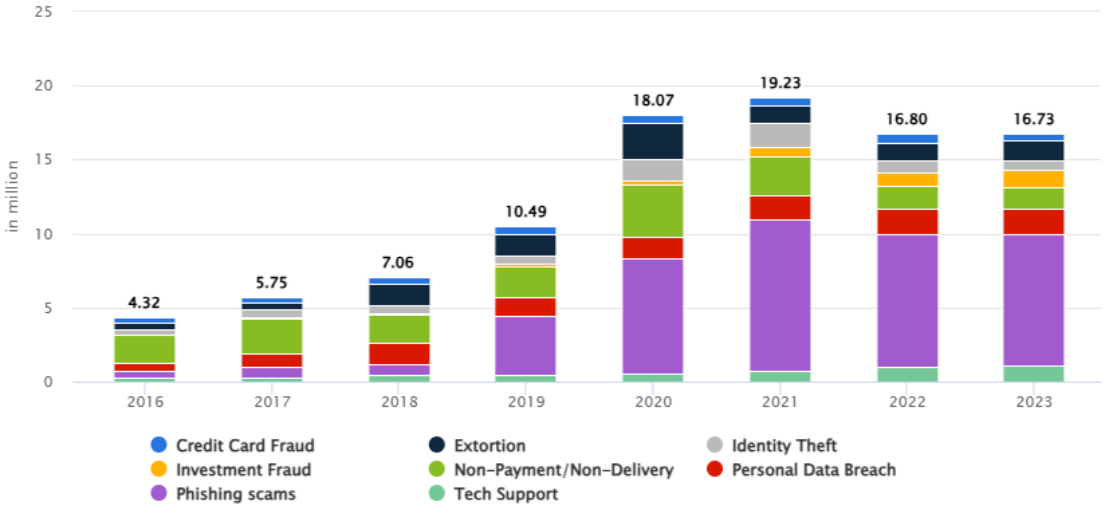

Figura 17: Tipi di attacchi informatici registrati dal 2016 al 2023

Questa tendenza è confermata anche dal costo stimato della criminalità informatica, che nel 2024 è stato valutato in 9,22 trilioni di dollari, con previsioni che indicano un aumento a 15,63 trilioni di dollari entro il 2029. (Cybersecurity - Worldwide, 2024)[39]

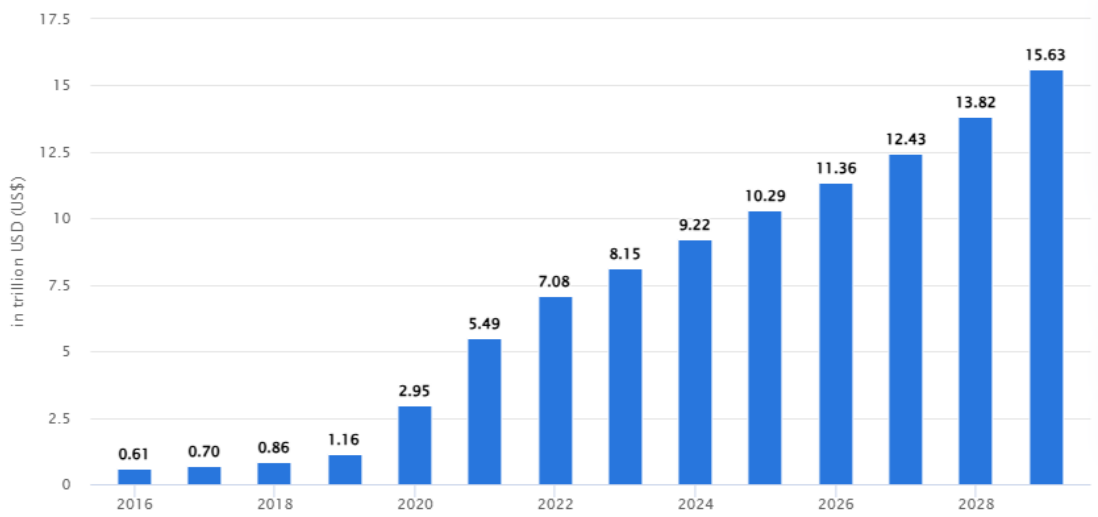

Figura 18: Costi stimati della crimanilità informatica dal 2016 al 2029

[39] Cybersecurity – Worldwide, 2024, https://www.statista.com/outlook/tmo/cybersecurity/worldwide

1.6 Come proteggersi dai danni legati al Cyber Risk: i framework da seguire

Le aziende devono implementare framework e policy di sicurezza informatica dettagliati per proteggere i propri asset digitali, garantire la conformità normativa e mantenere la continuità operativa in un panorama di minacce informatiche in continua evoluzione. Un approccio strutturato alla sicurezza informatica fornisce alle aziende una guida per la gestione del rischio, la difesa dalle minacce e la risposta agli incidenti. Ci sono diversi modelli e framework che possono aiutare le aziende nello sviluppo e nell'implementazione di procedure di sicurezza informatica efficaci.

Risk Management Framework (RMF): Il RMF è un framework che descrive come un'azienda deve essere strutturata e controllata per proteggere i propri asset. Questo framework è costituito da 5 componenti: identificazione, valutazione, attenuazione, creazione di report e governance.[40] Il RMF è stato creato dal National Institute of Standards and Technology (NIST) e si allinea con la funzione Identify di quest'ultimo, poiché permette di identificare e valutare i rischi prima di adottare misure di protezione. L'adozione dell'RMF nel framwork CINI, facilita la definizione delle priorità di intervento e aiuta le organizzazioni nel raggiungimento di livelli di maturità più elevati grazie ad una gestione del rischio ben strutturata.

Difesa in profondità: Il principio di difesa in profondità si basa sulla sovrapposizione di più linee di difesa da parte di un'organizzazione, in questo modo aumenta la probabilità che, se un attaccante riesce a superare una linea di difesa, una successiva lo bloccherà. [41] Alcuni esempi di strategie per implementare la difesa in profondità sono la protezione dei dati, la sicurezza dell'account, la sicurezza degli endpoint, la sicurezza della rete e la sicurezza fisica. La strategia di difesa in profondità si allinea con le funzioni Protect e Detect del NIST Framework, poiché utilizza più livelli di sicurezza; mentre nel Framework CINI, questo framework garantisce un miglioramento graduale delle difese, raggiugendo livelli di maturità dell'organizzazione sempre più elevati.

[40] https://www.servicenow.com/it/products/governance-risk-and-compliance/what-is-risk-management-framework.html#:~:text=Un%20framework%20di%20gestione%20dei,per%20proteggere%20i%20propri%20asset.

[41] https://www.checkpoint.com/it/cyber-hub/cyber-security/what-is-defense-in-depth/#:~:text=Il%20principio%20di%20difesa%20in,organizzazione%20%C3%A8%20vulnerabile%20alla%20difesa.

Architettura Zero Trust: Il modello Zero Trust è un framework che presuppone che nessuna connessione, utente o risorsa sia attendibile finchè non viene verificata. [42] L'approccio Zero Trust, non dà fiducia a priori e verifica continuamente ogni accesso, si allinea con le funzioni Identify e Protect del NIST Cybersecurity Framework e del Framework CINI, che pongono grande enfasi sulla gestione degli accessi (IAM).

Cybersecurity Maturity Model Certification (CMMC): Il CMMC è un framework di verifica progettato per garantire che tutte le aziende della Defence Industrial Base (DIB) implementino pratiche di sicurezza informatica adeguate. Il CMMC è suddiviso in cinque livelli, che spaziano dalle procedure fondamentali di informatica alle misure di sicurezza più sofisticate. Ogni livello si basa su quello precedente, richiedendo azioni sempre più complesse man mano che si sale di livello. Il CMMC è strettamente legato ai Tiers di implementazione del NIST Cybersecurity Framework, che stabiliscono livelli crescenti di maturità nella sicurezza; ed è in linea con il Framework CINI, in quanto i crescenti livelli di maturità (M1-M4), permettono di migliorare la sicurezza delle organizzazioni.

Framework di risposta agli incidenti: Un framework di risposta agli incidenti è un approccio strategico per rilevare e rispondere agli attacchi informatici. Comprende una serie coodinata di procedure come la preparazione, rilevazione, rimozione, test e revisioni post-incidente. [43] Questo framework è strettamente legato alla funzione Respond e Recover del NIST Cybersecurity Framework, fornendo linee guida su come gestire e mitigare gli impatti di un incidente informatico. Nel Framework CINI, la capacità di rispondere agli incidenti è fondamentale per arrivare a livelli di maturità più elevati (M3-M4), poiché consente alle organizzazioni di ridurre il tempo di reazione e limitare i danni.

Security Information and Event Management (SIEM): Il SIEM è una soluzione di sicurezza che aiuta le organizzazioni a riconoscere e affrontare potenziali minacce. I sistemi SIEM aiutano i team di sicurezza aziendali a rilevare le anomalie del comportamento degli utenti, raccogliendo e aggregando dati di log da server, dispositivi di rete e applicazioni. [44] Il Framework SIEM è strettamente legato alla funzione Detect

[42] https://www.trendmicro.com/it_it/what-is/what-is-zero-trust/zero-trust-architecture.html
[43] https://www.wiz.io/it-it/academy/incident-response-fast-track-guide
[44] https://www.ibm.com/it-it/topics/siem

del NIST Framework, assicurando un monitoraggio continuo per individuare eventuali minacce; stessa cosa vale anche per il Framework CINI.

ISO/IEC 27001: ISO/IEC 27001 è uno standard internazionale che mostra le best practices da seguire per la valutazione del rischio e l'implementazione di misure di sicurezza, aiutando le aziende a proteggere i propri asset informativi. Questo standard è fortemente collegato alla funzione Identify e Protect del NIST Cybersecurity Framework, poiché definisce requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS). [45] Nel Framework CINI, la ISO 27001 è uno standard che permette il miglioramento dei livelli di maturità, in particolare nei livelli M2-M4, che richiedono un approccio più strutturato alla gestione dei rischi e ai controlli di sicurezza. (Greatti, 2024)[46]

1.6.1 NIST Cybersecurity Framework

L'acronimo NIST sta per "National Institute of Standard and Technology" che nel 2014 ha pubblicato il documento "Framework for Improving Critical Infrastructure Cybersecurity" (Technology, 2014)[47] nel quale vengono descritte delle best practices da seguire al fine di proteggere i sistemi, i settori e le risorse più importanti per la sicurezza del Paese. Il Framework è suddiviso in tre parti: Core, Implementation Tier e Profile. [48]

Il Core è una struttura che organizza le attività di cybersecurity in cinque funzioni principali: la prima è l'Identificazione (Identify) che per gestire il rischio definisce le risorse critiche, i processi, i sistemi, e i dati. Successivamente la Protezione (Protect) che stabilisce misure di salvaguardia per comprende la gestione delle identità e degli accessi, la formazione, la sicurezza dei dati e la manutenzione. Poi abbiamo la Rilevazione (Detect) che introduce il monitoraggio e l'analisi per identificare tempestivamente gli eventi informatici. Poi abbiamo la Risposta (Respond) che si concentra sulla pianificazione della risposta per contenere e mitigare un incidente rilevato. Infine

[45] https://sicert.net/certificazione-iso-27001/
[46] Greatti, Matteo, Access control: le basi per la sicurezza informatica aziendale, 2024, https://www.agendadigitale.eu/sicurezza/protezione-dei-dati-sensibili-strategie-di-controllo-degli-accessi/
[47] National Institute of Standard and Technology, Framework for Improving Critical Infrastructure Cybersecurity, 2014
[48] https://vitolavecchia.altervista.org/cybersecurity-come-difendersi-dai-cyber-attack-con-nist-cybersecurity-framework-e-framework-cini/

abbiamo il Recupero (Recover) che fornisce linee guida per il ripristino delle funzioni compromesse e il miglioramento della resilienza. (Lavecchia, 2024)[49]

Ogni funzione è ulteriormente suddivisa in categorie e sottocategorie, con riferimenti informativi che offrono standard e linee guida specifiche per l'implementazione.

Gli Implementation Tiers definiscono i livelli di maturità nella gestione del rischio informatico. Sono organizzati in quattro livelli: Tier 1 gestisce il rischio in maniera puntuale; Tier 2 dove la gestione del rischio è approvata a livello dirigenziale; Tier 3 dove i processi di gestione del rischio integrati nelle operazioni aziendali; Tier 4 in cui è l'organizzazione ad adattare le sue pratiche in base ai cambiamenti delle minacce mostrando un elevato grado di flessibilità e innovazione.

I profiles rappresentano un allineamento tra i requisiti di cybersecurity e gli obiettivi aziendali, si distinguono in Current Profile che descrive la situazione attuale della sicurezza e il Target Profile che definisce gli obiettivi per migliorare la sicurezza. Il confronto tra questi profili permette di individuare i punti di debolezza e di sviluppare piani d'azione migliorativi.

Questo Framework sostiene l'adozione di standard internazionali ed è progettato per integrare la cybersecurity nella gestione del rischio aziendale e facilitare la comunicazione tra stakeholder interni ed esterni, utilizzando un linguaggio comune e incoraggiando la cooperazione tra organizzazioni e settori diversi. Le organizzazioni possono utilizzare il Framework per vari scopi come la verifica delle pratiche esistenti (confrontandole con le raccomandazioni del Core per individuare aree di miglioramento), la creazione di un programma di cybersecurity e la comunicazione dei requisiti di sicurezza con fornitori e partner.

[49] Lavecchia, Vito, Cybersecurity: Come difendersi dai cyber-attack con NIST Cybersecurity Framework e Framework CINI, 2024, https://vitolavecchia.altervista.org/cybersecurity-come-difendersi-dai-cyber-attack-con-nist-cybersecurity-framework-e-framework-cini/

1.6.2 Framework CINI

Il "Italian Cyber Security Report" (Franchina, 2015)[50] presenta un Framework Nazionale per la sicurezza cibernetica, adattato dal modello NIST statunitense, che si basa sulle prerogative del panorama italiano che è caratterizzato da un'elevata presenza di PMI. Alcune innovazioni introdotte sono i livelli di priorità ed i livelli di maturità che permettono alle organizzazioni di adattare gli interventi in base alle proprie risorse, capacità e necessità.

Il framework suddivide le azioni in tre categorie principali: Priorità Alta si tratta di misure fondamentali che possono essere molto costose ma garantiscono una base minima di sicurezza; Priorità media si tratta di interventi come il monitoraggio che sono poco costosi ma che aumentano notevolmente la sicurezza; Priorità bassa sono misure complesse da implementare, come le modifiche alle infrastrutture, ma che possono offrire un ulteriore livello di protezione.

La determinazione della priorità si basa su due criteri principali: il primo è la capacità dell'intervento di ridurre il rischio, mentre il secondo è la semplicità di implementazione. Questo approccio consente alle aziende di concentrarsi prima di tutto sugli interventi più critici e di conseguenza gestire le risorse in modo ottimale.

I livelli di maturità permettono di valutare il progresso ed il miglioramento delle strategie di un'organizzazione. I livelli sono: Minimo (M1), Intermedio (M2), Avanzato (M3), Adattivo (M4). Nel primo livello si associano pratiche di sicurezza elementari come la gestione delle credenziali di accesso localmente su ciascun dispositivo, senza una gestione centralizzata. Nel secondo livello le pratiche diventano più strutturate infatti le credenziali sono gestite attraverso una directory aziendale. Nel terzo livello vengono adottate soluzioni specialistiche per proteggere gli accessi privilegiati e gli asset critici. Nel quarto livello la gestione del rischio cyber è completamente integrata nella cultura aziendale.

[50] Franchina, Luca Albertini Stefano Armenia Roberto Baldoni Fabio Battelli Luca Boselli Stefano Buschi Alfredo Caputi Salvatore Carrino Francesco Ceccarelli Ludovica Coletta Romina Colciago Cosimo Comella Fabrizio d'Amore Ciro Di Carluccio Rita Forsi Luisa, Italiano Cyber Security Report, 2015

I livelli di maturità sono definiti specificamente per ciascuna sottocategoria del framework, la combinazione di questi due livelli permette alle organizzazioni di condurre analisi approfondite sul loro stato di sicurezza e pianificare un percorso di miglioramento.

Il report suggerisce priorità elevate e livelli minimi di maturità, per le PMI, in modo da garantire una protezione adeguata senza richiedere sforzi eccessivi. Il framework, per le grandi imprese, è uno strumento per richiedere standard minimi di sicurezza che siano allineati a livello internazionale.

Capitolo II: I costi della cybersecurity per le aziende

2.1 Gli investimenti iniziali

I costi derivanti dalla cybersecurity destinata alle aziende variano molto a seconda di diversi fattori, come le dimensioni dell'azienda, il settore, il tipo di protezione necessaria e la complessità delle operazioni.[51] Tra le principali voci di costo che un'azienda può trovarsi a supportare in ambito di cybersecurity, rientrano:

- Prevenzione e protezione: l'installazione e la manutenzione di firewall, antivirus e soluzioni di protezione avanzata (ne sono un esempio gli *anti-malware*, gli *intrusion detection systems*) possono costare da poche centinaia a decina di migliaia di euro, a seconda della complessità. Anche le soluzioni di backup e soluzioni di *disaster recovery*, fondamentali per il ripristino dei dati in caso di attacchi (ne rappresenta un esempio il *ransomware*), rappresentano un investimento che varia da qualche centinaio a diverse migliaia di euro all'anno, a seconda che si tratti di soluzioni *cloud* o *on-premise*.[52]
- Sicurezza dei dati: Attraverso sistemi di gestione e strategie di crittografia delle informazioni sensibili, si garantisce la protezione di questi ultimi. Le spese da affrontare affinché i dati vengano crittografati possono essere esose in base al loro volume e alla tipologia con la quale vengono criptati.[53]
- Formazione e consapevolezza: È importante prevenire possibili estorsioni di dati, essendo consapevoli di poter subire degli "attacchi phishing", attraverso la formazione del personale; quest'ultimo varia da un minimo di 50 € ad un massimo di 300 € per dipendente ed in base alla durata ed al livello di qualifica.
- Monitoraggio e gestione della sicurezza: Un'altra azione di prevenzione che la stragrande maggioranza delle imprese effettua è quella di rivolgersi ad enti che attuano un monitoraggio attivo delle minacce. Il costo si aggira tra i 1000 € ed i

[51] Sapienza, C. I. S. (2017). Cybersecurity National Lab.

[52] Ibidem.

[53] MANTELERO A., Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.

10000 € al mese rispetto alla tipologia del servizio ed alla grandezza della azienda.[54]

- Gestione degli incidenti e violazioni: in caso di attacco, le aziende devono sostenere costi per il ripristino dei dati, la gestione della crisi, le indagini forensi e le eventuali sanzioni. Il costo può rilevarsi considerevolmente elevato, con cifre che partono da migliaia di euro per le piccole violazioni, ma che arrivano a milioni di euro in caso di grandi attacchi (ne è un esempio il *ransomware* che paralizza le operazioni aziendali).[55]
- Compliance e audit: un aspetto importante è ottenere la conformità delle normative nei vari paesi; dunque, è necessario rivolgersi a società di consulenza affinché vi siano anche degli adeguamenti tecnologici. L'investimento è tanto più alto quanto è il grado di conformità a cui si vuole ambire.[56]
- Software e licenze: Sul mercato vi sono dei software, che è possibile acquistare con licenze di durata personalizzata, capaci di monitorare azioni malevole oppure di ridurre l'esposizone a rischi.

