Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2023/2024

ATTACCHI INFORMATICI E DATA BREACH IN AZIENDA: COME IL RISK MANAGEMENT E LA BUSINESS CONTINUITY POSSONO AIUTARE

Relatore: Prof. Ivan Rizzolo

Laureanda: Marta Colmaor

Matricola n. 2050859

INDICE

INTRODUZIONE

A livello globale la quantità di dati in circolazione contemporaneamente raggiunge livelli elevatissimi, il che rende estremamente difficile quantificarli in termini numerici. Nuovi dati vengono costantemente generati; inoltre, quelli esistenti possono essere modificati, aggiornati o cancellati.

Si tratta di dati di vario tipo, che possono essere espressi in diverse quantità e in diverse forme; senza considerare che essi possono essere collocati o conservati in spazi differenti, all'interno della rete o al di fuori di essa, nel mondo reale.

Molti di questi dati appartengono a persone fisiche, le quali, grazie alla diffusione delle nuove tecnologie e, in particolare, dei *social network***,** sono sempre più portate a condividere nuove informazioni su di sé. Informazioni che vengono utilizzate per manifestare all'esterno la propria identità e per comunicare agli altri la propria quotidianità, le passioni, le esperienze, lo stile di vita. Informazioni che, però, una volta immesse in rete, possono potenzialmente entrare nella disponibilità di chiunque.

Altri dati, anche non personali, sono conservati e utilizzati in misura sempre maggiore dalle imprese, che necessitano di essi per poter svolgere al meglio e in maniera più efficiente la propria attività imprenditoriale. I dati, soprattutto quelli informatici, che sempre più spesso vengono considerati il petrolio del nuovo millennio, consentono di svolgere una serie innumerevole di operazioni, come l'analisi e l'elaborazione, che permettono alle aziende di essere maggiormente competitive all'interno del mercato e di prendere decisioni migliori.

Purtroppo, però, può capitare che questi dati siano sottratti alle imprese da persone malintenzionate, sfuggendo così al controllo di chi ha diritti e doveri rispetto a tali dati. Questi ultimi, una volta acquisiti in modo illecito, possono essere utilizzati per gli scopi più disparati; ma l'obbiettivo principale dei *cyber* criminali potrebbe anche essere solo quello di creare un danno all'azienda presa di mira, in modo consapevole. Ciò si può verificare, ad esempio, nel caso delle infrastrutture strategiche, che sono quelle «Infrastrutture necessarie alla competitività del Paese e alla mobilità intelligente […] che rappresentano quindi le "priorità delle priorità"[1]».

[1] "Infrastrutture strategiche", in *Ministero delle infrastrutture e dei trasporti* [sito web], 2015, ultimo aggiornamento 21 maggio 2021, https://www.mit.gov.it/temi/infrastrutture/infrastrutture-strategiche (consultato il 19 settembre 2024).

In questo caso i cybercriminali potrebbero volerne interrompere, momentaneamente o per un periodo di tempo più prolungato, il corretto funzionamento.

Il mezzo attraverso cui, sempre più frequentemente, i soggetti malintenzionati sono in grado di accedere e di appropriarsi di dati altrui è rappresentato dalla rete Internet, mentre uno dei principali bersagli sono le imprese.

Con questo lavoro si vogliono analizzare quali sono i principali metodi e strumenti utilizzati dai *cyber* criminali per accedere a tali dati, quali sono le possibili minacce alla sicurezza dei dati, qual è la situazione degli attacchi informatici in Italia negli ultimi anni e quali possono essere gli strumenti di prevenzione a disposizione delle aziende per evitare di subire tali attacchi e di dover interrompere l'attività a causa di una violazione di sicurezza.

Ci si focalizzerà soprattutto sui due macro-concetti di *risk management* e di *business continuity*, regolati rispettivamente dagli Standard ISO 31000:2018[2] e ISO 22301:2019[3], che, se adottati in maniera corretta dalle imprese, consentono loro di non dover interrompere l'attività operativa a causa di un evento imprevisto, rappresentato, in questo elaborato, dall'attacco informatico.

[2] ISO/TC 262, "ISO 31000:2018 Risk management - Guidelines", in *ISO* [sito web], 2018[2], ultimo aggiornamento nel 2023, https://www.iso.org/standard/65694.html (consultato il 19 settembre 2024).
[3] ISO/TC 292, "ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements", in *ISO* [sito web], 2019[2], ultima modifica nel 2024, https://www.iso.org/standard/75106.html (consultato il 19 settembre 2024).

CAPITOLO I – DATA BREACH E ATTACCHI INFORMATICI IN ITALIA

1. Violazione di dati personali: nozione e normative

Prima di iniziare a trattare il tema delle violazioni di dati personali, è necessario definire che cosa si intende per "dati personali". La maggior parte delle regole e delle definizioni che hanno a che fare con questa tematica sono contenute nelle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, a cui si farà riferimento in seguito utilizzando il termine "GDPR". Il D.lgs. n. 101 del 2018 ha, poi, consentito che la normativa nazionale italiana venisse adeguata ai dettami europei.

In base a quanto previsto dall'art. 4 di tale Regolamento, un dato personale è «Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")»[1]. Esempi di dato personale sono il nome e il cognome; i numeri identificativi come il codice fiscale; il numero di telefono; l'indirizzo e-mail; i dati relativi all'ubicazione; gli identificativi online, per esempio gli indirizzi IP[2] o gli *username;* e tutte le altre informazioni che possono ricondurre ad una persona fisica specifica[3].

Sono considerati dati personali anche quelli sottoposti a tecniche di pseudonimizzazione[4], poiché, anche in questo caso, utilizzando informazioni ulteriori, sarebbe possibile ricondurre i dati in questione a determinati soggetti.

Una sottocategoria di dati personali sono i dati particolari, cioè quelli in grado di rivelare «[…] L'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici […], dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»[5]. C'è un divieto generale di trattare questo tipo di dati, salvo le deroghe stabilite dall'art. 9, par. 2 del GDPR, poiché, in base alle loro caratteristiche, essi sono considerati sensibili. Il loro trattamento, infatti, potrebbe arrecare problemi e limitazioni ai diritti e alle libertà fondamentali degli interessati[6].

[1] Regolamento (UE) 2016/679, art. 4, par. 1.
[2] Cfr. Considerando 30 del Regolamento (UE) 2016/679.
[3] Cfr. Regolamento (UE) 2016/679, art. 4, par. 1.
[4] Cfr. Considerando 26 del Regolamento (UE) 2016/679.
[5] Regolamento (UE) 2016/679, art. 9, par. 1.
[6] Cfr. Considerando 51 del Regolamento (UE) 2016/679.

Di grande rilievo, nell'ambito del GDPR, è anche l'art. 25, che introduce i concetti importantissimi di *Privacy by design* e di *Privacy by default*.

Per *Privacy by design* si intende che la protezione dei dati personali deve essere pensata e attuata fin dal momento della progettazione di un trattamento dati. L'art. 25, comma 1 del GDPR richiede che, dal momento in cui il Titolare del trattamento determina i mezzi e le finalità del trattamento, siano impiegate misure tecniche ed organizzative adeguate, come la pseudonimizzazione o la minimizzazione dei dati raccolti, al fine di garantire una protezione efficace. Tutto ciò è essenziale per soddisfare i requisiti stabiliti nel GDPR e per tutelare i diritti degli interessati[7]. Per *Privacy by default*, invece, si fa riferimento al fatto che i dati personali devono essere protetti per impostazione predefinita. Il GDPR, infatti, obbliga il Titolare del trattamento ad adottare, per impostazione predefinita, misure tecniche ed organizzative adeguate al trattamento. Ciò può avvenire, ad esempio, attraverso la raccolta dei soli dati necessari rispetto alla finalità di quello specifico trattamento[8].

È possibile, a questo punto, definire cosa sia una violazione dei dati personali. In base a quanto disposto dal GDPR, essa è «La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»[9].