Anche se l'investimento iniziale può sembrare alto, la cybersecurity è fondamentale per salvaguardare l'azienda da costi ben più gravi derivanti da attacchi, perdita di dati o danni alla reputazione.

Gli investimenti iniziali in cybersecurity per un'azienda variano a seconda delle dimensioni, della complessità e dei rischi legati al settore.

Tra i più importanti investimenti iniziali che un'azienda potrebbe affrontare per implementare una solida protezione informatica, vi sono quelli relativi all'infrastruttura di sicurezza in cui rientrano i firewall ed i sistemi di protezione, ossia una protezione di base contro intrusioni e attacchi. Il costo varia da 500 € a 5.000 € per firewall aziendali

---

[54] BUTTARELLI G., The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law 6.2 (2016): pp. 77-78.

[55] Montessoro, P. L. (2019). Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale. *LE ISTITUZIONI DEL FEDERALISMO*, *40*(3), 783-800.

[56] Ibidem.

di livello intermedio (per aziende di piccole/medie dimensioni). Le soluzioni *enterprise* possono arrivare a 20.000 € o più.[57]

Vi sono i sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), con un costo che varia da 1.000 € a 10.000 € in base alla complessità e alla dimensione della rete.

Per quel che concerne i *software antivirus* ed *anti-malware*, è possibile affermare che si tratta di un investimento in soluzioni antivirus avanzate e anti-malware, che non solo rilevano ma anche bloccano attacchi da virus e altre minacce. Il loro costo varia da 10 € a 50 € per licenza annuale per singolo dispositivo, ma per soluzioni aziendali complete, i costi possono salire a 1.000 € – 10.000 € all'anno.[58]

In merito ai sistemi di *backup* e *disaster recovery*, è possibile menzionare i *backup* locali e *cloud*, validi per garantire la protezione dei dati e poterli ripristinare rapidamente in caso di attacchi (un esempio si riconduce sempre al *ransomware*). Il costo per un sistema di backup base può partire da 500 €, ma per soluzioni aziendali scalabili e sicure (in cloud o su server aziendali), i costi possono partire da 5.000 € fino a oltre 20.000 € per grandi aziende.

Per quel che concerne la crittografia dei dati vi sono i sistemi di crittografia dei dati utili per proteggere le informazioni sensibili durante il transito e l'archiviazione. Il loro costo varia da 1.000 € a 10.000 €, in base al tipo di soluzione e al numero di dispositivi da proteggere.[59]

Relativamente ai controlli di accesso e autenticazione si afferma che i sistemi di gestione degli accessi ed autenticazione multifattoriale (MFA) sono utili per assicurarsi che solo gli utenti autorizzati possano accedere a dati o applicazioni sensibili.

---

[57] PEARSON S., Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. IFIP International Conference on Trust Management. Springer, Cham, 2017.

[58] RABAN Y., Privacy Accountability Model and Policy for Security Organizations (20121 C. Raab, Information Privacy: Ethics and Accountability, Ethik in den Kulturen-Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn (2017), p. 335, URL: https://inria.hal.science/hal-01651158v1/preview/450659_1_En_15_Chapter.pdf#page=2.

[59] MANTELERO A., Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.

La stima per la spesa di un pacchetto standard riferita ad un solo dipendente si aggira tra i 100 € ed i 500 € annui, diversamente un piano che copre qualsivoglia soluzione può raggiungere anche la cifra di 10000 €.[60]

Prestazioni di consulenza iniziale e audit di sicurezza sono necessari allo scopo di mettere in luce le fragilità dell'infrastruttura IT scongiurando situazioni rischiose per l'azienda stessa. Anche in questo caso è possibile spendere fino a 10000€ rispetto alla dimensione dell'infrastruttura e dunque della compagnia.

Altro fattore molto importante è l'implementazione di policy di sicurezza, si tratta della creazione di politiche di sicurezza aziendale, gestione delle password, sicurezza delle reti interne. I costi legati alla consulenza possono variare da 2.000 € a 15.000 € o più, a seconda delle dimensioni dell'azienda.[61]

Per quel che concerne la formazione e la consapevolezza, la formazione del personale implica di investire nella formazione continua per insegnare ai dipendenti a riconoscere le minacce comuni (*phishing*, *social engineering*, ecc.) e seguire le *best practices* di sicurezza. Il costo può variare da 500 € a 5.000 € per formazione annuale di dipendenti (con soluzioni *di e-learning* o corsi personalizzati).

Un importante settore poi si riconduce anche al monitoraggio della sicurezza e SIEM, si tratta di uno strumento per raccogliere e analizzare i dati di sicurezza in tempo reale, identificare minacce e vulnerabilità. Il costo per una piccola/mediana azienda, in merito alle soluzioni SIEM possono variare da 3.000 € a 10.000 € per l'installazione iniziale, mentre per soluzioni *enterprise*, il costo può salire fino a 50.000 € o più.

Nell'ambito delle licenze software e per gli aggiornamenti, inclusi sistemi di gestione delle vulnerabilità, firewall, strumenti di crittografia, ecc., il costo varia da 500 € a 5.000 € all'anno per licenze, in base al tipo di software scelto.[62]

---

[60] PEARSON S., Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. IFIP International Conference on Trust Management. Springer, Cham, 2017, URL: https://inria.hal.science/hal-01651158v1/preview/450659_1_En_15_Chapter.pdf#page=2.

[61] Ibidem.

[62] MANTELERO A., Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.

Si reputa peculiare anche la protezione per dispositivi mobili, ossia la sicurezza mobile (MDM), valida per gestire e proteggere dispositivi mobili e tablet utilizzati dai dipendenti ed il cui costo oscilla da 5 € a 50 € per ciascun dispositivo all'anno, ad ogni modo le soluzioni aziendali possono sfiorare anche i 10.000 € annuali per proteggere in blocco i dispositivi.[63]

Dunque alla luce di quanto appena analizzato, per quel che concerne le piccole imprese, gli investimenti iniziali in cybersecurity potrebbero aggirarsi intorno ai 5.000 € /15.000 €, con soluzioni di base come firewall, antivirus, backup e formazione.

Gli investimenti per le medie e grandi imprese possono partire da 20.000 € fino a superare i 100.000 €, a seconda delle soluzioni utilizzate come SIEM, crittografia dei dati e soluzioni di *disaster recovery*.

La cybersecurity rappresenta una spesa fondamentale per proteggere le aziende dagli attacchi informatici, si tratta di costi che possono essere sostenuti anche progressivamente, partendo da soluzioni base e arrivando pian piano a soluzioni più complesse.[64]

2.2 I costi operativi

Tra le spese che un'azienda deve sostenere periodicamente vengono collocati proprio quelle legate alla cybersecurity, tutelando il più possibile i loro sistemi dai pericoli come gli attacchi informatici. Tali spese, vengono affrontate cronologicamente dopo quelli che sono i costi degli investimenti iniziali legati all'installazione e configurazione delle infrastrutture. Si annoverano tra i costi operativi correlati alla cybersecurity, quelli relativi alla manutenzione, aggiornamento ed implementazione dei sistemi di sicurezza.

Gli aggiornamenti software si riconducono ai software di sicurezza (ossia *firewall*, *antivirus* ed i sistemi di protezione) richiedono aggiornamenti periodici per rimanere efficaci contro nuove minacce. I costi legati all'aggiornamento sono solitamente inclusi

---

[63] JASMONTAITE L., V. VERDOODT, Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights. Privacy and Identity Management. Time for a Revolution?, S. MAGUIRE, A metadata-based architecture for user-centered data accountability, Electronic Markets 25.2 (2015): 155-160

[64] Ibidem.

nelle licenze annuali o nei contratti di supporto. Per soluzioni aziendali avanzate, i costi di manutenzione possono variare da 1.000 € a 10.000 € all'anno, a seconda della complessità.[65]

In merito a manutenzione e supporto tecnico, l'assistenza continua si reputa necessaria per risolvere gli eventuali problemi tecnici e per applicare *patch* di sicurezza. Il costo oscilla da 1.000 € a 20.000 € all'anno per aziende di dimensioni medie o grandi, a seconda della quantità di sistemi da supportare e dei contratti di assistenza stipulati.

La formazione continua e la sensibilizzazione prevedono i corsi di formazione per dipendenti ed essi sono utili per mantenere il personale aggiornato sui rischi di sicurezza (ossia *phishing*, gestione delle password, protezione dei dati, ecc.), è importante fare formazione periodica.

Le spese che si affrontano sono influenzate dal modo in cui vengono erogate le lezioni per la formazione; infatti, con le nuove piattaforme di e-learning è possibile contenerle fino ad importi di 500 € annui per dipendente, invece per le aziende più strutturate quest' ultima può durare anche svariate settimane l'anno arrivando a costare anche 5000 € l'anno.

In aggiunta, è possibile anche organizzare simulazioni personalizzate di attacchi informatici al fine di testare la preparazione dei propri dipendenti e la capacità di operare sotto pressione, migliorandone, così, la prontezza e favorendo lavori di team building. Analogamente la somma da affrontare è in linea con il range di prezzi precedente.

Qualora vi siano degli incidenti di sicurezza è imprescindibile operare secondo strategie ben definite in modo da limitarne i danni. Per far ciò, è necessario mostrare un'alta responsività, circoscrivendo la violazione e cercando di ripristinare l'integrità del sistema con un efficace risposta. Sicché, particolare attenzione va posta nell'ambito della gestione degli incidenti, i danni a cui si va incontro sono di gravità esponenziale, comportando costi che vanno dalle poche decine di migliaia di euro, fino a centinaia di migliaia di euro.[66]

---

[65] Baldoni R., Luca Montanari Editors. 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness. Università degli Studi di Roma La Sapienza. 2014 https://www.sicurezzanazionale.gov.it/sisr.nsf/ sicurezza-in-formazione/la-cyber-security-in-italia.html

[66] BUTTARELLI G., Hitting the ground running: How regulators and businesses can really put data protection accountability into practice, Keynote speech at European Data Protection Days (EDPD)

Per quanto riguarda tipologie di attacco come i ransomware o quelli mirati, l'azienda potrebbe andare incontro a danni di entità ancora maggiore e trovarsi a dover recuperare i dati persi oltre a ripristinare l'integrità del sistema, perdendo la stima degli investitori. I danni monetari a cui si va incontro nel caso di attacchi ransomware possono superare svariati milioni di euro, inoltre si potrebbe anche incorrere in problemi legali.[67]

Vi sono le licenze software ed i rinnovamenti annuali mediante le licenze antivirus ed i firewall, per cui molte soluzioni richiedono rinnovi annuali delle licenze software.

Il costo può variare da 100 € a 1.000 € per dispositivo, ma per le soluzioni aziendali complete (antivirus aziendali, firewall e crittografia), i costi possono oscillare da 5.000 € a 30.000 € all'anno.

Vi sono anche i software di gestione delle vulnerabilità che si occupano di monitoraggio e gestione continua delle vulnerabilità nel sistema ed il costo va da 2.000 € a 20.000 € all'anno per licenze aziendali.

Per i costi di conformità e *audit*, è possibile menzionare l'*audit* di sicurezza e certificazioni per rispettare normative come il GDPR o altri standard di sicurezza (ossia ISO 27001, SOC 2), le aziende devono condurre audit periodici e ottenere certificazioni di sicurezza. Il costo va da 5.000 € a 50.000 € all'anno per *audit* e consulenze legali, a seconda della complessità e della frequenza.[68]

Infatti, le violazioni del GDPR comportano sanzioni nell'ordine di milioni di euro; di pari passo vi sono anche le spese che deve coprire l'azienda per la sua salvaguardia e difesa, quando avvengono queste violazioni di sicurezza. È l'azienda stessa che, per prevenire l'integrità della propria infrastruttura, deve monitorare la gestione dei dispositivi mobili, anche detta MDM, affinché le apparecchiature elettroniche abbiano un grado di sicurezza tale per cui non ci siano aperture verso l'esterno. In questo caso, le somme spese variano tra i 5 ed i 50 € annui per singolo dispositivo adattati alla grandezza della compagnia.

Dunque, se parliamo di piccole aziende i costi annuali a cui si va incontro possono arrivare a circa 20.000 € ; per le medie imprese, ci aggiriamo su somme che vanno da 20.000 € fino a 100.000 € che includono licenze software, monitoraggio, aggiornamenti

---

Conference Berlin, 15 May 2017, URL: https://www.edps.europa.eu/sites/default/files/publication/17-05-15_edpd_keynote_speech_en_0.pdf.

[67] Ibidem.

[68] Ibidem.

e corsi di formazione; infine, per le grandi aziende si può arrivare a costi operativi annuali che vanno oltre 100.000 € euro qualora si dovessero verificare eventi quali cyberattacchi o perdite di dati.[69]

Per le grandi aziende, invece si richiedono delle soluzioni più complesse e una protezione avanzata, potrebbero affrontare costi operativi annuali superiori a 100.000 €, con potenziali picchi legati a incidenti o attacchi di grande portata.

I costi operativi per la cybersecurity sono continui e vanno gestiti come una parte essenziale del budget aziendale. Una buona gestione della sicurezza e investimenti in prevenzione e formazione possono ridurre i costi futuri legati a incidenti di sicurezza e violazioni.[70]

2.3 Costi di monitoraggio e gestione

Un importante tipologia per migliorare il processo di protezione e, dunque, di aumentare la sicurezza dell'azienda stessa, e il monitoraggio della cybersecurity. In contemperanza con quanto detto in precedenza, questi variano secondo la grandezza della azienda ed alla ramificazione dell'infrastruttura IT. Di seguito un'analisi dettagliata dei principali costi di monitoraggio e gestione che le aziende possono sostenere:

Un *Security Operations Center* (SOC) rappresenta una soluzione di monitoraggio continua che analizza i dati e rileva eventuali minacce in tempo reale. Può essere gestito internamente o affidato a un provider esterno.[71]

Per quel che concerne il SOC interno, l'azienda crea un proprio team di esperti in cybersecurity che monitorano le reti 24/7. Questo richiede l'assunzione di personale specializzato, strumenti software, e infrastrutture adatte. I costi vengono suddivisi in:

---

[69] JASMONTAITE L., V. VERDOODT, Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights. Privacy and Identity Management. Time for a Revolution?, S. MAGUIRE, A metadata-based architecture for user-centered data accountability, Electronic Markets 25.2 (2015): 155-160

[70] Ibidem.

[71] CAFAGGI F., P. IAMICELI E G.D. MOSCO [2012], Gli ultimi interventi legislativi sulle reti, in Il contratto di rete per la crescita delle imprese, a cura di F. Cafaggi, P. Iamiceli, G.D. Mosco, Milano, p. 489 ss.

- Personale: la paga per figure come analisti di sicurezza, responsabili SOC e tecnici di supporto va da 50.000 € a 150.000 € annui per singolo dipendente ed in base all'esperienza.
- Tecnologie: Programmi software che effettuano monitoraggio e rilevamento di vulnerabilità, analisi dati con cifre nell'ordine di decine fino a centinaia di migliaia di euro.
- Costo totale annuo: le spese a cui l'azienda va incontro, per un dipartimento di sicurezza interno, dipendono dalla sua dimensione e oscillano tra i 150.000 € ed i 500.000 € euro.

Nell'ambito del SOC gestito esternamente, molte aziende scelgono di esternalizzare il monitoraggio a provider specializzati in SOC-as-a-Service. Il costo per un SOC esterno varia in base al livello di servizio e alle dimensioni della rete aziendale. Tipicamente, il costo per un servizio esterno di monitoraggio delle 24 ore può variare da:

- Piccole aziende: 1.000 € a 5.000 € al mese
- Medie imprese: 5.000 € a 20.000 € al mese
- Grandi aziende: 20.000 € a 100.000 € al mese

Il sistema SIEM (Security information and event management) permette di identificare le minacce attraverso i dati derivanti dal firewall, antivirus e sistemi di monitoraggio.[72]
L'implementazione di un sistema SIEM può essere costosa, in quanto richiede licenze, infrastrutture di gestione, e risorse per configurare e gestire il sistema. Tali software richiedono necessariamente la realizzazione di un sistema adeguato al loro funzionamento, infatti i costi di licenze, gestione e di risorse per la sua configurazione possono risultare esose.
Per piccole aziende si stimano somme che vanno da circa 5.000 € all'anno, mentre per implementazioni aziendali più avanzate, possono superare i 50.000 € all'anno.
In base alla dimensione della rete e del livello di monitoraggio desiderato, I costi operativi addizionali (personale, supporto, configurazione) possono aggiungere tra 10.000 € e 100.000 € annui.

[72] CAFAGGI F., P. IAMICELI E G.D. MOSCO [2012], Gli ultimi interventi legislativi sulle reti, in Il contratto di rete per la crescita delle imprese, a cura di F. Cafaggi, P. Iamiceli, G.D. Mosco, Milano, p. 489 ss.

Per rendere prevedibili e facilmente affrontabili gli attacchi è essenziale rilevare tempestivamente e continuamente le criticità e le lacune presenti nella rete, un esempio possono essere dei software obsoleti o configurazioni imprecise. Tali azioni vengono effettuate da programmi che utilizzano strumenti automatizzati affinché si possa scansionare con azioni regolari queste difformità, identificando falle o potenziali rischi. I costi sostenuti si possono suddividere in servizi di monitoraggio per piccolo e medie imprese che partono da un minimo di 500 € ad un massimo di 5.000 € all'anno, mentre per le grandi imprese le spese possono arrivare a più di 50.000 €.[73]

I servizi di risposta agli incidenti possono essere utilizzati anche per simulare attacchi e preparare l'azienda ad una risposta rapida ed efficace in caso di emergenza. Il costo da affrontare in seguito ad un incidente di sicurezza può variare da 10.000 € a 100.000 € o più, rispetto alla complessità e alla sua durata; il servizio consta della gestione dell'incidente, il recupero dei dati, la gestione legale e la salvaguardia della propria reputazione.

L'analisi continua dei dati di sicurezza e la generazione di report aiuta le aziende a comprendere meglio il loro profilo di rischio e a prendere decisioni efficaci per la gestione della sicurezza. [74]

Il costo del software di analisi/reporting può partire da 1.000 € a 10.000 € all'anno per soluzioni di base, ma può arrivare a 50.000 € o più per soluzioni avanzate o personalizzate destinate a grandi aziende.

Gli strumenti IAM aiutano nel monitoraggio per riconoscere azioni sospette o non autorizzate e si assicurano che solo persone autorizzate possano accedere ai dati sensibili. Le spese per l'implementazione di soluzioni IAM variano da 2.000 € a 50.000 € all'anno, a seconda della dimensione dell'azienda e della complessità dei sistemi.

Alla luce di quanto riportato, possiamo affermare che per le piccole realtà i costi di gestione, possono variare da 10.000 € a 50.000 € all'anno, con l'utilizzo di servizi di SOC esterni e software di monitoraggio delle vulnerabilità; nelle medie imprese, i costi annuali

---

[73] Ibidem.

[74] DENHAM E., delivered this speech at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017. She discussed the role of accountability in the GDPR, underlining that "We're all going to have to change how we think about data protection", URL: https://medium.com/the-secure-one/gdpr-makes-accounting-interesting-52c4bc53d05b.

di monitoraggio e gestione potrebbero oscillare tra 50.000 € e 150.000 €, includendo l'utilizzo di un SOC esterno, software SIEM e strumenti di analisi degli eventi di sicurezza. [75]

Nelle grandi aziende, con una rete complessa e una protezione avanzata, potrebbero affrontare costi annuali di monitoraggio e gestione superiori a 150.000 € all'anno, con servizi di SOC interni, sistemi SIEM avanzati, e una gestione continua delle vulnerabilità. I costi di monitoraggio e gestione sebbene possano risultare onerosi, sono essenziali per mantenere una difesa robusta contro le minacce informatiche in maniera tale da ridurre il rischio di gravi violazioni e per rilevare e rispondere tempestivamente agli attacchi.[76]

2.4 Costi di conformità

I costi di conformità costituiscono le spese che un'azienda deve supportare per garantire che le sue operazioni e pratiche siano in linea con le normative e gli standard di sicurezza informatica e protezione dei dati. Questi costi sono strettamente legati alla necessità di rispettare leggi e regolamenti nazionali e internazionali come il GDPR (*General Data Protection Regulation*), il PCI-DSS (*Payment Card Industry Data Security Standard*), la ISO/IEC 27001 (standard internazionale per la gestione della sicurezza delle informazioni), e altre normative specifiche di settore.[77] Un'analisi dettagliata dei costi di conformità legati alla cybersecurity prevede:

I. Audit e Certificazioni di Sicurezza

Relativamente a questa dimensione, le aziende devono sottoporsi regolarmente a audit di sicurezza per verificare la conformità alle normative e agli standard di sicurezza. Gli audit di sicurezza e compliance aiutano ad identificare eventuali lacune nella protezione dei dati e nella gestione della sicurezza. Relativamente ai costi:

[75] Ibidem.

[76] Ibidem.

[77] Mosco, G. D. (2017). La collaborazione tra imprese per la sicurezza informatica. *LUISS LAW REVIEW*, (2), 157-165.

- Gli audit interni possono rivelarsi meno costosi, tuttavia richiedono comunque la disponibilità di esperti interni. I costi per un audit interno possono variare da 5.000 € a 20.000 € all'anno.
- Gli audit esterni da parte di società di consulenza specializzate, garantiscono la conformità alle normative come il GDPR o PCI-DSS, e possono costare tra 10.000 € e 50.000 € all'anno, a seconda delle dimensioni dell'azienda e della complessità delle operazioni.

È molto impegnativo ottenere una certificazione come la ISO 27001 sia in termini di tempo che di risorse; infatti il costo per ottenere una certificazione ISO 27001 può variare da 10.000 € a 50.000 € per un'azienda di dimensioni medie, con costi annuali di mantenimento che possono variare da 5.000 € a 20.000 €.[78]

II. Adeguamento alle Normative di Protezione dei Dati (ne è un esempio il GDPR)

Le normative come il GDPR, soprattutto in UE, considerano la protezione dei dati personali una delle principali preoccupazioni per le aziende moderne. La consultazione legale spacializzata in privacy è necessaria per assicurarsi che vengano rispettate le normative, in maniera tale da implementare le politiche adeguate. Il costo legato alla consulenza legale sulla privacy può variare da 5.000 € a 20.000 € per la consulenza iniziale, con costi annuali di mantenimento che possono andare da 2.000 € a 10.000 €.

Inoltre, le aziende puntano a creare politiche aziendali per la protezione dei dati personali, la gestione delle richieste di accesso e la gestione dei consensi. Il costo varia da 2.000 € a 10.000 € per sviluppare politiche di privacy e procedure interne per la gestione dei dati.[79]

III. Formazione e Sensibilizzazione del Personale

Una parte significativa della conformità riguarda la formazione del personale per garantire che tutti i dipendenti siano consapevoli delle normative e delle *best practices* in ambito di sicurezza informatica e protezione dei dati.

È possibile menzionare la formazione obbligatoria (a titolo esplicativo, vi è il GDPR, sicurezza dei dati, privacy): le aziende devono fornire formazione continua al personale riguardo alle politiche di protezione dei dati e alle minacce informatiche. Il costo per la

---

[78] Baldoni, R., & De Nicola, R. (2015). Il futuro della Cybersecurity in Italia. *CINI-Consorzio Interuniversitario Nazionale Informatica*.

[79] Brighi, R., & Chiara, P. G. (2021). La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE. *Federalismi. it*, *21*.

formazione su GDPR e sicurezza dei dati può costare tra 500 € e 5.000 € all'anno per dipendente, a seconda della modalità (comprende e-learning, sessioni in aula e workshop).[80]

IV. Strumenti e Software per la Conformità

Le aziende necessitano di strumenti e software per garantire che i loro comportamenti siano conformi alle normative e per gestire le pratiche di protezione dei dati. Il costo per i software di gestione della conformità può variare da 1.000 € a 50.000 € all'anno, in base alla soluzione scelta e della dimensione dell'azienda.

Le aziende necessitano di un sistema per rilevare, notificare e gestire le violazioni dei dati per rispettare le normative con il GDPR. Gli oneri oscillano tra 1.000 € e 10.000 € all'anno per tali strumenti, a seconda della complessità. [81]

V. Monitoraggio e Reporting Continuo

Le aziende devono monitorare continuamente i dati ed i sistemi aziendali per garantire che siano conformi alle leggi sulla protezione dei dati. Ciò include la gestione dei diritti degli utenti, come il diritto di accesso e il diritto alla cancellazione dei dati. Affinché le aziende siano conformi con quanto detto in precedenza, è necessario che investano in soluzioni coerenti e che possano generare automaticamente report. I costi di monitoraggio continuo possono variare da 5.000 € a 30.000 € all'anno, a seconda del software scelto e del numero di utenti o dati trattati. [82]

VI. Gestione dei Rischi e delle Sanzioni

È fondamentale avere un programma di gestione dei rischi per ridurre al minimo il rischio di violazioni e le relative sanzioni. A tal proposito, alcune aziende scelgono delle assicurazioni per la protezione della privacy, per coprire eventuali multe o danni legati a violazioni della privacy e della sicurezza dei dati. Le cifre per queste ultime si aggirano tra 5.000 € e 50.000 € all'anno, a seconda della dimensione dell'azienda e del livello di copertura.

---

[80] Mosco, G. D. (2017). La collaborazione tra imprese per la sicurezza informatica. *LUISS LAW REVIEW*, (2), 157-165.

[81] Brighi, R., & Chiara, P. G. (2021). La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE. *Federalismi. it*, *21*.

[82] Ibidem.

VII. Sanzioni e multa per inadempimento

La non conformità nei confronti delle normative può implicare delle sanzioni legali o multe significative, il GDPR prevede multe che possono arrivare fino al 4% del fatturato annuo globale di un'azienda per violazioni gravi. Le sanzioni per la non conformità possono essere collegate a quelle per la violazione della privacy e della protezione dei dati, e possono variare da alcune migliaia di euro a milioni di euro, a seconda della gravità dell'infrazione.[83]

Nell'ambito dei costi di conformità, alla luce di quanto appena affrontato, si evince che presso le piccole aziende i costi di conformità possono variare da 5.000 € a 20.000 € all'anno, comprendendo audit, formazione, consulenza legale e software di base. Per le medie imprese, si va incontro a prestazioni comprese tra 20.000 € e 100.000 €, includendo i costi per le certificazioni, audit esterni, strumenti di gestione e formazione continua.

Per le grandi aziende, che devono rispettare normative internazionali più stringenti e gestire un elevato numero di dati, i costi di conformità possono superare i 100.000 € all'anno, includendo spese per audit complessi, software avanzati e consulenze legali specializzate. I costi di conformità, sebbene rappresentino un investimento, si reputano essenziali per evitare sanzioni legali e danni reputazionali derivanti da violazioni delle normative.[84]

2.5 Costi indiretti

Spese ausiliarie che si è costretti a sostenere sono quelle necessarie al funzionamento dei servizi di protezione ed ai loro strumenti. Queste ultime impattano direttamente sull'azienda andando a minarne la reputazione, la produttività e la redditività.

1. Perdita di reputazione e di clienti

Aver subito dei cyberattacchi o qualsivoglia violazione della privacy, ha un importante impatto direttamente su quella che è la fiducia nei confronti degli investitori dei partner e può portare alla cessazione di un rapporto, compresa la clientela a cui si è rivolti.

---

[83] Liotta, A. (2017). Una spinta delle imprese verso la Cybersecurity: l'iperammortamento come strumento di politica fiscale per l'innovazione. *LUISS LAW REVIEW*, (2), 143-156.

[84] Ibidem.

Infatti, subendo una perdita di clienti, questa ha un effetto diretto sugli introiti dell'azienda, stimando un danno reputazionale con la diminuzione di circa il 30% del ricavato annuale nei settori interessati.

Un altro aspetto da considerare in seguito agli avvenimenti sopracitati è la criticità di reperire nuovi clienti che non siano stati sfiduciati in precedenza, la difficoltà nel fronteggiare deimrisarcimenti danni e la perdita del proprio personale.

2. Aumento del turnover del personale

Le violazioni della sicurezza possono generare insicurezza tra i dipendenti, spingendoli a cercare opportunità lavorative altrove.[85] Per incentivare il personale a rimanere, molto spesso è necessario aumentare i salari o offrire premi, ma tutto ciò rappresenta un costo elevato per le aziende. Le spese di assunzione, formazione e integrazione dei nuovi dipendenti possono ammontare a 5.000 € - 20.000 € per ogni nuovo assunto, a seconda delle posizioni e del livello di esperienza.

3. Interruzione delle attività e perdita di produttività

Un attacco informatico, come ransomware o un'intrusione nei sistemi aziendali, può causare interruzioni delle attività aziendali. Il fermo dell'attività può ridurre la produttività, danneggiare la produzione e influire negativamente sul servizio al cliente.

In merito al costo relativo a ciò, è possibile menzionare la perdita di tempo e la disconnessione dai sistemi aziendali possono generare perdite che vanno da 2.000 € a 50.000 € al giorno a seconda della dimensione e del settore dell'azienda. Grandi aziende o settori come l'e-commerce possono subire perdite più gravi.

4. Costi legali e sanzioni

L'azienda, in caso di violazione, deve affrontare azioni legali e difendersi da cause molto costose da parte di clienti, partner o autorità di regolamentazione. Il costo legato ad un'azione legale può variare da 5.000 € a 500.000 € o più a seconda della gravità e della complessità del caso. In caso di non conformità a normative come il GDPR, le sanzioni possono arrivare fino al 4% del fatturato annuo globale in caso di violazioni gravi.[86]

5. Aumento dei costi assicurativi

---

[85] D'Ambrosio, M. (2022). Cybersecurity e project management: partnership necessaria. *Project Manager: 51, 3, 2022*, 19-26.

[86] Ibidem.

In seguito ad un attacco informatico, le aziende potrebbero dover rivedere le proprie polizze assicurative, aumentando i premi tra il 10% ed il 50% rispetto ai costi pre-attacco, a seconda della gravità dell'incidente.

6. Perdita di contratti e relazioni commerciali

La violazione della sicurezza può influire sulle relazioni con i partner commerciali, in quanto questi potrebbero percepire un maggiore rischio nel collaborare con un'azienda vulnerabile. Il costo come la perdita di contratti o la rottura di accordi con fornitori o partner può tradursi in perdite dirette per l'azienda. Alcuni partner potrebbero chiedere un risarcimento o decidere di non rinnovare gli accordi. Questo impatto può variare da 5.000 € a 500.000 €, a seconda dell'importanza dei contratti e degli accordi coinvolti.

7. Costi per il rafforzamento della sicurezza

L'azienda deve aumentare gli investimenti nella cybersecurity per migliorare le difese, ed evitare che si ripetano ulteriori attacchi in futuro.[87] Il costo legato all'aggiornamento delle soluzioni di sicurezza (come l'implementazione di un Firewall più avanzato, sistemi SIEM o detection & response tools) comporta spese aggiuntive che variano da 10.000 € a 100.000 € o più, a seconda delle dimensioni dell'azienda e della natura dell'incidente.[88] Se un attacco comporta la perdita o la corruzione di dati aziendali, l'azienda deve affrontare costi per recuperarli che possono oscillare da 10.000 € a 500.000 € o più, a seconda della gravità dell'incidente e della quantità di dati persi o compromessi.

8. Perdita di vantaggio competitivo

Nel caso in cui i dati sensibili o i segreti aziendali vengono rubati, l'azienda potrebbe andare in contro ad una perdita di vantaggio competitivo. I concorrenti potrebbero sfruttare tali informazioni per guadagnare un vantaggio sul mercato, con un impatto stimato fino al 20 – 30% sulla competitività dell'azienda.

Alla luce della trattazione appena esposta, i costi indiretti si riconducono al danno reputazionale, ossia alla perdita di fiducia dei clienti e la riduzione delle vendite può comportare perdite significative, anche fino al 30% del fatturato.

---

[87] Giacomello, G. (2018). Cybersecurity: human security. *Human Security*, (7).

[88] Onofri, S., Spagnuolo, C., & Tocci, F. (2017). Cyber Security: Agile, Prince2© e il Penetration Testing. *PROJECT MANAGER (IL)*, (2017/31).

Si rileva anche una fuga di risorse umane, per cui l'assunzione e la formazione di nuovi dipendenti possono costare tra 5.000 € e 20.000 € per ogni nuovo assunto.
In merito all'interruzione delle attività, la *downtime* può generare perdite che vanno da 2.000 € a 50.000 € al giorno.[89]
Nella dimensione dei costi legali e fiscali, le azioni legali e le sanzioni possono variare da 5.000 € a 500.000 €, a seconda della gravità.
Inoltre, l'incremento dei costi assicurativi si riconduce all'aumento dei premi assicurativi che può variare dal 10% al 50% rispetto ai costi pre-attacco.
Per quel che concerne, invece, gli investimenti in cybersecurity, il miglioramento delle difese può costare da 10.000 € a 100.000 €.
I costi indiretti della cybersecurity sono frequentemente sotto stimati, ad ogni modo, essi possono rivelarsi devastanti per un'azienda ed il loro impatto economico può superare di gran lunga i costi diretti di protezione.
Le aziende devono tenere conto di questi costi nel complesso della pianificazione della sicurezza informatica con lo scopo di mitigare i rischi legati agli attacchi e alle violazioni.[90]

[89] Ibidem.

[90] di Karolina Muti, O. C., & La Rocca, G. (2023). Il sistema-Paese Italia di fronte alle sfide dello spazio: tra space economy, cooperazioni internazionali e cybersecurity, URL: https://www.iai.it/sites/default/files/iai2315_en.pdf

Capitolo III: I rischi per l'azienda senza una adeguata cybersecurity

3.1 Furto di dati sensibili

Il maggior rischio a cui è sottoposta un'azienda, qualora non adotti delle misure adeguate contro i pericoli legati agli attacchi informatici, è proprio il furto di dati sensibili. Tali dati sono direttamente collegati sia alle informazioni personali dei clienti sia a quelle legate all'azienda stessa e possono comprendere anche strategie aziendali, dati finanziari, fino ad arrivare a documentazioni riguardo la proprietà intellettuale.

Le sanzioni legali a cui si va incontro sono regolamentate, come detto in precedenza, da normative quali il GPDR, inoltre vi è anche una perdita di denaro indiretta dovuta all'appropriazione indebita della proprietà intellettuale e di dati finanziari che causerebbero rispettivamente un vantaggio alla concorrenza e la possibilità di frodi economiche.[91]

È, dunque, imprescindibile adottare un efficace strategia di cybersecurity per scongiurare tali rischi, proteggendo dati, promuovendo la formazione del personale e dei clienti esterni, monitorando le reti aziendali e implementando continuamente la propria infrastruttura di difesa.[92]

3.2 Compromissione della privacy

La compromissione della privacy rappresenta uno dei principali rischi derivanti dalla mancanza di una cybersecurity adeguata. La divulgazione non autorizzata di informazioni personali espone le vittime al rischio di furto d'identità e frodi finanziarie. [93]

Le imprese che non rispettano le normative in tema di protezione dei dati, come il GDPR in Europa o il CCPA in California sono costrette a pagare multe significative e ad affrontare azioni legali.[94]

---

[91] Sotira, N. (Ed.). (2020). *Il fattore umano nella cyber security: Valori e strategie da costruire insieme*. FrancoAngeli.
[92] Ibidem.
[93] Baldoni, R., De Nicola, R., Prinetto, P. E., Anglano, C. F., Aniello, L., Antinori, A., ... & Zanero, S. (2018). Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici.
[94] Ibidem.

La compromissione della privacy implica l'esposizione di informazioni aziendali riservate o segreti commerciali, tutto ciò comporta anche danni agli utenti finali, tra cui stress psicologico, perché le persone si sentono violate nel loro spazio privato e danno economico, in quanto gli utenti subiscono perdite finanziarie dirette.
In questo modo i concorrenti riescono ad ottenere informazioni strategiche cruciali che mettono a repentaglio la competitività dell'azienda.
I dati compromessi che includono preferenze o comportamenti di acquisto, potrebbero essere usati da terze parti per scopi di marketing aggressivo o per vendere informazioni a terzi senza il consenso dell'utente. [95]

3.3 Interruzione delle operazioni aziendali

L'interruzione delle operazioni aziendali è un altro grave rischio connesso all'assenza di adeguate misure di cybersecurity. Gli attacchi ransomware, tra le principali cause di blocco operativo, impediscono l'accesso ai dati aziendali fino al pagamento di un riscatto, paralizzando le attività e causando perdite finanziarie. Anche se l'azienda recupera i dati, il tempo di inattività ha comunque un costo elevato.[96]
Un altro scenario che può causare l'interruzione delle operazioni aziendali è il furto o la distruzione dei dati aziendali. Se i dati critici, come documenti finanziari, registrazioni delle transazioni, piani di produzione o altre informazioni vitali, vengono persi o compromessi, l'azienda potrebbe trovarsi incapace di operare. Senza l'accesso ai dati, le aziende potrebbero dover sospendere i loro processi operativi fino a quando non vengano ripristinati. Questo porta a ritardi, perdita di produttività e, nei casi più gravi, a danni irreversibili alla gestione aziendale.
Molte aziende dipendono da sistemi informatici e piattaforme digitali per operare. Un attacco che comprometta i server aziendali, i sistemi di *cloud computing* o le reti aziendali può paralizzare completamente le operazioni aziendali. La perdita di accesso a questi sistemi potrebbe portare a gravi disagi, non solo per l'azienda ma anche per i clienti. La capacità di comunicare con i clienti, gestire ordini o fornire servizi potrebbe essere

[95] Ibidem.
[96] Baldoni, R., & Montanari, L. (2016). Italian national cyber security framework. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 168). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

interrotta. Le aziende potrebbero affrontare l'impossibilità di eseguire transazioni, rispondere alle richieste dei clienti o gestire il proprio inventario, con effetti negativi sulle entrate e sulla soddisfazione del cliente.

La dipendenza dalle tencologie per la gestione della catena di approvvigionamento e della produzione rende molte aziende vulnerabili a interruzioni operative. Il blocco dei sistemi ERP e di controllo della produzione può fermare la distribuzione dei prodotti, causando ritardi nelle consegne e difficoltà nel soddisfare la domanda dei clienti. Ripristinare le operazioni dopo un attacco richiede tempo e risorse, aumentando i costi aziendali.[97]

Se le comunicazioni aziendali sono compromesse (ad esempio, mediante attacchi di *phishing* o la compromissione delle piattaforme di email aziendali), l'azienda potrebbe non essere in grado di comunicare efficacemente con dipendenti, clienti e fornitori.