Danni fisici, materiali o immateriali, come la perdita del controllo sui propri dati personali o limitazioni dei propri diritti possono essere arrecati alle persone fisiche qualora si verifichi una violazione dei dati personali e questa non sia affrontata in modo adeguato e tempestivo. A causa di un tale evento, possono anche concretizzarsi discriminazioni basate sul contenuto dei dati oggetto della violazione di sicurezza – basti pensare alla possibilità che siano coinvolti dati particolari, come le convinzioni religiose o dati relativi alla salute, ma non solo –, furti di identità, danni economici e sociali, conseguenze reputazionali, perdite di riservatezza in riferimento a dati personali sottoposti a segreto professionale e altre ripercussioni sugli interessati. È anche possibile che, grazie ai dati coinvolti nella violazione, la pseudonimizzazione diventi reversibile, permettendo di identificare l'interessato attraverso una serie di informazioni diventate accessibili.[10]

[7] Cfr. Regolamento (UE) 2016/679, art. 25, comma 1.
[8] Cfr. Regolamento (UE) 2016/679, art. 25, comma 2.
[9] Regolamento (UE) 2016/679, art. 4, par. 12.
[10] Cfr. Considerando 85 del Regolamento (UE) 2016/679.

Per limitare i danni causati da una violazione di sicurezza, sulla base di quanto disposto dal Considerando 85 del GDPR, il Titolare del trattamento deve inviare una notifica dell'avvenuta violazione all'autorità di controllo competente, cioè al Garante per la protezione dei dati personali, non appena ne sia a conoscenza. È prevista una finestra temporale entro cui la notifica dovrebbe avvenire, cioè 72 ore dal momento in cui il Titolare del trattamento prende atto della violazione. I ritardi rispetto a questo temine prefissato, devono essere giustificati. Non è necessario notificare la violazione al Garante qualora il Titolare possa dimostrare che sia scarsamente probabile che la violazione possa pregiudicare i diritti e le libertà degli interessati[11].

2. Impatto derivante da una violazione di dati

Una violazione di dati, o *data breach*, può avvenire in vario modo e può provocare conseguenze differenti. Non si può dare per scontato, infatti, che una minaccia ai dati sia il frutto di un'intenzione volontaria e consapevole di un individuo di arrecare un danno.

Classificare i possibili motivi e mezzi che possono portare a compiere una violazione di sicurezza informatica è utile per capire a cosa ci si trova di fronte e, conseguentemente, per definire delle misure di protezione da applicare ai sistemi informatici e all'organizzazione aziendale nel suo complesso, per evitare che lo strumento telematico possa essere la via attraverso cui i dati vengono violati.

In questo lavoro ci si concentrerà prevalentemente sulle violazioni di dati che avvengono nei confronti delle realtà imprenditoriali utilizzando i dispositivi informatici come mezzo tramite cui accedere ai dati, poiché questo è il caso che avviene sempre più di frequente, come si analizzerà in seguito.

Occorre, a questo punto, introdurre il concetto di "minaccia", che può essere descritta come «[…] Ogni fonte potenziale di danno all'affidabilità e integrità di un sistema»[12]. Può essere generata da ignoranza, scarse competenze, incuria, mancata formazione, cattive intenzioni o da una mescolanza di questi fattori. È importante tenere conto anche delle vulnerabilità dei sistemi informatici, poiché potrebbero essere utilizzate in maniera inconsapevole per arrecare danni[13].

Una violazione di dati può verificarsi principalmente attraverso furti, frodi, comportamenti

[11] Cfr. *Ibidem*.
[12] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 23.
[13] Cfr. *Ibidem.*

dolosi, errori umani, accesso da parte di terzi non autorizzati, incidenti o disastri[14].

Il furto si realizza nel momento in cui un soggetto vuole sottrarre in modo volontario una parte del patrimonio altrui, per trarne profitto, senza, però, provare a camuffare la condotta. Peculiare può essere il caso di furto di beni immateriali, quali i *software*, le informazioni o i dati contenuti nei dispositivi informatici, poiché la condotta di appropriazione di tali beni può avvenire creando una copia digitale, lasciando inalterato l'originale. In tal caso, chi commette il fatto, potrebbe riuscire a nascondere che ciò si sia verificato[15]. D'altronde, nel Codice Penale Italiano del 1930, considerando anche le sue successive modifiche e integrazioni, non è previsto un reato di furto che riguardi nello specifico i dati informatici, come accade per altre fattispecie in cui, a seguito dell'articolo "principale", seguono uno o più articoli sullo stesso tema che coinvolgono dati o sistemi informatici. L'art. 624 c.p., infatti, fa riferimento solo alle cose mobili per descrivere la condotta di furto, lasciando, così, una questione aperta per quanto riguarda il caso di furto di dati e programmi informatici, che potrebbe essere inquadrato all'interno di questo articolo solo attraverso un'interpretazione estensiva.

Si può, poi, verificare una frode nel momento in cui l'attaccante si appropria di *asset* aziendali raggirando ed eludendo la sorveglianza posta a presidio dei sistemi informatici, ideata proprio per scongiurare che si verifichino delle violazioni di sicurezza. Questo tipo di minaccia ai dati può concretizzarsi anche grazie alla complicità di soggetti interni all'azienda, o può manifestarsi attraverso azioni eseguite esclusivamente da essi, in quanto titolari di posizioni privilegiate che consentono di conoscere una serie di informazioni non disponibili ai terzi[16]. Guardando la questione dal punto di vista penale, la si può ricondurre nell'art. 640-ter c.p. che tratta delle frodi informatiche. In base a tale articolo è punibile chi trae un ingiusto profitto ed arreca un danno a terzi attraverso l'alterazione del funzionamento di sistemi informatici o telematici o «intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti»[17].

Violazioni di dati possono anche essere la conseguenza di attività volontarie, spontanee e intenzionali volte ad arrecare un danno. Ne sono un esempio la distruzione, la cancellazione parziale o la deliberata alterazione di dati derivanti da virus, *malware* e altri programmi installati nei dispositivi informatici altrui. A questo proposito, l'art. 615-ter c.p. si occupa di sanzionare

[14] Cfr. *Ivi*, p. 24.
[15] Cfr. *Ibidem.*
[16] Cfr. *Ibidem*.
[17] Codice Penale, art. 640-ter.

l'accesso abusivo a sistemi informatici o telematici, punendo la condotta di colui che «[…] Abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo»[18]. Questa norma punisce una serie di condotte prodromiche alla commissione di reati più gravi, come i danneggiamenti informatici o la distruzione di dati o programmi. La presenza di misure di sicurezza a salvaguardia dello strumento informatico, in questa sede, è necessaria al fine di poter far rientrare la condotta all'interno dell'art. 615-ter c.p. In assenza di tali misure, infatti, non solo lo strumento informatico risulta essere più vulnerabile e più facilmente attaccabile, ma il fatto non può più essere punito sulla base di questo articolo. Un'altra norma che deve essere tenuta in considerazione, poiché anch'essa si occupa indirettamente della sicurezza informatica, incriminando condotte prodromiche alla commissione di un più gravi reati informatici[19], è l'art. 615-quater c.p., che punisce la detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici.

Anche semplici e non voluti errori umani possono condurre a violazioni di dati. Ciò può accadere quando gli utenti che utilizzano un dispositivo informatico tengono comportamenti negligenti, imprudenti, oppure quando sono scarsamente formati; quindi, non sono consapevoli delle azioni che stanno compiendo utilizzando tale strumento. Questo, molto spesso, può provocare involontariamente errori o guasti al dispositivo o ai sistemi informatici nella loro totalità e ripercussioni sui dati, più in generale[20].

Si possono anche verificare situazioni in cui terzi non autorizzati hanno accesso ai dati; il che non avviene per forza a seguito di furti, frodi o di attività volontarie. Può succedere, infatti, che le postazioni informatiche o i luoghi in cui i dati sono conservati siano lasciate incustodite e non siano presenti misure di sicurezza, consentendo, così, ai terzi che hanno la possibilità di accedere a tali locali, di prendere visione di quelle informazioni.