La perdita di accesso alle comunicazioni impedisce la coordinazione tra i team interni, ritarda la risposta alle esigenze dei clienti e compromette le relazioni con i fornitori, interrompendo i flussi di approvvigionamento e aumentando i tempi di risposta.

Il recupero da un'interruzione delle operazioni aziendali talvolta implica dei costi elevati. Questi includono il tempo e le risorse necessarie per ripristinare i sistemi, correggere i danni, e prevenire future violazioni. Oltretutto, le aziende potrebbero dover assumere esperti di *cybersecurity* per identificare e rimediare alla causa dell'interruzione.

I costi legati alla gestione dell'incidente, al ripristino della normale operatività e alla messa in sicurezza dei sistemi aumentano significativamente, spesso supera i guadagni aziendali a breve termine.

Un'interruzione prolungata delle operazioni aziendali ha un impatto diretto sul fatturato e sulle finanze aziendali, in quanto si rischia che i clienti si rivolgano alla concorrenza e l'azienda perde vendite o contratti importanti.

La perdita di fiducia da parte dei clienti e dei partner commerciali può essere difficile da recuperare. I danni economici legati alla perdita di vendite, alla necessità di compensare i clienti insoddisfatti, e alla perdita di opportunità di business possono avere un impatto a lungo termine sulla sostenibilità dell'azienda.[98]

---

[97] Weis, D. (2024). The Evolving Threat Landscape: Understanding Cyber Threats in the Digital Age. In *Boardroom Cybersecurity: A Director's Guide to Mastering Cybersecurity Fundamentals* (pp. 3-11). Berkeley, CA: Apress.

[98] Ibidem.

3.4 Danni alla reputazione

La Web reputation si riconduce al reperimento ed al controllo di supervisione, condotto mediante l'ausilio internet, di tutto quello che viene pubblicato online e che si riferisce ad uno specifico prodotto, ma anche servizio, progetto, evento, azienda o individuo.

La reputazione digitale costituisce un complesso di informazione, idee e riflessioni raccolti tramite il web su un certo brand che si sceglie di analizzare, un prodotto o quindi anche un servizio.

Essa non può essere confrontata, tuttavia va obbligatoriamente maturata nel tempo, per mezzo di molteplici prassi ed azioni.[99]

Le diramazioni riconducibili al web marketing, le quali si rendono necessarie alla creazione e allo sviluppo continuo della reputazione digitale, sono numerose.[100]

Generalmente all'interno della dimensione del web, affinché un'azione si possa ritenere di una certa utilità e funzionale, si sostiene occorra in primis articolare una strategia che punti ad un definito scopo e porti avanti un lavoro carico di costanza e di organizzazione.

Le community, i blog e i siti social si identificano come i contesti favoriti entro i quali il consumatore diviene consapevole circa la reputazione aziendale. qualità/prezzo.[101]

La concezione legata al termine "reputazione" risale agli inizi del Novecento, anni in cui, Henry Ford permise le prime legittimazioni ufficiali verso la reputazione aziendale, affermando che *"gli affari che generano solo profitti in denaro e nessun beneficio sociale non danno valenza all'immagine dell'impresa e pertanto si qualificano come affari poveri"*.[102]

Il concetto che si riconduce alla reputazione aziendale si affaccia sulla scena nella letteratura economica durante gli anni *'70 e '80, a motivo dell'*esigenza di comprendere il modo in cui gli stakeholder prendono delle decisioni in merito ad un'azienda di fronte a dati non precisi o ad ogni modo parziali.[103] Ogni cosa assume un volto diverso dagli anni '90, effettivamente, durante una fase precedente rispetto a questo periodo, le imprese non potevano basarsi su degli studi approfonditi circa la corporate reputation che gli

---

[99] Krasnow, M.M., Cosmides, L., Pedersen, E.J., Tooby, J. (2012). What Are Punishment and Reputation for? PLoS ONE ,7, pp. 45-62.

[100] Ibidem.

[101] Web reputation: cos'è la reputazione digitale e perché è importante?, 2020, consultabile al sito: https://www.bluemilk.it/it/articoli/web-reputation-cose-la-reputazione-digitale-e-perche-e-importante-it

[102] Farmer R., Glass B., *Building web reputation systems*, O'Reilly Media, Inc., 2010.

[103] Inversini A., Cantoni L., Dimitrios B., "*Destinations' information competition and web reputation*.", Rivista di Information technology & tourism 11.3, 2009, pp. 221-234.

rendessero possibile l'elaborazione di adeguate strategie di gestione della stessa: tutto si dimostrava essere stabile per cui una "positiva" reputazione si riteneva essere più desiderabile rispetto ad una negativa. Tuttavia durante gli anni *'90 prende avvio un reale stravolgimento, epoca in cui gli studi sulla reputazione aziendale progrediscono in maniera considerevole e cominciano ad approfondire in maniera specifica la capacità di tale asset di generare del valore*.[104] Benché vi siano una molteplicità di studi e approfondimenti in merito, non è ancora possibile evincere una definizione universale e condivisa circa la "reputazione" in grado di rappresentare tutta la complessità legata al concetto. Buona parte delle definizioni fruibili si accorpano tra di loro, consentendo di abbracciare nuove soluzioni, le altre si dimostrano essere invece dissonanti. Tra le prime formulazioni, è possibile menzionare quella di Fombrun, il quale si è occupato di fondare la Reputation Institute [105] nel 1996:

«La definizione di "reputazione aziendale" si qualifica come una rappresentazione percettiva delle azioni del passato dell'organizzazione e delle prospettive future che servono per descrivere la sua generale attrattività verso i portatori di interesse, confrontandola con i suoi principali concorrenti».[106]

La reputazione online può estendersi prevalentemente a due settori, quello inerente la dimensione personale e un altro riconducibile alla dimensione aziendale. In merito alla reputazione aziendale si definisce come web reputation aziendale, invece quando si esamina quella di un soggetto si farà riferimento alla web reputation personale. Volendo approfondire la questione, la web reputation personale si presenta come il prodotto derivante dal complesso delle azioni che la medesima porta avanti nel mondo dell'online, per tale ragione si ritiene necessario riservare una certa accuratezza verso ciascun contenuto che l'individuo o l'azienda pubblicherà, una raffigurazione o un commento. ciascuna traccia che si lascia in merito alla persona o all'azienda sul web stabilisce obbligatoriamente la propria reputazione personale.[107]

---

[104] Ibidem.

[105] Park C., Lee T. L., "*Information direction, website reputation and eWOM effect: A moderating role of product type.*" Rivista di Journal of Business research 62.1, 2009, pp. 61-67.

[106] Fombrun C.J., *Reputation: realizing value from the corporate image,* Harvard Business School Press, Boston, 1996, p. 72.

[107] Krasnow, M.M., Cosmides, L., Pedersen, E.J., Tooby, J. (2012). What Are Punishment and Reputation for? PLoS ONE ,7, pp. 45-62.

Per quel che invece concerne la web reputation di tipo aziendale, la questione si presenta pressocché similare. Il focus si colloca costantemente all'interno del contenuto pubblicato online, ad ogni modo non influiscono solo le azioni effettuate dalla medesima azienda ma anche le considerazioni e azioni effettuate dagli altri (per menzionare un esempio, vi sono gli utenti o i dipendenti aziendali). Le implicazioni e le conseguenze legate ad una pessima web reputation possono gravare in maniera incisiva sul business, creando l'effetto di un allontanando i possibili nuovi clienti.[108]

Essere in possesso di buona reputazione online positiva, si ritiene fondamentale, sia per i soggetti fisici che per la dimensione aziendale, in quanto per ciascuna delle due sfere settoriali, la reputazione digitale grava obbligatoriamente in merito al proprio operato.[109]

Volendo fornire una prima analisi teorica di insieme, si può menzionare la *"teoria di mantenimento delle norme gruppali"*, secondo il cui pensiero, la reputazione si correla alla capacità di fornire supporto e mantenimento nel tempo delle regole cooperative del gruppo. In tale eventualità si conferisce una valenza al conseguimento, mediante la cooperazione, di obiettivi condivisi negli interessi gruppali e si presume che siano puniti coloro i quali non rispettano le regole che si dimostrano essere vantaggiose per ognuno dei membri del gruppo. Un'ulteriore teoria è quella definita come *"teoria dello scambio sociale"*, in base alla quale, una reputazione positiva e valida promuove l'evoluzione dei rapporti personali benefici, fondati sulla fiducia reciproca, e il conseguimento di vantaggi individuali superiori. Di conseguenza vengono puniti coloro i quali si muovono azionando uno svantaggio nei confronti di terzi o sono scarsamente produttivi.[110]

In base al pensiero dei teorici Krasnow, Cosmides, Pedersen e Tooby, ognuna delle teorie si può ritenere valida, tuttavia esse sono in possesso di un differente potere predittivo, in base alle circostanze. Ognuna delle due teorie, effettivamente, può fornire delle spiegazioni, in circostanze differenti, in merito a quali siano gli obiettivi attesi per mezzo dell'attuazione di strategie cooperative e, ad ogni modo, dal momento che si ritiene fondamentale il mantenimento di una valida reputazione.[111]

---

[108] Fombrun C.J., *Reputation: realizing value from the corporate image,* Harvard Business School Press, Boston, 1996, p. 73.

[109]Cos'è la Web Reputation?, 2020, https://www.opengateitalia.com/oginews/cose-la-web-reputation/

[110] Fombrun C.J., *Reputation: realizing value from the corporate image,* Harvard Business School Press, Boston, 1996, p. 72.

[111] Krasnow, M.M., Cosmides, L., Pedersen, E.J., Tooby, J. (2012). What Are Punishment and Reputation for? PLoS ONE ,7, pp. 45-62.

I teorici hanno portato avanti degli esperimenti mediante i quali hanno voluto accertare la validità di ognuna delle due teorie e l'assunto in base al quale si possono condurre delle diverse predizioni, considerandole entrambe. In occasione del primo studio si puntava era a dare validità alla teoria dello scambio sociale e vi hanno partecipato circa 93 individui, invece alla seconda ricerca, la quale puntava a conferire validità nei confronti della teoria della conservazione delle regole del gruppo, hanno preso parte 119 individui.[112] Ai partecipanti si proponevano delle attività ludiche cooperative svolte assieme a dei partner, presenti all'interno del network del computer e, esaminando le differenti risposte fornite da ciascuno, essi potevano guadagnare o perdere dei dollari. Gli individui interagivano avvalendosi di alcuni script ordinari i quali consentivano di simulare gli eventuali comportamenti, capaci di mettere alla prova ciascuna delle teorie di riferimento. Gli esiti hanno considerato le risposte di fiducia, cooperazione e punizione espresse dagli individui. In ciascuno dei due studi, la reputazione è stata oggetto di valutazione mediante le risposte proposte a degli scenari ipotetici nel corso dei quali gli individui e i partner virtuali potevano collaborare o ingannare l'altro senza essere scoperti.[113]

A seguito delle verifiche in nessuno dei due studi si conferma la teoria del mantenimento delle norme gruppali, invece la teoria dello scambio sociale è stata molto sostenuta: pertanto pare che la reputazione sia correlata per lo più al favorire dei rapporti personali di vantaggio e contenenti innumerevoli scambi reciproci.[114]

Con molta frequenza, i soggetti disciplinano il proprio comportamento a seconda di quello innescato dal partner. Per quel che concerne l'impiego delle punizioni, ciò si pone in rapporto con la teoria dello scambio sociale: nel momento in cui i partecipanti erano a conoscenza del fatto che il partner era propenso a non attenersi alle regole, non obbligatoriamente essi sceglievano di punire il loro compagno in occasione di qualche impedimento da egli prodotto. Ne deriva che, non sempre si punta a punire il partner qualora lo stesso si comporti violando le regole del gruppo della cooperazione.[115]

Si ritiene basilare la volontà dell'individuo di tenere conto dell'intenzione del soggetto di proseguire la relazione con il partner o fermarla: qualora il soggetto voleva proseguire, si

[112] Hammerstein P (2003) The genetic and cultural evolution of cooperation. Cambridge, Mass: MIT Press.
[113] Camerer C (2003) Behavioral game theory: Experiments in strategic interaction: Princeton University Press.
[114] Ibidem.
[115] Camerer C, Loewenstein G, Prelec D (2005) Neuroeconomics: how neuroscience can inform economics. Journal of Economic Literature 43: 9–64.

procedeva a punire il partner, qualora questo agiva ostacolando il suo partner, all'inversione dei ruoli collaborava con lui; se si dimostrava propenso a fermare la relazione, non procedeva a punirlo, ma gli erigeva degli ostacoli.[116]

La reputazione si ritiene basilare se esiste la volontà di porre in essere degli scambi sociali positivi, fondati sulla fiducia reciproca. Nel 1997 Fombrun e Van Riel sono stati i fautori di un'evidenza scientifica relativa alla concezione sulla reputazione aziendale e, riferendosi a sei differenti dimensioni disciplinari, hanno fornito sei differenti definizioni. La suddivisione della reputazione in diverse dimensioni garantisce all'impresa l'eventualità di possedere una prospettiva sia di portata generale che specifica, consentendo di individuare eventuali criticità sulle quali muoversi e reagire con molta rapidità. Le sei dimensioni disciplinari a cui Fombrun e Van Riel fanno riferimento sono, quella concernente la macro-economia, dell'economia aziendale, della strategia, del marketing, la dimensione organizzativa e quella sociologica.[117]

Volendo approfondire lo studio dei due teorici precedentemente menzionati, i micro-economisti sono convinti che la reputazione aziendale rappresenti una sorta di segnale informativo circa elementi e fattori di un'impresa che non sono visibili per gli stakeholder esterni. In base al pensiero dei portatori di interesse occorre, difatti, poter disporre di dati relativi ai fattori che non si dimostrano capaci di osservare in maniera diretta l'obiettivo di accrescere la propria fiducia in direzione di prodotti ma anche di servizi impresari. Gli economisti del ramo aziendale, diversamente, sono convinti che la reputazione rappresenti una risorsa non materiale a cui si attribuisce un ruolo peculiare nella formulazione stessa del vantaggio competitivo e all'interno del meccanismo di creazione del valore impresario. Oltretutto, essi sostengono anche che, tenuto conto del basilare spessore delle risorse non materiali, si ritiene necessario puntare verso un approfondimento relativo alle strategie indicate per le aziende in grado di garantire la costante evoluzione, la conservazione ed il confronto. In base al pensiero degli esperti del settore della strategia aziendale, la reputazione non si qualifica solo come una risorsa non materiale a misurabile, ma anche in qualità di barriera nei confronti della mobilità.[118] In

[116] Krasnow, M.M., Cosmides, L., Pedersen, E.J., Tooby, J. (2012). What Are Punishment and Reputation for? PLoS ONE ,7, pp. 45-62.
[117] Ibidem.
[118] Micera, R., Crispino R., "*Destination web reputation as "smart tool" for image building: the case analysis of Naples city-destination*." Rivista di International Journal of Tourism Cities 3.4, 2017, pp. 406-423.

effetti reputazione che si palesa consolidata, non rende attuabile la mobilità e consente ad ogni organizzazione di difendersi dalla probabile emulazione proveniente dalla concorrenza. Il tutto si ritiene possibile dal momento che la reputazione si correla a determinati fattori distintivi e dagli elementi interni ed unici delle imprese considerate singolarmente.[119] Nella prospettiva riguardante la sfera del marketing, la reputazione spesso si riconduce ad un sinonimo di immagine provvista di brand e viene approfondita ed esaminata adottando la prospettiva della clientela o dell'utente finale, evidenziando la maniera in cui si produce. Si può definire come un ceppo di significati cognitivi ed affettivi collegati dai consumatori ai segnali ricevuti in merito ad un prodotto con ilquale si sono relazionati in maniera diretta o indiretta.[120]

Guardando a quanto riporta la teoria dell'organizzazione, la reputazione si può definire in qualità di riflesso esterno dell'identità e della cultura organizzativa, ossia una sorta di percezione relativa al comportamento organizzativo dal versante manageriale e, con più frequenza, degli stakeholder interni.[121] La cultura legata all'organizzazione genera una specie di influenza sulle percezioni e sulle motivazioni possedute dai manager, diversamente, l'identità dell'organizzazione agisce sulla loro modalità di interpretazione e reazione nei riguardi delle situazioni esterne. Una cultura e un'identità organizzativa adeguatamente coese rendono maggiormente omogenee le percezioni all'interno di un'impresa e fanno aumentare la probabilità che i manager illustrino una rappresentazione dell'organizzazione coerente con gli osservatori esterni.[122]

Secondo il pensiero dei sociologi, infine, la reputazione si può definire in qualità di congettura sociale, una valutazione composta da molteplici attori che agiscono sulle prestazioni di un'azienda rispetto a quello che ci si aspetta e alle normative in vigore all'interno di un ambito istituzionale. Guardando questa prospettiva di pensiero, la reputazione si identifica pertanto come un indicatore del grado di legittimazione di cui l'impresa può disporre nel comparto in cui si muove e presso il reticolato di interazioni a

[119] Anzelmo A., "*Il ruolo delle emozioni nella web reputation: il caso della comunicazione digitale vaticana*." Rivista Italiana di Filosofia del Linguaggio, 2020.
[120] Ibidem.
[121] Farmer, R. "*Web reputation systems and the real world*." *The reputation society. How online opinions are reshaping the offline world*, 2011, pp. 13-24.
[122] Ibidem.

cui ha dato vita congiuntamente ai suoi stakeholder.[123] Anche se non è stata maturata una definizione complessiva relativamente alla corporate reputation all'interno dei sei differenti comparti disciplinari, Fombrun e Van Riel individuano diversi fattori che rendono comuni le accezioni precedentemente palesate.[124]

Il primo elemento si riconduce alla visione altrui, per cui la reputazione non è qualcosa che si può possedere, ma si tratta di una sorta di valore conferito dagli altri. Essa effettivamente racchiude tutte le percezioni degli stakeholder, il loro giudizio in merito alle qualità di cui un'organizzazione è in possesso, per quelle che sono le sue azioni relative a periodi passati, in corso e future e in merito alle sue prestazioni di business: a tal proposito, la reputazione risulta influenzata anche dal background economico, sociale e personale degli stakeholder, ma anche dai vissuti esperienziali che questi hanno maturato mediante l'ambito organizzativo.[125]

Il secondo elemento si riferisce alla prospettiva legata alle tempistiche, per cui la reputazione si realizza poco a poco, si evolve e si potenzia nel tempo considerando che essa risulta dipendente dalle percezioni e queste possono modificarsi nel tempo; la reputazione aziendale si può definire in qualità di concetto dinamico e duraturo. Il terzo elemento si riconduce alla maniera di agire appartenente all'organizzazione. Se un'organizzazione agisce dimostrandosi socialmente responsabile, attinente alla sfera morale, trasparente, leale e in coerenza con la propria missione, assicurando prodotti, servizi e performance economiche in grado di rispondere ad ognuna delle richieste e delle aspettative della clientela, raggiungerà una adeguata ed efficiente reputazione; Il quarto elemento si collega alle fonti della reputazione originatesi dal vissuto esperienziale e dall'informazione.[126] L'esperienza si riferisce alla storia dei rapporti diretti che un soggetto ha acquisito per mezzo dell'impresa. L'informazione si riconduce ad un rapporto indiretto che lega assieme all'impresa e si può riferire ma anche coinvolgere diversi elementi della dimensione economica e anche differente, che gli stakeholder sono in grado di adoperare per emettere dei giudizi valutativi circa i comportamenti e le condotte

[123] Jundrio, H., Keni K., "*Pengaruh website quality, website reputation dan perceived risk terhadap purchase intention pada perusahahaan e-Commerce*." Rivista di: Jurnal Muara Ilmu Ekonomi dan Bisnis 4.2, 2020, pp. 229-239.
[124] Krasnow, M.M., Cosmides, L., Pedersen, E.J., Tooby, J. (2012). What Are Punishment and Reputation for? PLoS ONE ,7, pp. 45-62.
[125] Cankir, B., Lutfi Arslan M., Sadi Evren S., "*Web reputation index for XU030 quote companies*." Rivista di: Journal of Industrial and Intelligent Information 3.2, 2015.
[126] Ibidem.

comportamentali dell'azienda.[127] L'informazione può divenire fruibile attraverso la pratica della comunicazione con la divulgazione di notizie attuata per mano dei mass media e avvalendosi della pratica del passaparola, la quale si attiva in maniera spontanea fra gli individui.[128]

Il quinto elemento è collegato alla transitorietà evolutiva del costrutto del contesto di riferimento, per tale ragione, la medesima azienda si rende disponibile ad approfittare di una efficace reputazione all'interno di un determinato comparto, ad ogni modo può acquisirne una peggiore attraverso altre modalità. Relativamente ai fattori su menzionati, i due teorici precedentemente approfonditi, Fombrun e Van Riel, giungono alla maturazione di una definizione della corporate reputation: *«La corporate reputation si può delineare in qualità di una raffigurazione collettiva delle azioni e degli esiti precedentemente maturati di un'impresa che tende a fornire la descrizione relativa alla sua capacità di garantire ai diversi stakeholder dei risultati apprezzati. Valuta la collocazione di un'impresa sia al suo interno nella sfera dei suoi lavoratori sia al suo esterno nella sfera dei suoi stakeholder, inoltre anche nella sfera competitiva ed istituzionale»*.[129]

Questo tipo di definizione è stata e prosegue ancora oggi ad essere adoperata come prototipo rappresentativo da molteplici specialisti, in quanto tiene in considerazione la struttura multidimensionale di cui la corporate reputation si compone.[130] Attualmente, il "paradigma" ricondotto alla reputazione aziendale è ancora sostanzialmente complesso e frammentato. In aggiunta a ciò, si delinea la parziale esistenza di una linea di connessione: buona parte degli studi di riferimento si delineano come concordi nel sostenere che la dimensione percettiva rappresenta una sorta di punto di avvio della corporate reputation.[131] Nel dettaglio, ognuno degli stakeholder è in possesso di una propria percezione relativamente ad un'organizzazione, che può essere sia fondata su un'esperienza diretta sia influenzata dalle opinioni altrui, ne costituiscono un esempio i

---

[127] Allegri, M. R., "*Diritto all'oblio, tutela della web reputation individuale e "eccezione giornalistica". Spunti giurisprudenziali*." Forum di Quaderni Costituzionali Rassegna, 2018.
[128] Yonghong H., Greve P., "*Large scale graph mining for web reputation inference*." 2015 IEEE 25th International Workshop on Machine Learning for Signal Processing (MLSP), IEEE, 2015.
[129] Fombrun C.J., Van Riel C.B.M., *The reputational landscape*, "Corporate Reputation Review", Volume 1, N. 1-2, 1997, p. 10.
[130] Minghetti, V., Celotto E., "*Destination Web reputation: Combining explicit and implicit popularity to build an integrated monitoring system*." Rivista di: E-review of Tourism Research 6, 2015, pp. 1-5.
[131] Ibidem.

media. Questo genere di percezioni può anche essere successivamente condizionato dalle esigenze rese evidenti da ognuno dei portatori di interesse nei riguardi dell'impresa.[132]

Il teorico Wartick[133] sostiene che la reputazione aziendale sia costituita da diverse percezioni che gli stakeholder maturano relativamente a ciò che un'organizzazione mette in atto col fine di fornire soddisfazione a vantaggio delle loro richieste ed aspettative. I due teorici Bennet e Kottasz riportano invece che la reputazione aziendale si possa ritenere in qualità di *«fusione di ognuna delle speranze, percezioni e concezioni riconducibili alle qualità, ai fattori ed ai comportamenti di un'organizzazione che sono state acquisite nel tempo da clienti, impiegati, fornitori, investitori e dal grande pubblico e che derivano dall'esperienza di ognuno, dal passaparola, o persino dall'osservazione dei comportamenti che rientrano nel vissuto»*.[134]

Mutti fornisce una propria definizione per il termine reputazione con riferimento a quella riconducibile all'impresa come *«stabilizzazione temporale delle aspettative di una molteplicità di agenti, concernenti anche specifici attributi sia positivi che negativi di determinati individui, collettività ed istituzioni»*.[135]

L'autore approfondisce anche un altro aspetto posto al centro del dibattito, si tratta del legame costruito fra fiducia e reputazione. La fiducia si riconduce ad una dimensione soggettiva e poggia sulla singola esperienza personale riferita ad un individuo, diversamente la reputazione si qualifica come una raffigurazione condivisa della realtà che si basa sulla fiducia. In aggiunta alle percezioni, all'interno degli studi che hanno per tema la reputazione delle aziende, si richiamano talvolta anche ulteriori componenti correlate ad ulteriori dimensioni soggettive e sociali, tra cui si fa riferimento alle relazioni, alle aspettative ed ai flussi comunicativi.

Approfondendo il pensiero del teorico Cavazza[136], la reputazione si può definire in qualità di una costruzione sociale composta da ideali e percezioni che una data comunità pone in essere e sviluppa nel tempo. I comportamenti su cui si modella la reputazione sono quelli più in linea con le speranze della società, tra cui lapropensione alla cooperazione.

---

[132] Salluce, A., *Modalità alternative per la tutela della web reputazione*, 2017, pp. 341-360.

[133] Wartick S.L., *The relationship between intense media exposure and change in corporate reputation*, Rivista di: "Business & Society", Volume 31, N. 1, 1992, pp. 33-49

[134] Bennet R., Kottasz R., *Practitioner perceptions of corporate reputation: an empirical investigation*, Rivista di: "Corporate communications: an international journal", London Gulldhal University, Volume 5, N. 4, 2000, p. 234.

[135] Mutti A., Reputazione, "*Rassegna italiana di sociologia*", Bologna, Il Mulino, N. 4, 2007, pp. 601-622

[136] Cavazza N., *Pettegolezzi e reputazione*, Il Mulino, Bologna, 2012

Il teorico Nelli[137] espone il suo pensiero affermando la tesi che la coerenza dei comportamenti dell'impresa ed i segnali che la stessa veicola nel tempo ed in merito al proprio agire strategico concorrono a formulare la sua reputazione aziendale. Tale esteso complesso di segnali si qualifica come una fonte di informazione e valutazione in grado di permettere ai molteplici stakeholder di fare delle previsioni in merito al comportamento aziendale futuro e di formulare delle scelte a riguardo sulla base delle proprie aspettative e interpretazioni circa i suddetti segnali.

I teorici Corradini e Ferraris di Celle[138] espongono le proprie visioni sostenendo che la reputazione di un'impresa costituisce il prodotto delle relazioni pregresse tra la stessa ed i suoi stakeholder e palesa i suoi valori, il suo background interazionale e le modalità di cui dispone per fornire delle risposte riservate ai suoi pubblici di riferimento.[139]

Come ogni settore specifico, anche quello della Web Reputation presenta i propri modelli teorici e studi di riferimento che saranno di seguito approfonditi.

Il concetto relativo alla terminologia reputazione aziendale sta riscuotendo una considerevole dose di interesse per molteplici autori e studiosi nell'ambito della gestione aziendale, sia per quel che concerne la dimensione teorica che quella pratica. L'elemento che si prospetta come più particolareggiato con il quale doversi misurare, è costituito dal fatto che la letteratura di riferimento è molto lacunosa e di critico approfondimento analitico. Chi si deve occupare di far fronte a questo tema si manifesta come impossibilitato a muoversi in maniera sicura e disinvolta fra i molteplici studi, le differenti formulazioni, teorie e prospettive che nel tempo hanno incentivato la corporate reputation ad evolversi in un tema particolareggiato e caotico. Per essere nelle condizioni di supportare e provvedere a chi si approccia allo studio e all'analisi della materia oggetto di approfondimento del presente elaborato, negli anni sono state fornite delle differenti classificazioni per attuare una sorta di promozione verso una lettura più semplice e lineare rispetto ad un argomento prolisso e confuso come si presenta quello della corporate reputation.[140] Le categorizzazioni avanzate non si possono ritenere esaustive, tenuto conto

---

[137] Nelli R.P., *Corporate reputation: valore per l'impresa, garanzie per il consumatore*, Rivista di: "Consumatori, diritto e mercato", Volume 3, 2012, pp. 96-104

[138] Corradini I., Ferraris DI Celle B., *La reputazione. Nel tuo nome, il tuo valore*, FrancoAngeli, Milano, 2014.

[139] Ibidem.

[140] Mich, L., "*Requirements for a comprehensive and automated web reputation monitoring system: first iteration*." 2012, IEEE International Conference on Software Science, Technology and Engineering, IEEE, 2012.

della complessità e della vastità del tema, tuttavia esse sono funzionali a destreggiarsi con maggiore semplicità nell'ampia letteratura di settore.

I teorici Berens e Van Riel[141] fanno riferimento a tre differenti correnti nell'ambito dello studio relativo alla reputazione aziendale, sostenendo che innanzitutto, davanti alla prospettiva dell'aspettativa sociale si fa riferimento alle attese che i portatori di interesse conservano nei riguardi dei comportamenti delle persone.[142]

Per gli studi sulla personalità aziendale, si fa riferimento agli aspetti della personalità che le persone associano alle imprese, mentre per quel che concerne il filone della fiducia: fa riferimento alla percezione che le persone possiedono nei riguardi dell'onestà, dell'affidabilità e della benevolenza di un'impresa.[143]

I teorici Barnett, Jermier e Lafferty[144] categorizzano le differenti definizioni circa la terminologia "reputazione" all'interno di tre gruppi di significati, il primo si riconduce alla consapevolezza, si tratta di un gruppo entro cui afferiscono le definizioni secondo la quali gli stakeholder maturano una certa consapevolezza circa l'impresa, tuttavia non emettono dei giudizi a riguardi. Si tratta di definizioni che si concentrano con una certa particolarità sulle percezioni. Esse, dopo esser state aggregate, rappresentano la reputazione aziendale. A seguire vi è la valutazione, si tratta della categoria che accorpa tutti gli studi in cui l'elemento caratterizzante è rappresentato dal giudizio, dalla stima.[145]

La reputazione aziendale viene attribuita dalla stima dell'organizzazione. Infine vi è la risorsa, all'interno di questo gruppo si presentano accorpate le prospettive entro cui la reputazione aziendale viene rappresentata in qualità di risorsa intangibile, economica o finanziaria.[146]

Tali tre categorie confluiscono in tre differenti caratteri della concezione legata alla terminologia reputazione ma, ad ogni modo, ne mettono in evidenza la vastità e la

---

[141] Berens G., Van Riel C.B.M., *Corporate associations in the academic literature: three main streams of thought in the reputation measurement literature*, Rivista di: "Corporate Reputation Review", Volume 7, N. 2, 2004, pp. 161-178

[142] Ibidem.

[143] Ibidem.

[144] Barnett M.L., Jermier J.M., Lafferty B.A., *Corporate reputation: the definitional landscape*, Rivista di: "Corporate Reputation Review", Volume 9, N. 1, Palgrave MacMillan, 2006, pp. 26-38

[145] Francesconi, A., Dossena C., "*Web reputation management systems as strategic tools*." Rivista di: Management of the Interconnected World: ItAIS: The Italian Association for Information Systems. Heidelberg: Physica-Verlag HD, 2010, pp. 267-274.

[146] Ibidem.

radicalità del significato. Un lavoro molto similare si può attribuire al teorico Walker[147], egli opera una classifica in seno agli studi che hanno per tema principale la reputazione aziendale suddividendola in cinque gruppi, il primo gruppo riguarda gli studi percettivi, per cui il focus si pone sulle percezioni degli stakeholder, interni ed esterni, rispetto all'organizzazione; il secondo gruppo è quello degli aggreganti, in cui ci si concentra sulla prospettiva di tutti i gruppi di stakeholder rispetto ad un'organizzazione. A seguire vi sono i comparativi, essi si basano sulla comparazione fra la reputazione di un'organizzazione e gli altri concorrenti; si possono menzionare anche quelli positivi o negativi, essi si configurano come definizioni che conferiscono una certa evidenza sia verso l'aspetto positivo che verso quello negativo relativamente alla reputazione. A conclusione dei cinque gruppi, vi è quello dei fattori temporali, essi sono fondati sulla specificità temporale della reputazione e alla maniera in cui si potrà sviluppare nel tempo.[148]

Il teorico Gistri, studiando e acquisendo gli studi precedenti[149], opera una sorta di classifica della letteratura che si occupa della reputazione prendendo come carattere peculiare la prospettiva temporale, provando sottoscrivere una specie di linea evolutiva delle molteplici definizioni che si sono susseguite nel corso delle varie epoche. Sono dunque stati individuati tre differenti intervalli di tempo, essi rispondono sia ad una logica espositiva ma anche ad un ordinario mutamento del paradigma.

Il primo intervallo temporale arrivava fino al 1990 si preserva una sorta di dominio della prospettiva strategica. La reputazione viene considerata come una risorsa immateriale strategica la quale è in grado di favorire la redditività presente e futura dell'impresa, ma anche l'acquisizione di un vantaggio competitivo, tenuto conto della sua competenza quotata all'accrescimento considerevole dell'attrattività aziendale.[150] Oltretutto, quella in esame si identifica come una risorsa gestita in maniera completamente unidirezionale dall'impresa verso gli stakeholder.[151]

Nell'intervallo di tempo che va dal 1990 al 2006, si evince che accanto alla prospettiva strategica, comincia a farsi strada una prospettiva relazionale, che vede la reputazione

---

[147] Walker K., *A systematic review of the corporate reputation literature: definition, measurement and theory*, Rivista di: "Corporate Reputation Review", Volume 12, N. 4, 2010, pp. 357-387

[148] Aureli, S., Supino E., "*Web reputation and performance measurement systems in the hotel industry: An exploratory study in Italy*.", 2015, pp. 41-64.

[149] Gistri G., *Reputazione aziendale e crisis management: una prospettiva accademica professionale*, FrancoAngeli, Milano, 2018.

[150] Ibidem.

[151] Ibidem.

aziendale in qualità di percezione. Entro tale contesto, prendono piede sempre più la teoria denominata Stakeholder Theory e la concezione di stakeholder, esse vengono formalmente definite in via eccezionale da Freeman come *"ogni genere di gruppo o individuo in grado di influenzare o subire l'influenza dal raggiungimento degli obiettivi di un'organizzazione"*.[152] La Stakeholder Theory ha reso possibile lo spostamento del nucleo della responsabilità aziendale dagli azionisti (definiti anche come stockholder), i quali rappresentavano in principio gli unici portatori di interesse, in direzione di una gamma più ampia e diversificata di soggetti esterni ed interni all'impresa.[153] La reputazione aziendale, approfondendo appunto tale teoria, si genera dalla soddisfazione delle aspettative degli stakeholder. Contemporaneamente, si rende necessario assicurare un coinvolgimento diretto dei portatori di interesse presso i processi aziendali, si tratta in tal caso degli stakeholder engagement, col fine di poter elaborare una reputazione molto più radicata e massiccia, fondata esattamente su quegli aspetti e quelle variabili considerate di fondamentale rilevanza da questi soggetti. Quello che tende a presentarsi, è una sorta di forte circolo virtuoso in cui la reputazione trae chiaramente la propria origine dalle aspettative degli stakeholder, ad ogni modo, essa risulta essere anche alimentata dagli stessi, i quali vengono occupati in maniera attiva all'interno dei meccanismi gestionali e decisionali riguardanti interamente l'organizzazione.[154]

Infine, relativamente all'intervallo temporale che va dal 2006 e giunge fino ad oggi, è possibile identificare un approccio strategico e relazionale, essi convivono e si evolvono, anche se acquisisce una certa evidenza un gap relativo agli studi contemporanei in tema di reputazione aziendale che si riconduce alla necessità di comprendere i processi che si trovano nelle profondità delle fondamenta dell'evoluzione della corporate reputation. Si verifica anche una sorta di accrescimento dei contributi che si avvalgono dell'assunzione di una prospettiva multidisciplinare, andando ad integrare i nuovi esiti con le conoscenze già maturate.[155]

Facendo riferimento alla "web reputation" si sfocia necessariamente nel concetto di comunicazione nell'era digitale. Paul Watzlawick fu il primo ad esprimere una sorta di assioma in merito alla comunicazione tramandando che *"è impossibile non comunicare"*.

---

[152] Freeman R.E., *Strategic management. A stakeholder approach*, Pitman, Boston, 1984, p. 46.
[153] Aureli, S., Supino E., *Web reputation and performance measurement systems in the hotel industry: an exploratory study in Italy*, 2015, pp. 41-64.
[154] Ibidem.
[155] Ibidem.

Questo ha valenza anche per quel che concerne l'interazione virtuale, nella quale si presenta l'"internet of things" definito dal Censis come *«la nuova spina dorsale di tutto il sistema di comunicazione per mezzo della diffusione e del successo dei social networks»*.[156]

Quello che si fa o non si fa sul web, pertanto, è alla portata di tutti ed è anche sempre fruibile come un reale racconto personale. La rete, con l'espansione del concetto di networking, permette di essere in collegamento con un grandissimo quantitativo. La presenza sul web, l'interazione telematica e la good reputation online si qualificano come i tre elementi che favoriscono la realizzazione di un'identità digitale, si tratta di una specie di documento d'identità nella dimensione digitale, formata da notizie comprese nei siti web e nei social media ai quali è possibile accedere mediante una semplice ricerca in rete. La reputazione relativa alla gente e alle aziende è modellata in ragione di quello che viene raccolto in rete.[157]

I contesti digitali forniscono in epoca attuale degli spazi d'incontro diversi rispetto a quelli del passato[158], aprendo la possibilità di un'interazione diretta tra candidati e aziende che fa entrare in crisi i modelli di *sourcing* tradizionali ed evolve in *e-recruiting*.[159]

In ambito aziendale si verifica una vera e propria occasione che non si può quantificare, in quanto vengono oltrepassate le obsolete modalità di utilizzo dei mass media unilaterale, abbracciando la logica delle interconnessioni con le quali è più semplice connettersi liberamente con gli altri, condividendo i propri pensieri e assimilando stili di vita e valori. Le imprese, anche se più tardi, hanno sviluppato delle conoscenze sulla modalità più efficace di adoperare il web con i clienti, con i lavoratori dipendenti ed i candidati, in maniera da mettere in atto una concreta strategia di attrazione e fidelizzazione.[160]

Nella prospettiva del candidato la social reputation si identifica come l'occasione di confermare all'azienda alla quale si è interessati la propria reputazione professionale e le proprie competenze. Attraverso l'analisi di una recente ricerca di Adecco si evince che al primo posto tra le motivazioni che incentivano i recruiter a respingere candidature vi sono

---

[156] L., Macciocca Massimo, R., (2019), Massimo, Gestione e valorizzazione delle risorse umane, Maggioli Editore.