Infine, può accadere che un'impresa abbia adottato tutte le misure di prevenzione che ritiene siano adatte a proteggere la sua realtà, ma che, nonostante ciò, si verifichino degli eventi non prevedibili, come gli incidenti e i disastri, che possono arrecare danni, anche gravi, ai dati e ai

[18] Codice Penale, art. 615-ter.
[19] Cfr. Alberto CADOPPI et alt., *Cybercrime*, UTET Giuridica, Milano 2019, p. 693.
[20] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 25.

sistemi informatici aziendali[21].

Quando si verifica un *data breach,* la riservatezza, l'integrità e/o la disponibilità dei dati personali, che dovrebbero essere assicurate dal Titolare del trattamento e dal Responsabile del trattamento attraverso la predisposizione di misure tecniche e organizzative adeguate, possono essere compromesse[22].

Concretamente ciò può causare la perdita di dati – che può comportare una violazione della *privacy* –, la distruzione e/o la modifica di dati, l'impossibilità di accedere ai dati, danni ai sistemi e al loro corretto funzionamento o la divulgazione non autorizzata di tali informazioni all'esterno. Queste condotte sono sanzionate penalmente da vari articoli: l'art. 615-ter c.p.[23] al comma 2 prevede un aumento di pena se, a seguito dell'accesso abusivo, derivano «[…] La distruzione o il danneggiamento ovvero la sottrazione, […] o l'inaccessibilità al titolare del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti»[24]; l'art. 617-quater c.p. (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche); l'art. 617-sexies c.p. (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche); gli artt. 635-bis e quater c.p. in riferimento ai delitti di danneggiamento di informazioni, dati, programmi e sistemi informatici privati; gli artt. 635-ter e quinquies c.p. riguardanti i delitti di danneggiamento di informazioni, dati, programmi e sistemi informatici di pubblico interesse.

Astrattamente, invece, una violazione di dati può avere un ampio impatto sull'attività aziendale. Si possono verificare perdite di competitività nel mercato, perdite di fiducia e di credibilità da parte degli *stakeholder*, perdite reputazionali, carenze di opportunità e danni di immagine. L'affidabilità dell'impresa, in generale, può essere compromessa. Per giunta, se un *data breach* ha come oggetto categorie di dati che riguardano sicurezza nazionale o internazionale, democrazia, pace, stabilità, cooperazione, giustizia, diritti umani, ambiente, salute, istruzione, cultura e così via, possono esserci anche effetti di maggiore portata che ricadono sulla società nel suo insieme[25].

---

[21] Cfr. *Ibidem*.
[22] Regolamento (UE) 2016/679, art. 32, par. 1.
[23] Accesso abusivo ad un sistema informatico o telematico.
[24] Codice Penale, art 615-ter, comma 2, n. 3.
[25] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine

2.1. Minacce interne ed esterne

Le minacce alla sicurezza dei dati e dei sistemi informatici possono provenire principalmente da due fronti.

Il primo è costituito dalla rete informatica, poiché, essendo essa una rete pubblicamente accessibile, consente a chiunque di poterla utilizzare, anche in modo anomalo, per eseguire una serie infinita di azioni. Internet rappresenta, infatti, lo strumento principale attraverso cui è possibile eseguire attacchi informatici e causare violazioni di dati verso entità anche molto distanti dall'attaccante, conosciute o casuali. I *cyber* attaccanti sempre più spesso riescono a sfruttare il fatto che, al giorno d'oggi, la quasi totalità dei dispositivi, delle attrezzature e dei macchinari aziendali sono allacciati alla rete. Basti pensare al caso dell'*Internet of Things*, che consente di connettere in rete potenzialmente qualsivoglia oggetto. Internet è lo strumento più difficile da tenere sotto controllo per quanto riguarda le minacce alla sicurezza dei dati, poiché è in continua evoluzione ed espansione.

Il secondo fronte è rappresentato da tutte le persone che hanno qualche tipo di relazione con l'impresa. Si tratta non solo di soggetti interni, come i dipendenti, che potrebbero ricoprire posizioni che consentono loro di essere a conoscenza di informazioni utili in merito alle misure di sicurezza applicate a dati e sistemi informatici; ma anche di soggetti esterni, verso cui l'azienda è, nella maggior parte dei casi, impotente[26].

In entrambi i fronti sono presenti delle componenti interne ed esterne, che, talora, però, possono essere difficili da distinguere.

La rete informatica, infatti, può essere distinta in una dimensione interna, Intranet e in una esterna, Internet. Intranet «[…] È una rete web interna, cui sono collegati i dipendenti, che vi trovano tutte le informazioni utili: dall'elenco dei dipendenti […]; fino alle notizie […]. Tutto quanto serve, informa e motiva le persone»[27]. È una rete chiusa e più facilmente controllabile, quindi meno soggetta alle minacce informatiche esterne, poiché è più complesso accedervi se non si è all'interno di una cerchia ristretta di soggetti. Internet, d'altro canto, «[…] È un mezzo che permette […] la comunicazione di molti a molti, in un tempo scelto, su scala globale»[28].

[PDF], https://clusit.it/rapporto-clusit/ (consultato il 23 settembre 2024), p.305.

[26] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 26.

[27] Alessandro LUCCHINI, *Intranet - Teoria e pratica*. Apogeo Editore, Milano 2004, p. 16.

[28] Manuel CASTELLS, *Galassia internet,* Feltrinelli, Milano 2006 [Traduzione di Stefano VIVIANI].

Essendo una rete più estesa, può più facilmente essere utilizzata per accedere ai dati, violando la sicurezza dei sistemi informatici aziendali.

Anche per le persone che si relazionano con un'impresa, può essere complicato tracciare il confine tra ciò che è interno e ciò che sta al di fuori. Non è detto, infatti, che i dipendenti di un'azienda siano solo soggetti interni, che hanno diritti e doveri stabiliti dal rapporto di lavoro. È sempre più diffusa, infatti, la pratica dell'esternalizzazione di attività e progetti verso soggetti terzi. Consulenti a progetto sono impiegati sempre più spesso dalle aziende. Essi, sebbene siano oggettivamente soggetti esterni all'impresa, vengono frequentemente trattati al pari dei dipendenti interni. Ciò può avvenire, per esempio, attraverso il conferimento di autorizzazioni che consentono loro di poter accedere a tutte le strutture aziendali, che comprendono sia gli accessi fisici, che quelli logici. Questi collaboratori devono rispettare le regole aziendali dell'impresa con cui cooperano, comprese quelle di sicurezza dei dati, ma ci sono anche aspetti che riguardano il loro modo di lavorare o la loro formazione che non possono essere controllati dall'azienda in cui operano, poiché non ne dipendono in modo diretto[29]. Resta, perciò, da capire se essi debbano essere qualificati come soggetti interni o esterni all'azienda e, quindi, se possano rappresentare delle minacce interne o esterne. Questa classificazione è importante, poiché, quanto più una minaccia è rappresentata da soggetti o entità esterne, tanto più l'influenza che l'impresa riesce ad esercitare su di loro, per esempio dal punto di vista contrattuale, sarà inferiore. Più si allarga la cerchia delle minacce esterne, più la sicurezza deve essere rafforzata dal lato dei dispositivi e dei sistemi informatici, dal momento che essi diventano l'opzione più semplice ed efficace per queste persone nel caso in cui volessero attaccare l'azienda[30].

La distinzione tra questi due profili di minaccia verrà presa in considerazione nel capitolo II per identificare i possibili rischi a cui l'impresa va incontro nel contesto della Gestione del rischio.