[157] CORRADINI I., FERRARIS DI CELLE B. (a cura di), La reputazione. Nel tuo nome, il tuo valore, FrancoAngeli, Milano, 2014

[158] https://www.meliusform.it/l-impatto-social-e-la-web-reputation-nel-recruiting.html

[159] Ibidem.

[160] A., Martini, S., Zanella, Social Recruiter. (2017), Strategie e strumenti digitali per i professionisti HR, Franco Angeli

la pubblicazione di foto improprie (secondo un dato del 20%), dati non coerenti con il curriculum (per un dato del 18,2%) e l'evidenza di aspetti legati alla personalità non adeguate alla posizione di lavoro aperta (per un dato del 16%). Tra gli altri dati considerati ci sono anche i commenti negativi in merito ai datori di lavoro odierni o precedenti (per un dato dell'11%), contenuti di carattere discriminatorio (per un dato dell'8,4%) e per finire un network mediocre. L'importante è realizzare un'immagine coerente della propria persona rispetto al profilo professionale ed ulteriori aspetti che generalmente all'interno del curriculum tradizionale del candidato non vengono menzionati, come interessi, commenti e ulteriori soft skills.[161]

Occorre dunque conservare delle valide relazioni sociali, ossia il networking di relazioni che incentivano nuovi contatti e visibilità; è peculiare possedere un valido profilo pubblico sempre aggiornato e curato, capace di rispecchiare le proprie propensioni e competenze, attirando verso di sé una certa dose di interesse. I social network propongono molte opportunità, permettono di mostrare la propria persona più di un semplice curriculum, che rende chiaro limitatamente quel che si è.[162]

Nel mondo del lavoro, che è in continua trasformazione, aziende e lavoratori devono adeguarsi alle nuove tendenze e restare sempre un passo avanti, per non ritrovarsi al di fuori dal mercato.

Le sfide dell'odierna *digital transformation* portano verso un grande risultato per il benessere delle relazioni professionali, prodotto dalle occasioni di fare networking, realizzare accordi, joint venture, alleanze, eventi tra gente lontana, andando oltre lo spazio fisico e producendo valore mediante contenuti e legami condivisi, d'altro canto rendono necessaria la cura della propria identità sul web in quanto ciò può influenzare il proprio futuro e la propria vita professionale.[163]

Resta tuttavia basilare, entro tale ambito di incisiva evoluzione e mutamento[164], che chi gestisce e regola la selezione deve porre sempre al centro di ogni cosa il contatto

[161] CORRADINI I., NARDELLI E., La reputazione aziendale. Aspetti sociali, di misurazione e di gestione, FrancoAngeli, Milano, 2015
[162] Ibidem.
[163] DE LUCIA G., DONEDDU S., SGARIGLIA A., Rischio reputazionale: il modello Pirelli, in INVERNIZZI E., ROMENTI S. (a cura di), "Progetti di comunicazione per la reputazione aziendale", FrancoAngeli, Milano, 2013
[164] LAMBOGLIA R., D'ONZA G., Un modello di gestione del rischio reputazionale. Dall'identificazione al fronteggiamento, "Management control", Vol. 3, 2013, pp. 7-34

umano[165]; il progresso tecnologico ed i mezzi ad esso correlati, si comportano come un ausilio ed un supporto per il professionista HR. Occorre tenere a mente che dietro ad un cv si pone sempre un essere umano che ha una storia e abilità e competenze, non costantemente captabili attraverso da un profilo social.[166]

Gli effetti connessi all'ascesa delle tecnologie abilitanti, riconducibili alla quarta rivoluzione industriale e permanenti a tutto il XXI secolo, si ripercuotono sia sui sistemi produttivi e organizzativi, ma anche sui processi relazionali interpersonali che intercorrono fra datori di lavoro e dipendenti, candidati e recruiter.[167] Per cui le imprese ritengono sempre più rilevante investire in politiche e pratiche manageriali finalizzate alla valorizzazione, sviluppo e soddisfazione del capitale umano.[168]

Se prima il candidato aveva bisogno di individuare la giusta modalità e strategia per suscitare l'interesse del team di selezione del personale e comprovare le proprie hard e soft skills, nel corso degli ultimi anni, è l'azienda a dover attrarre le risorse: i metodi di recruiting devono divenire meccanismi di marketing in quanto, nello stesso modo del comportamento d'acquisto di un consumatore, un candidato necessita di documentarsi e compiere accurate valutazioni prima di proporsi per un vacant pubblicato su un sito aziendale, una job board o un social network. La facilità di accesso ad Internet e ai social media dirige considerevolmente il mercato del lavoro e la selezione delle opportunità di interesse di un candidato.[169] Attualmente, il primo contatto del candidato con l'organizzazione si verifica per lo più in via digitale, e pertanto mediante la visualizzazione di Tweet, la consultazione di blog e siti internet come Glassdoor. Successivamente, il fruitore provvederà in maniera consapevole a collegarsi agli specifici careers site con l'obiettivo di compiere la registrazione. *«Acquisiscono valore la User Experience ossia la Candidate Experience, ma anche il lavoro condotto dal Digital HR Manager. Le persone che procedono con la propria candidatura possiedono alte aspettative in merito alle aziende e sul meccanismo di recruiting a cui prendono parte,*

[165] Ibidem.
[166] MARASCA S. (a cura di), Misurazione della performance e strumenti di controllo strategico, Esculapio, Bologna, 2011
[167] Zahrudini N., Afrianty T.W. (2020). The Impact of Electronic Recruitment towards Employer Branding through Candidate Experience (Survey on Recent Graduates of Business Administration, Faculty of Administrative Science, University of Brawijaya Batch 2013). Wacana– Vol. 23, No. 1.
[168] Balbi T., Bongiorno G., Damiano D., Ferrara F., Valenti G. (2017). HR Digital Transformation. Competenze e attività dell'HR nell'industria 4.0. Free Your Talent.
[169] Carpenter L. (2013). Improving the Candidate Experience. Strategic HR Review. Vol. 12, 203-208.

pertanto occorre gestire il proprio brand e il percorso in azienda se ci si vuole garantire vantaggio competitivo ed evitare che quest'ultime lo facciano al loro posto».[170]
Si renderà pertanto possibile mantenere sotto controllo l'efficacia e la solidità della propria identità, ridimensionando il gap tra ciò che si è e come si viene percepiti.[171]

3.5 Rischi finanziari

Qualora non si adottino le giuste precauzioni in merito alla cybersecurity, si aumenta la possibilità di andare incontro a rischi finanziari, minando, così, il proprio equilibrio economico.[172]
Un fattore che può indebolirne il capitale è l'appropriazione indebita delle liquidità dell'azienda. Ciò avviene in seguito alla trafuga di informazioni bancarie, come credenziali o PIN, attraverso le quali vengono effettuati spostamenti di denaro o transazioni fittizie da parte dei malviventi.
Un ulteriore rischio, che può compromettere la stabilità finanziaria, è costituito dai cosiddetti attacchi ransomware. Questi prevedono l'alterazione dei flussi di accesso ai sistemi aziendali, impossibilitando l'utilizzo dei propri dati per periodi prolungati di tempo, comportando un'interruzione della produttività con conseguente perdita di profitti.
Lo scopo principale di tale attacco è quello di ottenere un riscatto dall'azienda che si trova costretta a pagare i malviventi affinché ripristinino lo status iniziale. Non sempre, in seguito al pagamento, è garantita la restituzione dei dati e talvolta questi ultimi vengono ugualmente immessi in rete.
Effetto secondario derivante da violazioni del genere è la perdita di fiducia da parte di clienti e dei fornitori, nonché la compromissione dell'immagine dell'azienda, causando delle diminuzioni di contratti che colpiscono direttamente la propria economia e favorendo la concorrenza.
Le aziende che non rispettano le normative sulla protezione dei dati, come il GDPR (General Data Protection Regulation) in Europa o il CCPA (California Consumer Privacy Act) negli Stati Uniti, rischiano ulteriori sanzioni in caso di violazioni.

[170] CareerArc Group LLC. (2016). State of the Candidate Experience Study. CareerArc Report.
[171] Ibidem.
[172] Liu, S., & Cheng, B. (2009). Cyberattacks: Why, what, who, and how. *IT professional*, *11*(3), 14-21.

Dopo un attacco informatico, l'azienda dovrà sostenere costi significativi per ripristinare i sistemi compromessi e rinforzare le difese informatiche. Questi costi possono includere l'assunzione di esperti di cybersecurity, l'acquisto di software di protezione aggiuntivi e l'implementazione di nuove politiche di sicurezza.[173]

Le aziende potrebbero dover affrontare danni a lungo termine alla loro performance finanziaria, con un impatto negativo sulla loro capacità di pagare i dipendenti, investire nelle operazioni o restituire i debiti.[174] Inoltre, i danni indiretti derivanti dalla perdita di produttività o dal rallentamento delle attività economich,e possono essere difficili da quantificare ma altrettanto gravi.[175]

3.6 Strategie di mitigazione dei rischi

Fondamentale è contenere le conseguenze degli attacchi informatici attraverso quelle che sono le strategie di mitigazione dei rischi. Per far sì che una strategia sia efficace essa deve essere proattiva, effettuando un monitoraggio costante, e reattiva, prevedendo strategie d'intervento qualora vi sia effettivamente un attacco.Tra le principali strategie che un'azienda può adottare vi sono:

1. Implementazione di politiche di sicurezza aziendale che devono coprire le best practices per la gestione delle informazioni, l'accesso ai dati, l'uso delle risorse aziendali e la protezione dei dispositivi. Tra le misure da adottare vi è la creazione e l'applicazione di politiche chiare per l'accesso ai dati sensibili, l'utilizzo delle risorse aziendali, per il trattamento e la protezione dei dati (tramite GDPR o CCPA) e la gestione dei dispositivi.
2. Formazione e sensibilizzazione dei dipendenti, una delle vulnerabilità in un'azienda è spesso il fattore umano. Gli attacchi come il phishing vengono subiti principalmente dai dipendenti, che potrebbero non essere sempre consapevoli delle minacce informatiche.[176] È importante organizzare dei corsi di formazione regolari per i dipendenti su come

[173] Ibidem.
[174] Donaldson, S. E., Siegel, S. G., Williams, C. K., Aslam, A., Donaldson, S. E., Siegel, S. G., ... & Aslam, A. (2015). Common Cyberattacks. *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, 281-295.
[175] Ibidem.
[176] Hale, G. (2017). Companies need to formulate a cybersecurity plan: cybersecurity has made significant strides in terms of companies' awareness, but there is still a long way to go, according to experts at the SANS ICS Security Summit. *Control Engineering*, *64*(6), DE5-DE5.

riconoscere e prevenire attacchi informatici, sensibilizzare sul corretto utilizzo delle password e sull'importanza di aggiornare regolarmente i software.

3. L'autenticazione a Più Fattori (MFA) aggiunge un ulteriore livello di protezione agli accessi, richiedendo agli utenti di effettuare più passaggi per autenticarsi. È imprescindibile adoperare l'MFA su tutti i sistemi aziendali, inclusi accessi a reti interne, piattaforme di cloud e strumenti di comunicazione aziendale. Grazie a ciò, nonostante un malintenzionato sia in possesso di unapassword compromessa, gli sarà ostico accedere al sistema stesso.

4. Crittografia dei dati, si tratta di un metodo di sicurezza fondamentale per salvaguardare le informazioni riservate. Consiste nel cifrare i dati rendendoli illeggibili a chiunque non sia autorizzato ad accedervi. Solo le persone autorizzate posseggono la chiave di decrittazione attraverso cui avviene la decodifica. Si consiglia di crittografare i dati sensibili, sia quando sono archiviati che quando sono in transito attraverso le reti aziendali, nella fattispecie di utilizzare protocolli di sicurezza come TLS per quelli in transito e crittografia a livello di file o database per i dati archiviati.[177]

5. Backup regolari e sicuri, un'abitudine indispensabile per proteggere i dati aziendali da attacchi come i ransomware. Nel caso in cui i malintenzionati rendano inaccessibile il database dell'organizzazione, i backup permettono di ripristinare le informazioni senza la necessità di dover pagare alcun riscatto. È importante effettuare dei backup regolari per tutti i dati critici, conservarli presso luoghi sicuri, (es. cloud o in archivi esterni protetti da crittografia), infine è necessario testare sistematicamente i backup per assicurarsi che possano essere ripristinati.

6. Monitoraggio e rilevamento delle minacce della rete è essenziale affinché si agisca tempestivamente rispetto a malfidi movimenti così da impedire intrusioni malevole. Intrusion detection (IDS) e intrusion prevention (IPS) costituiscono sistemi specializzati per monitorare costantemente il traffico di rete. In una configurazione più avanzata si tende anche ad integrare, in modo combinato, soluzioni di Security Information and Event Management (SIEM) affinché vengano collezionati e ispezionati i dati legati a tali movimenti e, dunque, migliorando la capacità di rilevamento di minacce avanzate.

[177] Ibidem.

7. La gestione delle vulnerabilità comporta l'adozione e l'implementazione di un programma di *patch management* che garantisca l'applicazione tempestiva di aggiornamenti e patch di sicurezza sui sistemi operativi, software e applicazioni aziendali.
8. Segmentazione della rete, una strategia che prevede la separazione della rete aziendale in sezioni più piccole ed isolate in base alla funzione. Questo rende più difficile per un hacker compromettere tutta la rete in caso di violazione.[178]
9. Piani di recupero e *business continuity*, in quanto anche con le migliori misure di prevenzione, gli attacchi informatici possono verificarsi. Un piano di recupero e continuità aziendale adeguatamente strutturato si reputa essenziale per minimizzare i tempi di inattività e garantire il ritorno alle normali operazioni. È necessario creare dei piani dettagliati per il recupero rapido dei sistemi, per il ripristino dei dati e per la gestione delle comunicazioni interne ed esterne, e le modalità di coordinamento tra i vari dipartimenti.
10. L'assicurazione cyber non è altro che una polizza assicurativa che copre la società dagli esborsi causati da eventuali attacchi informatici, preservandone le finanze. Esistono diversi livelli di copertura in base a quelle che sono le disponibilità della azienda stessa ed ai rischi specifici a cui è esposta.
11. Collaborazione con esperti di *cybersecurity* con lo scopo di implementare le migliori pratiche e per ricevere consulenza in merito alla tutela dei sistemi aziendali. In base a quanto detto è necessario assumere un collaborare con consulenti specializzati in *cybersecurity* per eseguire *audit* di sicurezza regolari, valutare le vulnerabilità, migliorare le difese informatiche e gestire gli incidenti per imparare a rispondere in modo adeguato.
12. Valutazione dei rischi e *auditing* periodico, aiutano a verificare che le misure di sicurezza siano adeguate e conformi con le *best practices*. L'adozione di un approccio integrato e proattivo destinato alla mitigazione dei rischi informatici si reputa cruciale per ridurre la probabilità di attacchi e per ridurre al minimo l'impatto di eventuali incidenti. Le aziende devono combinare politiche di sicurezza, formazione continua dei dipendenti, tecnologie di protezione avanzate e piani di recupero con lo scopo di garantire una protezione valida contro le minacce informatiche.[179]

[178] Ibidem.
[179] Soriano, J. (2025). Cyber-attacks: how can companies limit the risks in a global environment of growing security threats?–Global Security Mag Online.

Capitolo IV: Cybersecurity nella pubblica amministrazione

4.1 La digitalizzazione della pubblica amministrazione

La trasformazione digitale che ha coinvolto la pubblica amministrazione rappresenta un obiettivo prioritario che favorirà la scomparsa della carta, l'abbattimento dei costi e l'erogazione di servizi molto più validi ed utili negli interessi del cittadino. Si può dedurre che tutto il processo pur presentandosi notevolmente complesso, tragga le sue fondamenta dai pilastri appena menzionati.

Gli attori con le loro funzioni interessati al meccanismo di trasformazione digitale della pubblica amministrazione sono menzionati nella Fig. 19. [180]

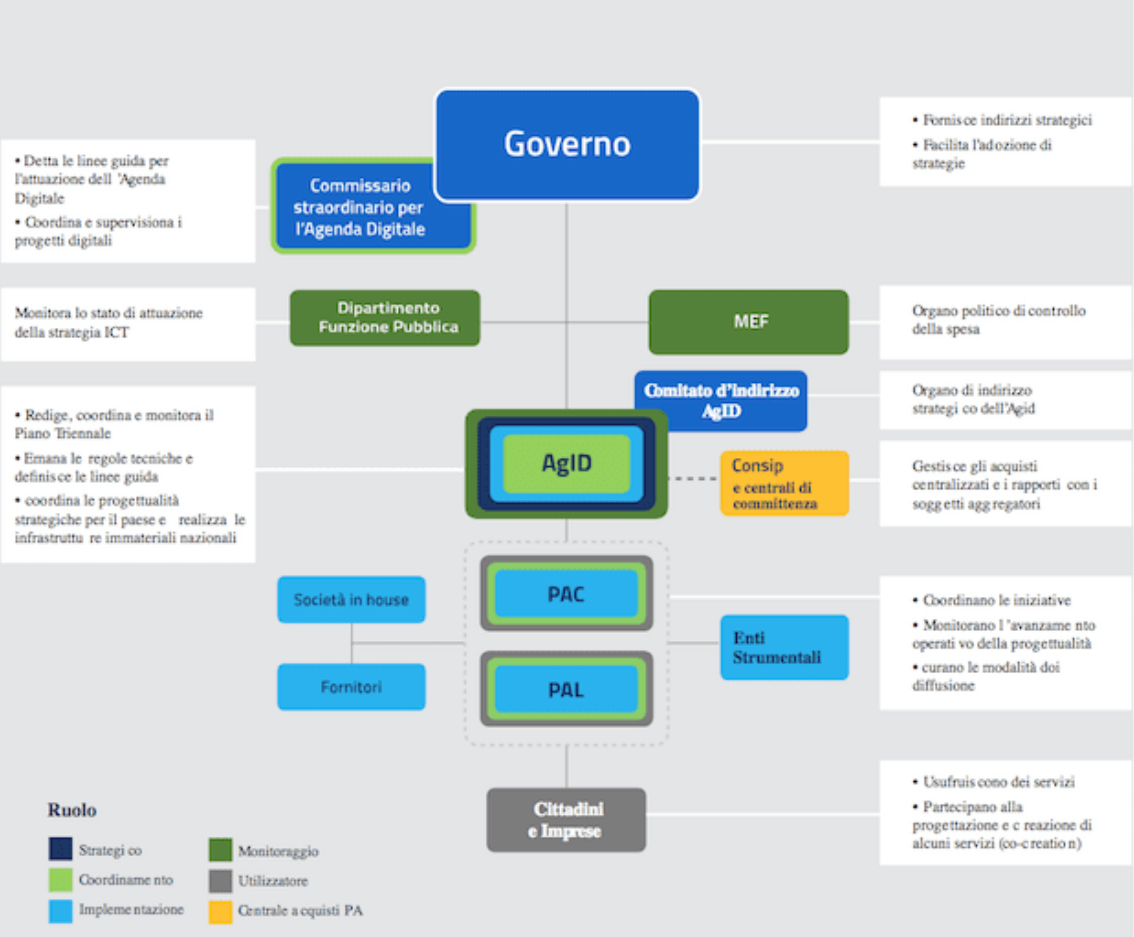

Figura 19: Enti e soggetti interessati alla digitalizzazione
https://www.bucap.it/news/trasformazione-digitale-pubblica-amministrazione.htm

[180] Montessoro, Pier Luca. "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale." *LE ISTITUZIONI DEL FEDERALISMO* 40.3, 2019, pp. 783-800.

Il Piano Triennale 2019-2021 descrive le linee di azione con cui i Ministeri e gli Enti Pubblici devono perseguire l'obiettivo di favorire la trasformazione digitale di tutto il Paese.[181]

L'interoperabilità permette di implementare i sistemi informatici, uniformando le architetture informatiche e promuovendo l'uso di procedimenti condivisi, che garantiscono il completo scambio di informazioni presso la Pubblica Amministrazione.

La pubblica amministrazione, quotidianamente, produce e gestisce moltissimi dati ed informazioni. Per usufruire al massimo delle grandi potenzialità, è necessario che i dati siano gestiti in maniera più sistematica per mezzo di:

- Basi di dati d'interesse nazionale che devono contenere dati verificati; essere omogenei per tipologia e per dati; contenere dati di rilievo per le attività stesse della pubblica amministrazione.
- Open data per quel che concerne la pubblica amministrazione per i soggetti che hanno accesso a specifiche informazioni.
- Vocabolari controllati e modelli dei dati.[182]

Gli strumenti che consentono di raggiungere gli obiettivi del Piano triennale sono le infrastrutture fisiche, ossia:

- Data center: contenenti più infrastrutture ICT, sono molteplici quelli previsti nella pubblica amministrazione, la loro gestione costituisce circa il 39% della spesa ICT annuale nelle PA. Vanno valorizzati i data center che funzionano meglio per ridurre la spesa.
- Cloud: si prevede che esso sia del tutto omogeneo e condiviso nella pubblica amministrazione, ciò semplificherà le condivisioni e le modifiche.
- Connettività: deve essere stabile e potente. Il tutto deve poter contare sulla sicurezza per mezzo di antivirus e firewall.

Per raggiungere i macro-obiettivi e i micro-obiettivi del Piano triennale per l'informatica all'interno della pubblica amministrazione, l'AgID (ossia l'Agenzia per l'Italia digitale) ha definito cinque strumenti:

- Repository del codice sorgente;
- Catalogo delle API con documentazione, ambienti di test e sandbox;

[181] Viganò, Luca. "Nuove frontiere della cybersecurity." *Picotti L. (a cura di), Automazione, Diritto e Responsabilità, Napoli, Edizioni Scientifiche Italiane*, 2023, pp. 213-220.
[182] Santaniello, Mauro. "Monocratic cybersecurity." *Rivista di Digital Politics* 2.3, 2022, pp. 305-330.

- Documentazione tecnica;
- Strumenti di service design;
- Strumenti per la gestione di progetto.

In merito alla sicurezza dei dati vi è il CERT-PA (ossia il Computer Emergency Readiness/Response Team). Esso rientra nell'AgID e agisce supportando le pubbliche amministrazioni nel prevenire e affrontare le minacce informatiche con l'utilizzo di diversi data base come ad esempio il Cyber security knowledge base ed il National vulnerability database.[183]

Il Modello strategico si pone l'obiettivo di implementare il sistema informativo della Pubblica Amministrazione attraverso diverse attività come: lo sviluppo di servizi digitali migliori riducendo i costi, l'organizzazione e l'informatizzazione tra le Pubbliche Amministrazioni.[184]

4.1.1 Politiche di sicurezza informatica nella pubblica amministrazione

I servizi digitali erogati dalla Pubblica Amministrazione sono peculiari e fondamentali per il funzionamento del sistema Paese.

Gli attacchi informatici come malware e ransomware progrediscono costantemente a causa dell'evoluzione delle tecniche di ingegneria sociale finalizzate ad ingannare gli utenti finali dei servizi digitali sia interni che esterni alla PA.[185] È fondamentale frenare queste minacce perchè ciò garantisce che il sistema informativo della Pubblica Amministrazione sia disponibile, integro e riservato, di conseguenza questo accresce la fiducia dei cittadini nei servizi digitali erogati dalla PA.[186]

Il pericolo di attacchi hacker nella PA si ritiene molto grave perchè le istituzioni che assicurano lo svolgimento delle funzioni pubbliche e governative, raccolgono e

[183] https://www.bucap.it/news/trasformazione-digitale-pubblica-amministrazione.htm#:~:text=Facilitare%20il%20coordinamento%20tra%20le%20pubbliche%20amministrazioni;%20Consentire,che%20riducano%20i%20costi%20e%20migliorino%20i%20servizi.

[184] Lorè, Filippo, and Paolo Musacchio. "Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva?." *Amministrativ@ mente-Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"* 1, 2021.

[185] https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/capitolo_6_sicurezza_informatica.html

[186] Matassa, Manfredi. "La regolazione della cybersecurity in Italia." *La sicurezza nel cyberspazio*, 2023, p. 21.

conservano dati sensibili di massima segretezza, che hanno a che fare con la tutela e la sicurezza nazionale.

Anche per l'Unione Europea è diventato un obiettivo primario salvaguardare la pubblica sicurezza dagli attacchi hacker perchè, al giorno d'oggi, sono le tecnologie digitali che gestiscono un quantitativo di attività sempre più elevato.

L'AgID, ossia l'Agenzia per l'Italia digitale, per implementare le procedure cyber nella PA**,** quest'ultima ha predisposto delle linee guida, destinate agli enti pubblici ed organizzazioni private, che si riferiscono alla formazione, conservazione, e gestione dei documenti informatici per una più accurata sicurezza informatica.[187]

4.2 Rischi ed interventi previsti

Le normative che mettono in evidenza la riservatezza e l'integrità dei dati sono l'art. 51 del Codice dell'Amministrazione Digitale (CAD) l'art. 32 del Regolamento Generale sulla Protezione dei Dati (GDPR).[188] Queste legislazioni, stabiliscono l'importanza di realizzare procedure che garantiscono la continuità dei servizi ed il ripristino tempestivo dei sistemi nell'eventualità vi fossero incidenti. Il Piano Triennale per l'Informatica delle PA 2024-2026 stabilisce ulteriori misure, obiettivi ed azioni da rispettare per la sicurezza informatica.

Tali disposizioni necessitano di adempimenti che spesso si ripetono. È significativo dunque coordinare le attività, così da non replicare i processi volti a garantire la sicurezza. Per bilanciare il contesto normativo e tecnologico occorre una adeguata gestione organica e strutturata del processo.[189]

L'art. 17 del CAD introduce per gli enti pubblici la figura del "Responsabile per la Transizione Digitale" (RTD) che deve favorire le linee guida per la protezione dei dati e dei servizi digitale, in maniera tale da coinvolgere l'amministrazione sui rischi derivanti da un attacco informatico.[190]

---

[187] https://www.boolebox.com/it/cyber-security-nella-pa-rischi-interventi-soluzioni/

[188] https://www.ictsecuritymagazine.com/articoli/cybersecurity-nella-pubblica-amministrazione-garantire-la-continuita-dei-servizi-attraverso-la-sicurezza-integrata/

[189] Lauro, Alessandro. "La cybersecurity." *Il contrasto al terrorismo negli ordinamenti democratici*. Brixia University Press, 2022, pp. 113-124.

[190] https://www.ictsecuritymagazine.com/articoli/cybersecurity-nella-pubblica-amministrazione-garantire-la-continuita-dei-servizi-attraverso-la-sicurezza-integrata/

Il punto fragile di tutta la catena della sicurezza informatica di un'organizzazione è nelle persone, pertanto occorre gestire la sicurezza informatica con azioni organizzative e decisionali, muovendo dai vertici delle amministrazioni. È necessario gestire la sicurezza informatica attraverso diverse normative: l'art. 12 comma 3-bis del CAD fornisce linee guida per l'uso sicuro degli strumenti ICT, l'art. 13 del CAD stabilisce la formazione continua del personale per diffondere gli impatti sull'organizzazione in caso di attacchi informatici.

Nella pubblica amministrazione, la sicurezza informatica porta ad utilizzare tecnologie informatiche che conferiscono integrità e robustezza.[191]

4.3 Il cloud geo-distribuito

Lo *storage* distribuito è un sistema di archiviazione *software-defined* che limita l'accesso ai dati agli utenti autorizzati.[192] I dati distribuiti permettono di implementare strumenti di monitoraggio fondati sul cloud per prevenire ed esaminare un attacco informatico e ripristinare i dati.[193]

Lo *storage cloud* distribuito si basa sull'*edge computing* e sullo *storage* e rappresenta un ulteriore passo in avanti in quanto consente di archiviare i dati in regioni prossime alle sedi di un'azienda, consentendo trasferimenti dei dati più rapidi, riducendo la congestione della rete, e minimizzando i rischi di perdita di dati.[194]

[191] Ibidem.
[192] Rossa, Stefano. *Cybersicurezza e pubblica amministrazione*. Editoriale Scientifica, 2023.
[193] https://www.nutanix.com/it/info/distributed-storage
[194] Raffiotta, E. "L'erompere dell'intelligenza artificiale per lo sviluppo della pubblica amministrazione e dei servizi al cittadino." *AI ANTHOLOGY-Profili giuridici, economici e sociali dell'intelligenza artificiale*. Il Mulino, 2022.

4.4 Regolamenti e normative odierne in tema di Cyber security

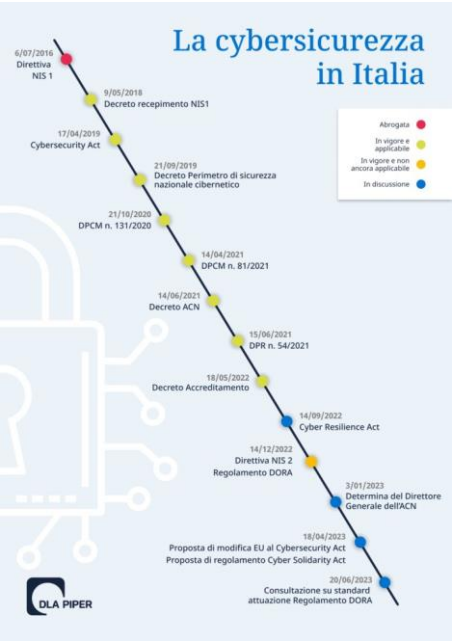

Figura 20: https://dirittoaldigitale.com/2023/10/09/cybersecurity-italia-cyberitalia-evoluzione-normativa/

La "**Cybersicurezza**" permette di analizzare e rilevare le minacce informatiche in maniera tale da utilizzare misure adeguate di prevenzione per garantire la sicurezza di sistemi informatici.[195]

La diffuzione delle tecnologie dell'informazione e della comunicazione (ICT), ha condotto ad una progressiva esposizione dei sistemi e delle infrastrutture ad attacchi informatici sempre più sofisticati e letali. Tutto ciò è avvalorato dal rapporto del Clusit del 2023 in cui si dimostra che dal 2018 al 2022 è stata rilevata una crescita globale degli attacchi informatici pari al 60%. Mentre secondo uno studio di IBM, l'Italia nel 2024 ha registrato il 7,6% degli attacchi a livello globale con un costo medio di 3 milioni di Euro per le imprese italiane che li hanno subiti. [196]

L'Unione Europea ha deciso di inserire come priorità legislativa la necessità di prevenire e contrastare gli attacchi informatici, infatti dal 2016 ad oggi si è registrato un'esponenziale aumento delle attività in tema di cybersecurity.[197]

[195] https://dirittoaldigitale.com/2023/10/09/cybersecurity-italia-cyberitalia-evoluzione-normativa/
[196] https://dirittoaldigitale.com/2023/10/09/cybersecurity-italia-cyberitalia-evoluzione-normativa/
[197] Borriello, Giuseppe, and Gaia Fristachi. "Stato (d'assedio) digitale e strategia italiana di cybersicurezza." *Rivista di Digital Politics* 2.1-2, 2022, pp. 157-178.

La Direttiva NIS, introdotta nel 2016, è una delle normative fondamentali in tema di cybersicurezza in Europa, con l'obiettivo di migliorare la sicurezza delle reti e dei sistemi informativi in tutta l'UE.

Gli obiettivi principali prevedevano di migliorare la resilienza e la sicurezza delle infrastrutture critiche (es. energia, trasporti, sanità, bancario, telecomunicazioni); stabilire obblighi di sicurezza per operatori di servizi essenziali e fornitori di servizi digitali; la comunicazione di incidenti gravi: gli operatori devono segnalare incidenti significativi alla Autorità nazionale di cybersicurezza entro 72 ore.

I soggetti interessati sono gli operatori di servizi essenziali, ossia settori come energia, trasporti, sanità, banche, ecc.; i fornitori di servizi digitali come le piattaforme online, motori di ricerca, servizi di cloud computing.

Le principali disposizioni prevedono l'adozione di misure per prevenire e ridurre i rischi legati alla cybersicurezza ed una cooperazione tra le autorità nazionali per la gestione degli incidenti e la condivisione delle informazioni.

Il GDPR è entrato in vigore nel 2018, non è specificatamente una normativa di cybersicurezza ma stabilisce regole sulla protezione dei dati personali all'interno dell'UE e impone obblighi di sicurezza riguardo al trattamento di questi dati.

Gli obiettivi principali di questa normativa prevedono la protezione dei dati personali da accessi non autorizzati; ed anche responsabilità e trasparenza da parte delle imprese che devono informare tempestivamente le autorità di protezione dei dati in caso di violazione.

Tra i soggetti interessati vi sono tutti coloro che trattano dati personali nell'UE, sia che abbiano sede nell'UE, sia che operino fuori dall'UE ma trattino dati di cittadini UE.

Le principali disposizioni sono l'implementazione di misure di sicurezza appropriate per proteggere i dati (ad esempio, crittografia, pseudonimizzazione); le comunicazioni all'autorità di protezione dei dati entro 72 ore ed infine l'integrazione della protezione dei dati dalla progettazione dei sistemi (la privacy by design e by default).[198]

La direttiva 2013/40/UE stabilisce norme minime per la punibilità dei crimini informatici in Europa, affrontando attività come l'accesso illecito ai sistemi informatici, l'uso di software dannosi, il phishing, ecc.

[198] Ibidem.

Gli obiettivi principali sono combattere i crimini informatici, la manipolazione dei dati, i reati di pirateria informatica e l'armonizzazione delle leggi penali, ossia garantire che i crimini informatici siano trattati in modo uniforme in tutta l'UE.

Le principali disposizioni riguardano la definizione di crimini informatici, ossia quelle attività come hacking, frodi informatiche, attacchi DDoS (Distributed Denial of Service); delle sanzioni penali, ossia pene detentive o sanzioni per chi compie crimini informatici.

Il Cybersecurity Act, entrato in vigore nel 2019, rafforza il mandato dell'Agenzia dell'Unione Europea per la cybersicurezza (ENISA) e stabilisce un certificato europeo di cybersicurezza.

Tra gli obiettivi principali punta a rafforzare ENISA, ossia l'Agenzia dell'Unione Europea per la cybersicurezza, la quale ha ricevuto poteri più ampi per supportare gli Stati membri e le imprese; la certificazione della cybersicurezza, per cui il regolamento istituisce un sistema di certificazione per la cybersicurezza a livello europeo per garantire che i prodotti e i servizi tecnologici siano sicuri.

Tra i soggetti interessati, vi sono le imprese tecnologiche, i produttori di software, hardware e servizi digitali.

Le principali disposizioni riguardano la creazione di una politica di certificazione comune ed il rafforzamento della cooperazione tra Stati membri mediante il coordinamento e la condivisione delle informazioni sulle minacce informatiche.

Nel 2020, la Commissione Europea ha adottato una nuova strategia di cybersicurezza che mira a proteggere le infrastrutture critiche, rafforzare la resilienza e promuovere una cybersicurezza forte nell'UE.[199]

L'Europa è leader globale nella regolamentazione della cybersicurezza grazie all'attuazione delle normative descritte in precedenza ossia la Direttiva NIS, il GDPR, il Cybersecurity Act che mirano a proteggere le infrastrutture critiche, i dati personali e le informazioni sensibili. Con l'evoluzione delle minacce informatiche, è probabile che l'UE continui a sviluppare e aggiornare la propria legislazione per affrontare nuove sfide.[200]

[199] Ibidem.
[200] Ibidem.

4.5 Le politiche italiane

L'ACN (Agenzia per la Cybersicurezza Nazionale) è stata creata per utilizzare l'esperienza accumulata negli anni dall'Italia ma anche quella maturata dagli altri Paesi per migliorare la sicurezza informatica in Italia.[201]

L'ACN è sotto la responsabilità del Presidente dei Ministri e coordina tutte le amministrazioni competenti in materia di cybersecurity.[202]

L'ACN rappresenta un nuovo pilastro che è stato attestato ad un unico soggetto governativo, che si aggiunge a quelli già esistenti ossia: Prevenzione e repressione dei reati informatici (Polizia di Stato), Difesa e sicurezza militare dello Stato nello spazio cibernetico (Ministero della Difesa) ed infine Ricerca ed elaborazione informativa (Organismi di informazione per la sicurezza). L'obiettivo è garantire la coerenza delle iniziative, migliorare la spesa, fornire un quadro chiaro e aggiornato all'Autorità politica, ed infine il coordinamento tra i soggetti pubblici coinvolti in materia di sicurezza cibernetica, anche per assicurare nei contesti internazionali una postura nazionale unitaria.[203]

L'Agenzia mira a divenire un centro di competenze, sia per altre amministrazioni pubbliche che al suo interno. A partire dal 2022, mirate campagne porteranno al reclutamento di 800 esperti entro il 2027, evitando la fuga di talenti italiani all'estero.