3. Situazione della sicurezza informatica in Italia: analisi del rapporto Clusit 2024

Un approfondimento dello stato attuale della sicurezza informatica in Italia è necessario, ora, per comprendere quali sono i principali metodi informatici utilizzati dai *cyber* criminali per

[29] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, pp. 26-27.
[30] *Ivi*, p. 28.

attaccare i sistemi informatici, qual è la gravità di tali minacce e quali sono i principali *target* degli attaccanti. Questo è utile se si vuole diffondere una cultura della prevenzione in questo ambito, poiché, nonostante l'Italia sia uno dei Paesi più colpiti da questi attacchi, molto spesso le imprese tendono a sottovalutare il problema o a sottostimare le conseguenze che ne possono derivare, almeno fino a quando una violazione di sicurezza si verifica nel concreto.

Per eseguire questa analisi si farà riferimento al Rapporto Clusit[31], realizzato dall'Associazione Italiana per la Sicurezza Informatica, una realtà che ha come scopo la promozione e diffusione della cultura e della consapevolezza sul tema della sicurezza informatica. Il Rapporto Clusit del 2024 si basa sui dati raccolti nell'anno precedente in riferimento agli incidenti considerati "gravi" andati a buon fine e sulla base delle informazioni disponibili in fonti pubbliche. Esistono, infatti, anche incidenti che, sebbene siano conosciuti da una cerchia ristretta di soggetti, non hanno risonanza pubblica. Nonostante esistano obblighi di notifica, infatti, non sempre le violazioni di dati vengono dichiarate; oppure può accadere che siano le autorità stesse a non rendere pubblici gli incidenti notificati[32].

Va prioritariamente precisato, inoltre, che gli attacchi che riferiscono alla riservatezza dei dati, all'interno di questo Rapporto, sono sottorappresentati, a causa del fatto che, per le loro caratteristiche sostanziali, potrebbero non essere conosciuti neanche alle aziende colpite. Infatti, a meno che i *cyber* attaccanti non decidano di rendere pubblica l'informazione, le organizzazioni *target* potrebbero non avere contezza di quanto accaduto[33].

Il Rapporto Clusit inizia facendo una panoramica generale di quali siano stati gli incidenti di sicurezza più rilevanti avvenuti nel panorama mondiale durante il 2023[34], da cui è possibile constatare che, quantitativamente parlando, la situazione sia di gran lunga peggiorata rispetto ai dati raccolti negli anni precedenti, seguendo una crescita costante. Mensilmente, infatti, gli attacchi di severità grave a livello mondiale sono passati da 139 a 232[35]. Ad aumentare non è solo la quantità numerica e, quindi, la frequenza con cui essi si verificano, ma anche qualitativamente parlando gli attacchi sono sempre più efficaci e provocano conseguenze

[31] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 25 settembre 2024).
[32] Cfr. *Ivi*, p. 51.
[33] Cfr. *Ibidem*.
[34] Cfr. *Ivi*, p. 7.
[35] Cfr. *Ivi*, p. 9.

sempre più impattanti[36].

In generale, rispetto alle previsioni, che sono indicate dalla linea di tendenza tratteggiata nella FIG.1, il numero di attacchi informatici particolarmente gravi, nel 2023, è stato superiore. Sono stati censiti, infatti, 2.779 attacchi, il maggior numero mai registrato[37].

FIG. 1. Rapporto Clusit 2024, p. 11 - Andamento dei Cyber attacchi gravi nel periodo 2019-2023

Il Rapporto passa, poi, a fare un resoconto di cosa sia accaduto nello specifico nel nostro Paese. L'Italia, infatti, risulta essere un bersaglio molto facile e uno dei preferiti dagli attaccanti, tanto da essere stata colpita dall'11% degli attacchi avvenuti a livello globale[38]. Questa percentuale è molto alta, se si pensa banalmente che a livello mondiale il numero di Stati suscettibili di essere danneggiati è elevato.

3.1. Principali minacce informatiche

Analizzare quali sono le possibili minacce, cioè da dove possono provenire gli attacchi e le motivazioni che vi stanno dietro, è utile per capire da cosa le aziende si devono guardare le spalle.

Secondo il rapporto Clusit, a livello mondiale, la ragione principale per cui avvengono le violazioni di sicurezza è il *cybercrime*[39]. I reati cibernetici, cioè quelli «[…] Realizzabili da chiunque nel web, in grado di colpire potenzialmente qualsiasi vittima ad esso connessa, od

[36] Cfr. *Ibidem*.
[37] Cfr. *Ivi*, p.12.
[38] Cfr. *Ivi*, p. 10.
[39] Cfr. *Ivi*, p. 13.

anche ad esso estranea»[40] sono la motivazione principale e sempre più in crescita che spinge i *cyber* attaccanti a compiere delle violazioni di sicurezza.

Il secondo tipo di attacco che avviene più di frequente è quello di *Hacktivism*[41], che si sostanzia nello sfruttamento delle conoscenze informatiche e telematiche per perseguire fini sociali, etici o politici. Può avvenire attraverso la diffusione di informazioni personali o confidenziali su persone o organizzazioni, il cosiddetto *doxxing*; oppure causando dei *DoS*[42] nella rete informatica, per metterla fuori uso; oppure ancora intaccando l'integrità di un sito web per modificarne il contenuto visivo[43].

Per converso, i casi di spionaggio e di guerra d'informazione sono diminuiti in modo significativo[44], come si può vedere dal grafico nella FIG. 2.

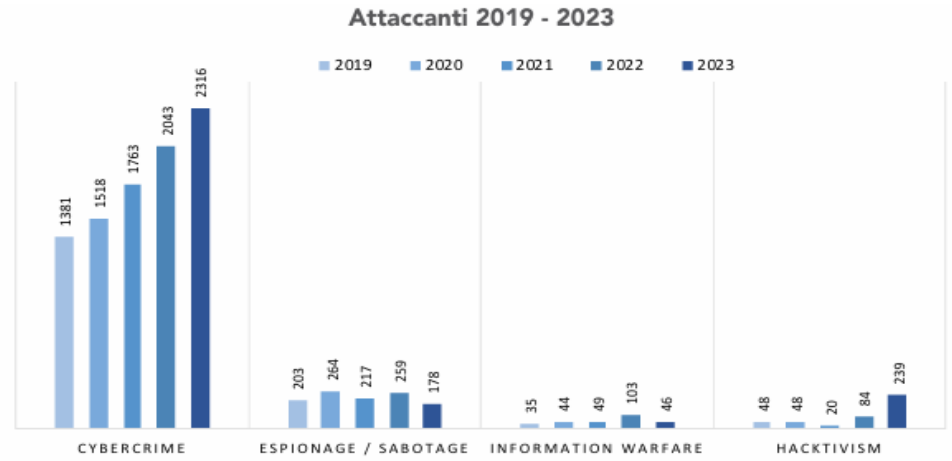

FIG. 2. Rapporto Clusit 2024, p. 14 – Cause degli attacchi informatici dal 2019 al 2023

Per quanto riguarda, invece, le tecniche utilizzate dai *cyber* attaccanti per eseguire tali azioni, il *malware* si conferma essere il veicolo di attacco principale. I *malware*, comunemente detti "virus", sono programmi informatici utilizzati per arrecare danni ai sistemi informatici altrui,

[40] Cfr. Alberto CADOPPI et alt., *Cybercrime*, UTET Giuridica, Milano 2019, p. 48.
[41] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 settembre 2024), p. 13.
[42] Un attacco di *Denial of Service*, *Dos*, è diretto ad arrestare un dispositivo informatico, una rete o un servizio. Cfr. Rapporto Clusit 2024 sulla sicurezza ICT in Italia, p. 60.
[43] Manolo FARCI et al., "Media digitali e tecnoculture maschili", in *Media digitali, genere e sessualità*, Mondadori Education, 2022, p. 275.
[44] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 settembre 2024), p. 13

per appropriarsi di informazioni o per eseguire altre condotte illecite[45]. I *malware* vengono inseriti all'interno di un dispositivo informatico attraverso l'installazione, superando eventuali barriere di sicurezza, e sono in grado di modificare le impostazioni di sistema, di attivarsi per eseguire azioni malevole e di propagarsi. Questa è la tecnica preferita dagli attaccanti, utilizzata il 36% delle volte[46].