La Polizia di stato attraverso il Servizio di Polizia Postale e delle Comunicazioni si occupa delle prevenzione e del contrasto ai crimini informatici. Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), protegge le infrastrutture critiche informatizzate dai reati informatici. Il Dipartimento di Pubblica Sicurezza ha creato la Direzione Centrale per la Sicurezza Cibernetica che opererà il Computer Emergency Response Team (CERT) del Ministero dell'Interno, istituito per garantire la sicurezza delle reti e dei sistemi informativi, attraverso la prevenzione e la gestione degli eventi critici. Per quanto riguarda l'Arma dei Carabinieri, il Reparto Indagini Telematiche del Raggruppamento Operativo Speciale (ROS) è istituito per contrastare la criminalità informatica, mentre per la Guardia di Finanza è il Nucleo

[201] A. A. V. V., Strategia nazionale di cybersicurezza, 2022-2026, ANC, consultabile al sito: https://giurisprudenza.unimc.it/it/ricerca/dirittoapplicato/site-news/ACN_Strategia.pdf

[202] ACN, Strategia Nazionale di Cyber Sicurezza 2022-2026, Mario Draghi, URL: https://www.ilnautilus.it/wp-content/uploads/2022/05/ACN_Strategia.pdf

[203] ACN, Piano Strategico 2024-2026, URL: https://www.acn.gov.it/portale/documents/d/guest/piano-strategico-acn-2024-2026_copia_timbrata

Speciale Tutela Privacy e Frodi Tecnologiche (NSTPFT) che si occupa del contrasto delle frodi telematiche ed informatiche, nonché alla tutela della privacy. Il Ministero della Difesa definisce e coordina la politica militare, la governance e le capacità militari nell'ambiente cibernetico, nonché lo sviluppo di capacità cibernetiche e la protezione delle proprie reti e sistemi sia sul territorio nazionale sia nei teatri operativi all'estero.[204] La Difesa, attraverso le articolazioni specialistiche dedicate, conduce operazioni militari cibernetiche offensive e difensive nei casi previsti. Il Comparto Intelligence si occupa della ricerca ed elaborazione per proteggere gli interessi dell'Italia, contrastando gli attacchi informatici. La Cyber Diplomacy, gestita dal Ministero per gli Affari Esteri e la Cooperazione Internazionale (MAECI), utilizza strumenti dispomatici per proteggere gli interessi nazionali nello spazio cibernetico. La presente strategia coinvolge anche gli operatori privati, il mondo accademico e della ricerca, nonché la società civile nel suo complesso e la stessa cittadinanza. L'obiettivo ultimo della sicurezza cibernetica nazionale può essere raggiunto solo attraverso il contributo di tutte le componenti del tessuto sociale.[205]

4.5.1 Il PNRR

Ulteriore strumento strategico per affrontare le sfide è il Piano Nazionale di Ripresa e Resilienza (PNRR). Nell'ambito della Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", sono incluse le attività di transizione digitale della Pubblica Amministrazione, quali il progetto del Cloud Nazionale e la digitalizzazione dei processi e servizi per i cittadini, la cui realizzazione porterà al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese. Inoltre, lo specifico Investimento 1.5 "Cybersecurity" - pari a 623 milioni di euro - rimesso all'Agenzia per la Cybersicurezza Nazionale quale Soggetto Attuatore, prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber, con strette connessioni, a livello nazionale e internazionale, con tutti i principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. Ciò, al fine di conseguire un'autonomia

[204] Ibidem.
[205] Ibidem.

tecnologica nazionale ponendo la cybersicurezza e la resilienza a fondamento della trasformazione digitale della Pubblica Amministrazione.

Con il programma Next Generation EU (NGEU), l'Unione prevede investimenti e riforme per accelerare la transizione ecologica e digitale, migliorare la formazione delle lavoratrici e dei lavoratori, e conseguire una maggiore equità di genere, territoriale e generazionale. L'Italia è la prima beneficiaria dei due principali strumenti del NGEU: il Dispositivo per la Ripresa e Resilienza (RRF) e il Pacchetto di Assistenza alla Ripresa per la Coesione e i Territori d'Europa (REACT-EU). Il dispositivo RRF richiede agli Stati membri di presentare un pacchetto di investimenti e riforme: il Piano Nazionale di Ripresa e Resilienza (PNRR).[206] Il Piano si articola in sei Missioni e 16 Componenti. Le sei Missioni del Piano sono:

1. Digitalizzazione, Innovazione e Competitività, cultura e turismo;
2. Rivoluzione verde e transizione ecologica;
3. Infrastrutture per una mobilità sostenibile;
4. Istruzione e ricerca;
5. Inclusione e coesione;
6. Salute.

Il piano di attuazione, d'intesa con il Dipartimento per la Trasformazione Digitale (DTD) nella sua veste di Amministrazione Titolare dell'investimento, è organizzato in tre principali aree d'intervento e, in accordo alle regole tecnico-organizzative del PNRR, coinvolgerà tutti i principali attori nazionali, pubblici e privati, del mondo della cybersecurity:

- Servizi Cyber Nazionali (174 milioni di euro): Contribuendo all'attivazione e piena operatività dell'Agenzia, le reti e i servizi che saranno realizzati potenzieranno le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber.
- Interventi di potenziamento della resilienza Cyber per la PA (301,7 milioni di euro): Le capacità cyber della PA sono un elemento fondante per una transizione digitale sicura del Paese, assicurando quindi adeguati livelli di sicurezza per i dati e i servizi dei cittadini.

[206] Butera, F. (2022). Il PNRR per rigenerare le organizzazioni italiane nella transizione ecologica e digitale 1. *Techne*, *23*, 26-34.

- Laboratori di scrutinio e certificazione tecnologica (147,3 milioni di euro): Il raggiungimento di un'autonomia tecnologica nazionale passa necessariamente anche dal potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica, in stretta collaborazione con il mondo privato dell'industria e dell'accademia.[207]

4.5.2 Italia Digitale 2026

La trasformazione digitale della PA prevede la realizzazione di servizi più efficienti e accessibili, in linea con gli obiettivi dell'UE. Gli investimenti di rilievo, già citati, che hanno lo scopo di configurare la trasformazione del nostro Paese, sono il Piano Nazionale di Ripresa e Resilienza (PNRR) e l'Italia Digitale 2026.[208]

La prima missione del PNRR, quella dedicata alla digitalizzazione, si divide in 3 componenti e si pone come obiettivo la modernizzazione digitale delle infrastrutture di comunicazione del Paese, della Pubblica Amministrazione e del sistema produttivo.

Nell'aprile 2021 è stato definito il Piano strategico per la transizione digitale e la connettività del Paese, conosciuto come Italia Digitale 2026. Il primo compito, che spetta al Dipartimento per la trasformazione digitale, riguarda il passaggio verso il Cloud della PA entro il 30 giugno 2026. In Italia, la resposnsabilità della migrazione dei dati e dei servizi è stata affidata al Polo Strategico Nazionale.

In questo progetto, sono state introdotte anche iniziative volte a formare i cittadini e ad arricchire le loro competenze nel campo delle tecnologie digitali.[209]

4.5.3 PA Digitale 2026

Frutto della collaborazione tra il Dipartimento per la trasformazione digitale e dell'Agenzia per la Cybersicurezza Nazionale (ACN), la Strategia Cloud Italia segna le modalità di passaggio al cloud di dati e servizi digitali della Pubblica Amministrazione.

---

[207] Ibidem.

[208] https://www.polostrategiconazionale.it/media/news/obiettivi-italia-digitale-2026/#:~:text=Uno%20degli%20obiettivi%20dell%E2%80%99Europa%20%C3%A8%20creare%20un%20futuro,realizzazione%20di%20servizi%20pi%C3%B9%20efficienti%20e%20universalmente%20accessibili.

[209] Ibidem.

L'obiettivo principale consiste nell'accompagnare oltre il 75% delle PA nella fase di migrazione dei dati e degli applicativi informatici verso il cloud. Impresa che andrà a risolversi positivamente entro il 2026 nel rispetto degli obiettivi generali del PNRR.
Gli altri obiettivi di Italia Digitale 2026 mirano a:

- La digitalizzazione della PA, ovvero la trasformazione dei servizi pubblici in modalità digitale, tra cui la diffusione dell'identità digitale ad almeno il 70% della popolazione. Il fine è quello di creare cittadini capaci di gestire la propria identità digitale in autonomia. In questo modo si otterrà una semplificazione delle procedure burocratiche, l'automatizzazione degli iter e un miglioramento dell'efficienza dei processi amministrativi.
- Innovazione tecnologica, ossia il favorire l'adozione di tecnologie innovative da parte delle imprese e incoraggiare la ricerca e lo sviluppo in questo ambito attraverso una serie di investimenti verso start-up e progetti in grado di supportare la crescita economica.
- Connessione e infrastrutture digitali così da garantire un'ampia copertura e connettività ad alta velocità su tutto il territorio italiano, creando le basi per lo sviluppo di servizi digitali sempre più avanzati e accessibili.
- Adottare il cloud computing e portare il 75% delle PA e gli enti locali a utilizzare i servizi in cloud e far sì che almeno l'80% dei servizi pubblici essenziali siano disponibili per l'erogazione online a tutti i cittadini.
- Sviluppo delle Competenze Digitali dei cittadini e promozione dell'alfabetizzazione digitale tra la popolazione, per favorire il consolidamento di capacità per discernere tra rischi del web e le opportunità.[210]

4.6 I costi della Pubblica Amministrazione

La cybersicurezza nell'ambito della pubblica amministrazione si presenta come un aspetto cruciale, considerando che le istituzioni governative gestiscono una vasta quantità di dati sensibili e infrastrutture critiche. Di seguito una panoramica sui principali costi e rischi associati ad una protezione inadeguata della cybersicurezza:

[210] Polo strategico nazionale, Gli obiettivi di Italia Digitale 2026, novembre 2023, articolo consultabile al sito: https://www.polostrategiconazionale.it/media/news/obiettivi-italia-digitale-2026/

Vi sono in primis gli investimenti in infrastrutture e tecnologia, ad esempio l'acquisto di hardware e software di sicurezza come firewall, antivirus, sistemi di rilevamento delle intrusioni (IDS), software per la protezione dei dati (Cifrataggio), soluzioni per la gestione delle identità e dell'accesso (IAM); ed infine la manutenzione perchè le soluzioni di cybersicurezza devono essere costantemente aggiornate.

I costi connessi alla formazione continua del personale amministrativo e degli operatori pubblici sono essenziali per garantire che tutti i dipendenti comprendano le best practice in termini di sicurezza informatica (phishing, gestione delle password, uso sicuro dei dispositivi).

È possibile menzionare anche i costi di compliance, perchè la pubblica amministrazione deve rispettare le normative di sicurezza come il Regolamento Generale sulla Protezione dei Dati (GDPR) ed deve rispettare gli standard di sicurezza come ISO/IEC 27001.

È essenziale gestire i piani di risposta agli incidenti per limitare i danni in caso di violazione della sicurezza. I costi di una risposta rapida includono risorse umane, consulenze esterne, e strumenti per il monitoraggio e l'analisi degli incidenti.

Infine è possibile menzionare le assicurazioni contro le perdite da attacchi informatici, per cui alcune amministrazioni potrebbero considerare l'acquisto di polizze assicurative per coprire i costi legati derivanti dalle violazioni della sicurezza, come il recupero dei dati, la gestione delle cause legali e la risoluzione dei danni.[211]

[211] Maturità cyber, ora serve collaborazione. Frattasi: "l'ACN è al fianco delle aziende"https://www.cybersecurity360.it/cybersecurity-nazionale/maturita-cyber-ora-serve-collaborazione-frattasi-lacn-e-al-fianco-delle-aziende/

Conclusione

Nel mondo d'oggi, le aziende per operare dipendono sempre di più dalla tencologia e dai sistemi digitali, di conseguenza sono esposte sempre più frequentemente ad attacchi informatici. In questo contesto abbiamo introdotto il concetto di "Cyber Security" che non riguarda solo la protezione dei dati aziendali ma anche la difesa contro i rischi finanziari, reputazionali e legali.

La digitalizzazione rende le aziende sempre più vulnerabili alle minacce informatiche, questo perchè quasi tutte le operazioni aziendali come la gestione delle risorse aziendali, la comunicazione interna, la vendita online ed i sistemi digitali sono state soggette alla trasformazione digitale. Per proteggere la propria infrastruttura digitale e ridurre al minimo i rischi, le aziende devono adottare un approccio strategico alla cybersicurezza, che includa: gli investimenti in tecnologie di protezione, l'adozione di misure di prevenzione, la creazione di una cultura della cybersicurezza, la gestione delle vulnerabilità della supply chain e la risposta agli incidenti.

Oggi la cybersicurezza è un investimento fondamentale per ogni azienda, indipendentemente dalla sua dimensione, settore o geolocalizzazione. Con l'aumento degli attacchi informatici, i rischi in cui incorrono le aziende nel non adottare la sicurezza informatica può essere più elevato rispetto agli investimenti necessari per attuarla.

D'altra parte, investire in cybersicurezza comporta una serie di costi che le aziende devono considerare attentamente. Questi costi variano in base alla dimensione dell'azienda, al settore, alla maturità dei sistemi di sicurezza e alla strategia complessiva di gestione del rischio. La cybersicurezza oggi rappresenta un costo inevitabile ma necessario per le aziende. Sebbene i costi iniziali possano sembrare elevati, i danni derivanti da un attacco informatico sono significativamente più alti e possono compromettere la sopravvivenza dell'azienda. Investire in misure di prevenzione, formazione dei dipendenti, software di sicurezza e risorse dedicate è fondamentale per ridurre i rischi. Le aziende devono considerare la cybersicurezza non solo come una spesa operativa, ma come un investimento strategico per proteggere i propri dati, garantire la fiducia dei clienti e evitare danni finanziari.

Bibliografia

A., G. G. (2024). On the problem of defining and defining the definitions of "Information Security" and "Cyber Security".

A., L. V. (2010). Fundamentals of National Security Of Ukraine .

Clusit. (2024). *Rapporto Clusit 2024 primo semestre*. Retrieved from Rapporto Clusit 2024 primo semestre: https://clusit.it/wp-content/uploads/area_stampa/2024/Rapporto_Clusit_2024_primo_semestre.pdf

Comitel. (2023). *Rapporto Clusit 2023*. Retrieved from Rapporto Clusit 2023: https://www.comitel.net/blog/rapporto-clusit-2023-italia-sotto-assedio/

Cybersecurity - Worldwide. (2024). Retrieved from Cybersecurity - Worldwide: https://www.statista.com/outlook/tmo/cybersecurity/worldwide

Franchina, L. A. (2015). Italiano Cyber Security Report.

G. Faggioli, M. A. (2024). *Rapport Clusit.*

Giusti, N. (2024). *Attacchi informatici in Italia aumentati del 65%*. Retrieved from Attacchi informatici in Italia aumentati del 65%: https://gdprzerosanzioni.it/news-gdpr-news-privacy/attacchi-informatici-in-italia-aumentati-del-65/

Goodyear, M. P. (2010). Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers.

Greatti, M. (2024). *Access control: le basi per la sicurezza informatica aziendale*. Retrieved from Access control: le basi per la sicurezza informatica aziendale: https://www.agendadigitale.eu/sicurezza/protezione-dei-dati-sensibili-strategie-di-controllo-degli-accessi/

I., G. O. (2017). Information and Cybersecurity: Conceptual Principles and Pratical Aspects.

Lavecchia, V. (2024). *Cybersecurity: Come difendersi dai cyber attack con NIST Cybersecurity Framework e Framework CINI*. Retrieved from Cybersecurity: Come difendersi dai cyber attack con NIST Cybersecurity Framework e Framework CINI: https://vitolavecchia.altervista.org/cybersecurity-come-difendersi-dai-cyber-attack-con-nist-cybersecurity-framework-e-framework-cini/

M., S. N. (2019). Information security in the context of modern challenges: theory and practice .

Manuela Gianni, P. C. (2024). *Le minacce informatiche più pericolose e i principali settori nel mirino*. Retrieved from Le minacce informatiche più pericolose e i

principali settori nel mirino: https://www.digital4.biz/executive/minacce-informatiche-piu-pericolose-settori-colpiti-italia-mondo/

O., M. A. (2016). Cybersecurity in public administration: theory and practice .

P., M. S. (2018). Strategies for ensuring information and cyber security of the state.

PoliMi, O. D. (2023/24). *Cybersecurity in Italia: il mercato registra valori record*. Retrieved from https://www.osservatori.net/comunicato/cybersecurity-data-protection/cybersecurity-italia-mercato-crescita/

S., T. V. (2015). Cybersecurity in the National Security System of Ukraine .

SSMLG Gudimetla Naga Venkata, A. R. (2024). Cyber Security in business management . Warta Saya.

Technology, N. I. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

V., C. G. (2020). Cybersecurity: modern threats and protection .

V., T. I. (2015). Cybersecurity and protection of information system .

V., Z. O. (2021). Information Security: Textbook .

Baldoni R., Luca Montanari Editors. 2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness. Università degli Studi di Roma La Sapienza. 2014 https://www.sicurezzanazionale.gov.it/sisr.nsf/ sicurezza-in-formazione/la-cyber-security-in-italia.html

BUTTARELLI G., Hitting the ground running: How regulators and businesses can really put data protection accountability into practice, Keynote speech at European Data Protection Days (EDPD) Conference Berlin, 15 May 2017, URL: https://www.edps.europa.eu/sites/default/files/publication/17-05-15_edpd_keynote_speech_en_0.pdf.

BUTTARELLI G., The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law 6.2 (2016): pp. 77-78.

CAFAGGI F., P. IAMICELI E G.D. MOSCO [2012], Gli ultimi interventi legislativi sulle reti, in Il contratto di rete per la crescita delle imprese, a cura di F. Cafaggi, P. Iamiceli, G.D. Mosco, Milano, p. 489 ss.

CIS SAPIENZA E CONSORZIO CINI [2016], 2015 Italian Cyber Security Report. Un Framework Nazionale per la Cyber Security, 4 febbraio 2016, disponibile all'indirizzo www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf

CIS SAPIENZA E CONSORZIO CINI [2017], 2016 Italian Cyber Security Report. I controlli essenziali di sicurezza in un ecosistema cyber nazionale, 2 marzo 2017, disponibile all'indirizzo www.cybersecurityframework.it/sites/default/files/csr2016web.pdf

CONFINDUSTRIA E CERVED [2016], Rapporto PMI 2016, disponibile all'indirizzo https://know.cerved.com/it/studi-e-analisi/rapporto-cerved-pmi-2016

CONSORZIO CINI [2015], Il futuro della Cyber Security in Italia. Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni, aa cura di R. Baldoni e R. de Nicola, disponibile all'indirizzo https://www.consorzio-cini.it/index.php/it/labcshome/libro-bianco

DENHAM E., delivered this speech at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017. She discussed the role of accountability in the GDPR, underlining that "We're all going to have to change how we think about data protection".

ISTAT [2015], Struttura e competitività del sistema delle imprese industriali e dei servizi – Report anno 2013, 9 dicembre 2015, disponibile sul sito www.istat.it

JASMONTAITE L., V. VERDOODT, Accountability in the EU Data Protection Reform: Balancing Citizens' and Business' Rights. Privacy and Identity Management. Time for a Revolution?, S. MAGUIRE, A metadata-based architecture for user-centered data accountability, Electronic Markets 25.2 (2015): 155-160

MANTELERO A., Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law (2013), 3(4): 229-238. http://dx.doi.org/10.1093/idpl/ipt016, pp.234-326.

Montessoro, P. L. (2019). Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale. *LE ISTITUZIONI DEL FEDERALISMO*, *40*(3), 783-800.

MOSCO G.D. [2017], Consorzi per il coordinamento della produzione e degli scambi, in Commentario del codice civile Scialoja-Branca-Galgano, Bologna, 2017

Mosco, G. D. (2017). La collaborazione tra imprese per la sicurezza informatica. *LUISS LAW REVIEW*, (2), 157-165.

PEARSON S., Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. IFIP International Conference on Trust Management. Springer, Cham, 2017.

RABAN Y., Privacy Accountability Model and Policy for Security Organizations (20121 C. Raab, Information Privacy: Ethics and Accountability, Ethik in den Kulturen-Kulturen in der Ethik: Eine Festschrift für Regina Ammicht Quinn (2017), p. 335.

Sapienza, C. I. S. (2017). Cybersecurity National Lab.