Al secondo posto troviamo veicoli di attacco sconosciuti, mentre al terzo vengono in rilievo le vulnerabilità dei sistemi o delle reti su cui gli attaccanti fanno leva per accedere ai dispositivi e ai contenuti informatici[47].

Nonostante il *malware* continui a rappresentare in valore assoluto lo strumento a cui i *cyber* criminali fanno più spesso ricorso, in termini percentuali esso incide in misura minore sul totale degli attacchi. Al contrario, lo strumento del *Distributed Denial of Service*[48], che in valori assoluti si classificherebbe solo come la quinta modalità preferita dagli attaccanti utilizzata per introdursi nei sistemi, in termini percentuali cresce del +98%. Altrettanto vale per gli attacchi basati sulle vulnerabilità, costantemente in aumento[49].

In calo, invece, sono i tentativi di *phishing* e di *Social Engineering*[50], che agiscono sul fattore umano, manipolando i destinatari per ottenere qualcosa in cambio. Rispetto alle altre modalità di esecuzione dei crimini cibernetici, questa non sfrutta le lacune dei sistemi informatici, ma le vulnerabilità delle persone[51]. Nonostante ciò, esso resta un fattore da cui è ancora necessario difendersi attraverso la prevenzione e la diffusione di una consapevolezza d'uso degli strumenti digitali.

Anche spostandoci nella dimensione nazionale, la causa principale degli attacchi informatici gravi avvenuti nel nostro Paese è il *Cybercrime*, che rappresenta il 64% degli attacchi totali,

---

[45] Marco MEZZALAMA et alt., "Anatomia del malware" in *Mondo Digitale*, AICA, 2013, p. 2.
[46] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 settembre 2024), p. 20.
[47] Cfr. *Ibidem*.
[48] Un attacco di *Distributed Denial of Service*, *DDoS*, è in grado di amplificare la portata di un attacco *Dos*, attraverso l'uso di un gran numero di dispositivi, chiamati *botnet*, in grado di creare del traffico in rete, in particolare verso uno specifico *target*, con lo scopo di esaurirne le risorse di funzionamento e di renderlo indisponibile. Cfr. Rapporto Clusit 2024 sulla sicurezza ICT in Italia, p. 60.
[49] Cfr. *Ivi*, p. 21.
[50] Cfr. *Ibidem*.
[51] Cfr. *Ivi*, p. 74.

segnando un incremento del 13%[52]. Segue, come avviene anche a livello mondiale, il fenomeno di *Hacktivism*, che aumenta vertiginosamente, passando dai 13 eventi del 2022 ai 112 registrati nell'anno successivo[53], tanto che quasi il 47% di questo tipo di attacchi avvenuti a livello globale si è realizzato nei confronti di entità situate nel nostro Paese[54]. Nel 2023 non ci sono stati, invece, significativi attacchi attribuibili allo spionaggio, al sabotaggio o alla guerra d'informazione[55].

La modalità di attacco preferita dai *cyber* attaccanti, se a livello mondiale è rappresentata dal *malware*, a livello italiano si identifica negli attacchi *DDoS*, che aumentano del 1.486% rispetto al 2022[56]. I *malware* si guadagnano "solo" la seconda posizione, nonostante gli incidenti di questo tipo abbiano subìto un incremento in termini assoluti. Anche il *phishing* subisce una crescita in valore assoluto, che gli consente di essere la quarta modalità di attacco più utilizzata, superata solo dai veicoli di attacco sconosciuti [57]. Il *phishing*, che si conferma essere una tecnica molto efficace, viene particolarmente sfruttato come mezzo di infezione per i *ransomware*[58], che sono programmi informatici malevoli che infettano i dispositivi informatici e bloccano l'accesso alla totalità o a parte dei contenuti in essi presenti, a seguito di cui i *cyber* attaccanti chiedono che venga pagato un riscatto per riottenerne la disponibilità. Questo dimostra come nel nostro Paese il fattore umano sia ancora un punto debole che gli attaccanti riescono a sfruttare perfettamente utilizzando strategie di *social engineering*[59]. Per colmare queste vulnerabilità è necessario incrementare la consapevolezza riguardo le minacce informatiche, attraverso una costante e concreta formazione di coloro che utilizzano i dispositivi digitali.

Gli attacchi informatici, oltre a poter avere motivazioni diverse e a poter essere veicolati da mezzi differenti, possono essere anche di vario tipo. Quello più comune è l'attacco multiplo, «Caratterizzat[o] da scenari complessi che coinvolgono una combinazione di diverse tattiche […]»[60]. Un altro tipo di attacco, secondario, è quello in cui vengono esfiltrati dati particolari o riservati da un dispositivo o da una rete[61], causando un *data breach*. Nel nostro Paese, durante

[52] Cfr. *Ivi*, pp. 36-37.
[53] Cfr. *Ivi*, p. 37.
[54] Cfr. *Ibidem*.
[55] Cfr. *Ibidem*.
[56] Cfr. *Ivi*, pp. 41-42.
[57] Cfr. *Ivi*, p. 42.
[58] Cfr. *Ivi*, p. 144.
[59] Cfr. *Ivi*, p. 43.
[60] *Ivi*, p. 79.
[61] Cfr. *Ibidem*.

il 2023, sono state notificate all'Autorità Garante 2.037 violazioni di dati personali[62].

Una parentesi importante nell'analisi del rapporto Clusit deve, infine, essere dedicata alle infrastrutture critiche, cioè alle «[…] Realtà strategiche del Paese, di carattere pubblico o privato, deputate all'erogazione dei servizi essenziali e allo svolgimento dei compiti più importanti a favore della collettività»[63]. Verso questo specifico *target*, infatti, dal punto di vista statistico, si concretizzato sempre più spesso attacchi informatici, che meritano un approfondimento. Si tratta, per lo più, di attacchi volti a «[…] Paralizzare, bloccare o […] creare nocumento ai sistemi informatici e alle reti telematiche delle infrastrutture critiche»[64]. Da un tale evento, oltre all'effetto paralizzante e dannoso verso l'attività operativa, è anche possibile che derivi un'esfiltrazione di informazioni utili ai *cyber* criminali. La motivazione principale che spinge a svolgere questo tipo di attacchi verso le infrastrutture strategiche è il *cybercrime,* che, però, appare in una veste peculiare, poiché «[…] Caratterizzat[o] dall'abuso di componenti tecnologiche informatiche da parte di vere e proprie associazioni a delinquere […]»[65].

È necessario, quindi, sia nel caso delle infrastrutture strategiche, sia nel caso di tutte le altre realtà imprenditoriali, che gli organi di vertice si occupino di organizzare e far seguire corsi di prevenzione al personale che opera in tali realtà, al fine di diffondere una consapevolezza dello strumento informatico e dei rischi che esso porta con sé. Molti dei comportamenti che vengono eseguiti tramite l'utilizzo di un dispositivo digitale, in maniera automatica e impulsiva, infatti, possono nascondere delle insidie, che non dovrebbero essere sottovalutate, ma, anzi, essere prese in considerazione. Esistono, inoltre, alcune credenze in merito alla sicurezza delle comunicazioni informatiche, in particolare in riferimento ai protocolli di rete, che sono infondate, pertanto devono essere smentite.

3.1.1. HTTPS è sicuro come crediamo?

Una credenza molto diffusa tra chi non è esperto della materia e utilizza gli strumenti informatici per navigare in rete è che il protocollo HTTPS, creato per proteggere la comunicazione che avviene tra *client* e *server*[66], debba essere preferito rispetto ad HTTP, in

[62] Cfr. Pasquale STANZIONE et alt., "Relazione annuale 2023", in *Garante Privacy* [sito web], Roma 2024, 279 pagine [PDF], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10032003 (consultato il 2 ottobre 2024), p. 193.
[63] *Ivi*, p. 97.
[64] *Ibidem*.
[65] *Ibidem*.
[66] *Ivi*, p. 130.

quanto il primo sarebbe sinonimo di sicurezza della comunicazione in rete.

In realtà, oggi, quasi il 99.5% degli attacchi di *phishing* sfrutta il protocollo HTTPS, a dimostrazione del fatto che la "S" finale non indica l'affidabilità del sito web verso cui l'utente è indirizzato[67].

È dagli anni '90 che nella barra degli indirizzi dei diversi *browser* è presente un'icona a forma di lucchetto che precede i *link* agli indirizzi web che utilizzano il protocollo HTTPS[68]. Essa serve per indicare che la connessione di rete tra il *browser* e il sito è sicura e non può essere manomessa o intercettata da terzi. È, però, un residuo di un periodo in cui i siti che utilizzavano HTTPS come protocollo erano molto pochi. HTTPS, infatti, agli inizi era molto raro e Internet Explorer valorizzava questa rarità comunicando agli utenti che la connessione era protetta. In questo modo l'icona del lucchetto attirava l'attenzione degli utilizzatori sulla sicurezza fornita dal sito[69]. Questa icona, però, con il passare degli anni, si è capito possa illudere l'utente finale in merito all'affidabilità e all'attendibilità del sito e possa interferire con il giudizio che l'utente ha del sito in questione[70]. Ma, «Se l'uso di una connessione HTTP di tipo semplice (http://) sicuramente non fornisce nessuna garanzia sulla controparte, l'uso del protocollo HTTPS, senza successive verifiche sul tipo di certificato, chi lo ha emesso e per quali scopi, parimenti non può darci nessuna indicazione di sicurezza»[71].

Una connessione che usa HTTPS assicura all'utente che la comunicazione sia cifrata; a garanzia di ciò esiste il certificato SSL/TLS. Quest'ultimo può essere validato in vario modo, per esempio attraverso il *Domain Validation*, che, oltre ad assicurare che la comunicazione sia sicura e cifrata, dimostra che chi richiede tale certificato ha anche il controllo del dominio. I *phisher* utilizzano sempre più spesso domini certificati con questa modalità, che però dicono molto poco su chi possieda quel determinato sito web. Il *Domain Validation*, infatti, ci dice solo chi può avere accesso a tale dominio, non chi ne sia il proprietario. Questa ambiguità viene utilizzata dai *cyber* attaccanti per far credere all'utente finale che il sito web verso il quale esso

---

[67] *Ibidem*.
[68] Cfr. David ADRIAN et alt., "An Update on the Lock Icon", in *Chromium Blog* [sito web], 2023, ultimo aggiornamento 2 maggio 2023, https://blog.chromium.org/2023/05/an-update-on-lock-icon.html (consultato il 2 ottobre 2024) [tradotto in italiano da chi scrive].
[69] Cfr. *Ibidem*.
[70] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 2 ottobre 2024), p. 130.
[71] *Ivi,* p. 130.

viene reindirizzato, sia un sito sicuro.[72].

Questo è il motivo principale che nel 2023 ha spinto Google Chrome a rimuovere quel tipo di icona dalla barra degli indirizzi e a sostituirla con una più neutra[73]. L'intenzione, infatti, è di evitare che il lucchetto sia considerato sinonimo di affidabilità e di sicurezza[74].

Un'altra informazione molto utile, che dovrebbe essere condivisa il più possibile, è che un *click* sull'icona che precede l' "https://" dà la possibilità all'utente di visionare tutte le misure di sicurezza di quel sito, compresa la validità dei certificati ad esso associati[75]. Questo è un passaggio molto utile e che dovrebbe essere seguito quando si naviga sul web, soprattutto su siti che non si conoscono, poiché contiene informazioni importanti e valide sulla sicurezza.

3.2. Severità degli attacchi

Dopo aver analizzato le principali e più recenti minacce informatiche è necessario concentrarsi su un elemento strettamente correlato: la severità dell'attacco. Esaminare quanto un attacco possa essere severo significa andare a determinare qual è l'impatto che può derivare dall'incidente informatico[76].

Da quanto emerge dal Rapporto Clusit 2024, negli ultimi anni la gravità degli incidenti informatici nel complesso è aumentata considerevolmente[77]. A crescere sono soprattutto gli attacchi informatici che provocano conseguenze critiche[78].

Le variazioni della severità di un attacco possono essere osservate a partire da tre parametri: in base al tipo di attaccante, in base al tipo di vittima o in base alla tecnica di attacco.

Basandoci sul soggetto attaccante, « Il confronto tra i dati 2023 […] e 2022 […] evidenzia un'evoluzione nella *severity* degli incidenti dovuti a *Cybercrime*, andando a sottolineare che, indipendentemente dai numeri, gli attacchi nel 2023 […] hanno determinato mediamente

[72] Cfr. *Ivi*, pp. 130-131.
[73] Cfr. *Ivi,* p. 130.
[74] Cfr. David ADRIAN et alt., "An Update on the Lock Icon", in *Chromium Blog* [sito web], 2023, ultimo aggiornamento 2 maggio 2023, https://blog.chromium.org/2023/05/an-update-on-lock-icon.html (consultato il 2 ottobre 2024) [tradotto in italiano da chi scrive].
[75] Cfr. *Ibidem*.
[76] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 2 ottobre 2024), p. 22.
[77] Cfr. *Ibidem*.
[78] Cfr. *Ivi*, p. 23.

conseguenze maggiormente critiche»[79]. Gli attacchi con conseguenze critiche relativi all'*Hacktivism*, invece, diminuiscono[80].

Relativamente alle vittime, invece, è possibile riscontrare un incremento degli impatti critici nei confronti degli istituti finanziari e assicurativi, del settore sanitario, di quello tecnico-scientifico-professionale e di quello informatico[81].

In ultima istanza, basandoci sulle tecniche utilizzate per condurre l'attacco, è possibile rilevare che tutte hanno comportato un'ampia percentuale di conseguenze critiche[82]. Il *malware* e il *phishing* rimangono costanti nel provocare conseguenze critiche; gli attacchi che approfittano delle vulnerabilità presenti nei sistemi, invece, determinano conseguenze più gravi rispetto al 2022. Un dato particolare emerge per quanto riguarda i *DDoS* che, sebbene siano aumentati numericamente, hanno provocato conseguenze molto meno gravi, se paragonate all'anno precedente[83].

A livello nazionale la severità alta è in linea con il dato mondiale, mentre quella critica è molto inferiore. L'impatto di severità media, al contrario, è molto più alto. Complessivamente è un quadro positivo, poiché vuol dire che gli attacchi critici ci danneggiano meno che nel resto del mondo e che gli attacchi con impatto medio, anche se più numerosi, provocano conseguenze più limitate[84]. Ciò nonostante, questo fa notare che attacchi potenzialmente meno gravi, che in altri Stati vengono prevenuti o mitigati di più – motivo per cui non rientrano affatto nella statistica – in Italia arrivano ad avere gravità di livello medio, a causa della scarsa cultura in ambito di prevenzione[85].

3.3. I bersagli preferiti dagli attaccanti

A livello globale la maggior parte degli attacchi informatici è diretta verso bersagli multipli. Seguono gli incidenti che colpiscono il settore sanitario, quelli nei confronti di istituzioni e organismi governativi, quelli verso istituti assicurativi/finanziari e quelli che impattano sul settore informatico. Si accodano, poi, nella classifica il settore educativo, quello manifatturiero, quello dei trasporti e quello delle vendite; tutti in incremento rispetto all'anno precedente. Il

[79] *Ivi*, p. 25.
[80] Cfr. *Ibidem*.
[81] Cfr. *Ivi*, p. 27.
[82] Cfr. *Ivi*, p. 29.
[83] Cfr. *Ibidem*.
[84] Cfr. *Ivi*, p. 45.
[85] Cfr. *Ivi*, p. 46.

settore manifatturiero, nello specifico, raggiunge il suo massimo storico per numero di incidenti[86].

In Italia, nello specifico, sono avvenuti 310 attacchi noti di particolare gravità[87], segno che i *cyber* criminali tendono a prediligere i *target* situati nel nostro Paese, dal momento che questi ultimi sono meno capaci di proteggersi adeguatamente. Ciò è molto grave, soprattutto se si pensa al fatto che gli investimenti in sicurezza informatica continuano a crescere[88]. A conferma di questo dato, nel 2023 l'Italia ha speso 2,149 miliardi di euro in cybersicurezza, che corrispondono a circa lo 0,12% del PIL[89].

Il settore verso cui è diretta la maggior parte degli attacchi, come è possibile vedere nella FIG. 3, è quello governativo, seguito dal manifatturiero e da quello dei trasporti[90].

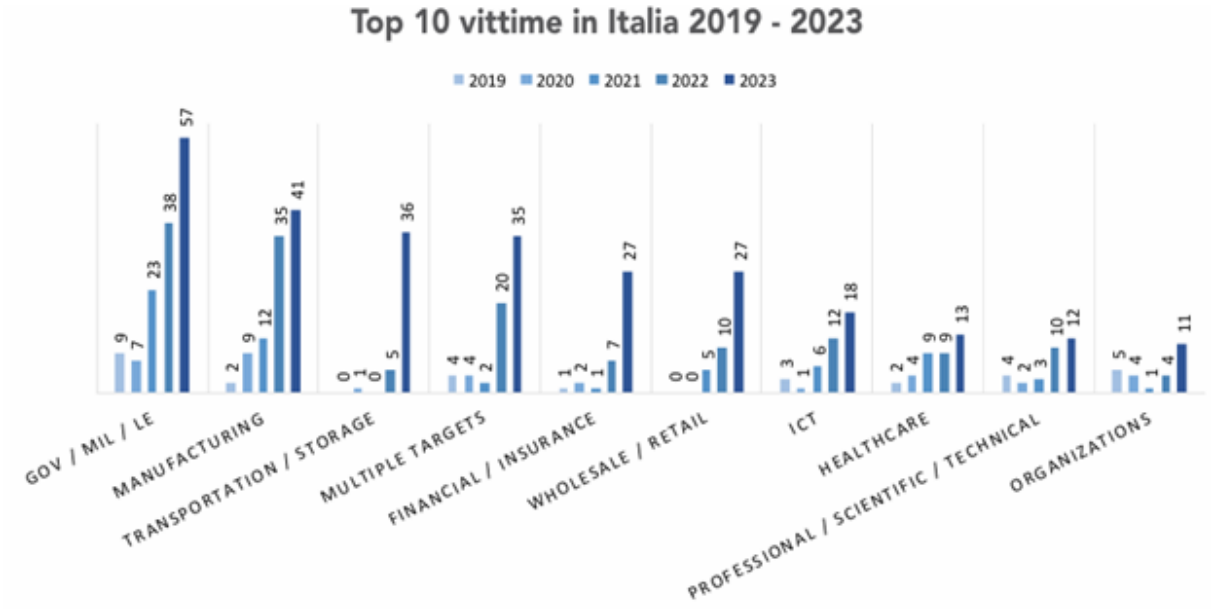

Fig. 3. Rapporto Clusit 2024, p. 40 – Top 10 vittime in Italia 2019-2023

Sono, poi, in aumento gli attacchi che arrecano danno ad alcuni settori vitali per la collettività, come le strutture sanitarie – questi dati sono in parte inclusi negli attacchi multipli nella FIG. 3 – poiché le reti informatiche di queste strutture spesso sono poco protette e poco reattive. Le informazioni che esse possiedono, come i dati particolari dei pazienti, inoltre, sono

[86] Cfr. *Ivi,* p. 15.
[87] Cfr. *Ivi*, p. 33.
[88] Cfr. *Ivi*, p. 34.
[89] Cfr. *Ivi*, p. 5.
[90] Cfr. *Ivi*, p. 38.

di ampio interesse per i *cyber* criminali[91]. Dal momento che le strutture sanitarie non possono permettersi di interrompere la loro attività, in cui anche lo strumento informatico è, il più delle volte, necessario, questi attacchi risultano particolarmente redditizi, soprattutto se condotti utilizzando *ransomware*. Spesso in questo settore si decide di pagare in tempi brevi il riscatto richiesto dagli attaccanti[92]. Sulla base dei dati raccolti nel 2023 è possibile dire che il 93% degli incidenti pubblici andati a buon fine nei confronti di questo specifico settore ha comportato conseguenze gravi o gravissime[93] e ciò può mettere a rischio, oltre ai dati personali dei pazienti, la continuità delle cure mediche e la sicurezza dei dispositivi impiegati a questo scopo[94].

3.4. Considerazioni finali Rapporto Clusit 2024

Nel complesso i dati raccolti nel Rapporto Clusit del 2024 risultano peggiori rispetto all'anno precedente. Attaccare il nostro Paese è facilmente possibile per i cyber criminali, principalmente perché gli strumenti di prevenzione e di reazione agli attacchi informatici utilizzati non sono all'altezza. Dando un rapido sguardo al futuro, è possibile dire che probabilmente questi dati sono destinati ad aggravarsi, dato che le modalità di attacco sono sempre più sofisticate, anche grazie all'uso dell'Intelligenza Artificiale[95].

Se le imprese e tutte le altre realtà presenti nel territorio vogliono essere all'altezza, è necessario che adottino fin dalla fase di *design* strumenti di difesa e di reazione. È molto importante, infatti, essere capaci di «[…] Identificare, analizzare, valutare e gestire i rischi informatici, sia con misure preventive che di mitigazione, ma anche nella prospettiva di gestire il trasferimento del rischio verso terzi […]»[96]. Come si vedrà, il fattore umano è quello su cui occorre principalmente agire, poiché esso può costituire sia una minaccia, sia una risorsa. «[…] Basare la sicurezza e la gestione delle vulnerabilità solo sui *penetration test* triennali o annuali, non è più sufficiente […]. È necessario ragionare in ottica di processi di reale presidio continuo della sicurezza di prodotti e servizi lungo l'intero ciclo di vita […]»[97].

Il bisogno di migliorare il livello della *cybersicurezza* ha portato l'Unione Europea ad adottare la Direttiva NIS 2[98] del 2022, recepita in Italia dal D.lgs. 4 settembre 2024, n. 138, che

[91] Cfr. *Ivi*, pp. 98-99.
[92] Cfr. *Ivi*, p. 99.
[93] Cfr. *Ivi*, p. 158.
[94] Cfr. *Ivi*, p. 160.
[95] Cfr. *Ivi*, p. 39.
[96] *Ivi*, p. 47.
[97] *Ivi*, p. 48.
[98] Direttiva UE 2022/2555, attuata in Italia con il D.lgs. 4 settembre 2024, n. 138.

estende l'ambito di applicazione della precedente Direttiva NIS[99].

La Direttiva NIS 2 impone agli Stati Membri di determinare una strategia nazionale per la *cybersicurezza* e di designare autorità competenti in materia, come il *Computer Security Incident Response Team*[100]. Richiede a coloro che sono soggetti a tale disciplina di dotarsi di un sistema di gestione dei rischi, di saper gestire la continuità operativa per garantire che le attività possano proseguire senza interruzioni significative, di essere in grado di rilevare, gestire e segnalare in modo tempestivo gli incidenti informatici, di adottare modelli organizzativi per gestire la *cybersecurity*, di responsabilizzare gli organi di gestione e di prevedere attività di formazione in questi ambiti[101].

[99] Direttiva UE 2016/1148, attuata in Italia con il D.lgs. 18 maggio 2018, n. 65.
[100] Cfr. *Ivi*, p. 160.
[101] Cfr. *Ivi*, pp. 161-162.

CAPITOLO II – RISK MANAGEMENT E SFIDA ALL'INCERTEZZA

1. Percezione del rischio

Nel nostro Paese la percezione del rischio in ambito informatico è molto bassa. Una tendenza strettamente connessa è quella di sottovalutare il rischio di perdere la disponibilità, l'integrità e la confidenzialità di dati e informazioni.

Per analizzare come generalmente il rischio è percepito dalle persone è utile fare riferimento al concetto di "incertezza". Quest'ultima può essere definita come l'impossibilità di sapere preventivamente ciò che accadrà in futuro; fa parte della quotidianità nella quale siamo immersi e non può essere rimossa totalmente. Negli ultimi anni, a causa del cambiamento epocale avvenuto dal punto di vista sociale e tecnologico, l'incertezza è aumentata e, con essa, l'instabilità e l'imprevedibilità delle cose[1]. In un periodo storico in cui l'informazione e la comunicazione rappresentano sempre più spesso il veicolo tramite cui viene diffusa la conoscenza, è importante capire quale relazione ci sia tra informazione e percezione dell'incertezza. Se «Da un lato l'informazione è il fattore in grado di ridurre o aumentare il grado di incertezza»[2], «Dall'altro […] ne rappresenta il prodotto, ovvero, l'insieme di tutti i dati che una qualsiasi situazione genera […]»[3]. I due concetti sono strettamente collegati: maggiore è l'incertezza di cosa accadrà, maggiore sarà anche la quantità di informazioni disponibili[4].

Il rischio, in un contesto di incertezza, misura in termini di probabilità se un danno possa essere concretamente generato da una fonte di pericolo[5]. Il rischio, quindi, combina la possibilità che si verifichi un evento avverso e le conseguenze che possono derivarne[6]. La frequenza, invece, determina quante volte il danno può verificarsi all'interno di una parentesi temporale predefinita[7]. Il calcolo del rischio in termini matematici serve a comprendere quanto

[1] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 2.
[2] *Ibidem*.
[3] *Ibidem*.
[4] Cfr. *Ibidem*.
[5] Cfr. *Ivi*, p. 4.
[6] Cfr. *Ivi*, p. 9.
[7] Cfr. *Ivi*, p. 10.

una situazione di pericolo possa essere seria e permette di poterla affrontare in modo adeguato[8].

La percezione del rischio può essere diversa tra soggetti differenti, condizionata da elementi quali l'età, il sesso, il *background* culturale e familiare, le esperienze e la cultura in materia di rischio[9].

2. Perché investire in prevenzione?

Dal momento che è impossibile eliminare del tutto l'incertezza, una scelta astuta per le aziende è quella di sfruttarla in modo intelligente. Viviamo, infatti, in un contesto di costante cambiamento e rinnovamento, nel quale saper affrontare l'incertezza in maniera proattiva, andando a trasformarla in opportunità, è essenziale per le realtà imprenditoriali[10]. Per farlo si può seguire il metodo delle "3 R": Riconoscere, Ridurre e Rispondere all'incertezza. Per prima cosa, infatti, è necessario avere consapevolezza e analizzare la situazione che si vuole affrontare; per secondo è necessario gestire l'incertezza attraverso la prevenzione del rischio; infine, se la prevenzione è impossibile, è necessario limitare o trasferire all'esterno i danni creati dal verificarsi di un rischio[11].

Il *Risk Management* viene sviluppato negli Stati Uniti tra il 1940 e il 1950 come processo continuo di prevenzione dei rischi. Esso consiste nel pianificare a priori e in modo consapevole modalità e strategie di gestione dei rischi interni ed esterni alle imprese e ha come obiettivo finale quello di ridurre l'incertezza che si verifichi un evento avverso. Si inserisce nelle attività aziendali: non è una funzione indipendente, ma «una parte fondamentale delle attività di pianificazione, organizzazione, controllo, direzione e coordinamento»[12]. Richiede a coloro che usufruiscono di tale metodologia di possedere una visione complessiva della struttura aziendale, dal punto di vista operativo e gestionale[13]. Lo scopo ultimo è quello di sviluppare e diffondere una vera e propria cultura del rischio a tutti i livelli aziendali.

In Italia, come si è visto, manca questa cultura della prevenzione, per motivi diversi. Ciò può essere causato dall'assenza di conoscenza dei possibili rischi presenti all'interno della realtà

[8] Cfr. *Ivi*, p. 12.
[9] Cfr. *Ivi*, p. 20.
[10] Cfr. *Ivi*, p. 31.
[11] Cfr. *Ivi*, p. 33.
[12] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 31.
[13] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 71.

imprenditoriale; meno si ha contezza dei rischi presenti, meno sono le possibilità di riuscire a gestirli e limitarli in maniera appropriata. Un'altra possibile causa è quella economica, poiché spesso le aziende credono di poter fare a meno della prevenzione in quest'ambito, per evitare di dover spendere somme di denaro che non ritengono essere necessarie e, al contrario, pensano sia più giustificato e meno dispendioso pagare per risolvere il problema dopo che un certo rischio si è concretizzato[14]. «Se imparassimo a pensare alla prevenzione come uno strumento anche per risparmiare (sia economicamente, sia in termini di salvaguardia dell'ambiente coinvolto e delle persone che lo vivono), avremmo società più sicure e sane»[15].

Se guardiamo il problema dal punto di vista dell'infrastruttura informatica e dei dati in essa presenti, diventa ancora più importante la capacità dell'azienda di saper creare preventivamente un ambiente sicuro e reattivo, in grado di limitare la possibilità che si verifichino incidenti o attacchi informatici che causano violazioni di dati. L'arco temporale in cui questo tipo di eventi deve essere contrastato è, infatti, quello che precede l'attacco e non quello successivo. Scegliere di proteggere preventivamente e in modo strategico il patrimonio aziendale in questa parentesi temporale è una scelta che può creare grandi vantaggi, andando a ridurre al minimo la possibilità che si verifichino degli eventi avversi[16].

Anche la protezione dati deve essere garantita. Questo avviene sia grazie al rispetto, da parte dell'azienda, della normativa in materia di tutela dei dati personali, utilizzando misure tecniche e organizzative adeguate come la cifratura, la pseudonimizzazione o predisponendo *by design* e *by default* misure che garantiscano la sicurezza di dati e informazioni, ma anche avendo consapevolezza di come strutturare un quadro complessivo di gestione dei rischi[17].

2.1. Casi di obbligatorietà

Le Linee guida sulla gestione del rischio sono contenute nello Standard ISO 31000:2018[18]. Essendo, però, uno Standard e non una norma, la sua applicazione non è obbligatoria per le

[14] Cfr. *Ivi*, p. 74.
[15] *Ibidem*.
[16] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 44.
[17] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 17 ottobre 2024), pp. 305-306.
[18] ISO/TC 262, "ISO 31000:2018 Risk management - Guidelines", in *ISO* [sito web], 2018[2], ultimo aggiornamento nel 2023, https://www.iso.org/standard/65694.html (consultato il 20 ottobre 2024).

imprese, le quali, nella maggior parte dei casi, possono decidere se aderirvi o meno. Tuttavia, esistono altre norme, come la direttiva NIS, che richiedono a certi tipi di imprese di aderire a un sistema di gestione dei rischi. Le aziende potrebbero adempiere a tali prescrizioni attraverso l'utilizzo delle linee guida in questione.

A livello europeo si ritiene che la cybersicurezza sia il pilastro portante della trasformazione digitale in tutti i settori; perciò, nel 2016 è stata emanata la Direttiva NIS[19] sulla sicurezza delle reti e dei sistemi informativi nell'Unione. Essa si occupava di sicurezza cibernetica[20] e voleva garantire che le reti e i sistemi informatici fossero resistenti ad azioni in grado di compromettere la disponibilità, autenticità, integrità o riservatezza dei dati trattati. Uno dei modi in cui ciò poteva avvenire era la promozione di una cultura di gestione del rischio[21]. Destinatari di tale Direttiva erano gli operatori dei servizi essenziali, cioè i «soggetti pubblici o privati che forni[va]no un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali nonché dipendente dalla rete e dai sistemi informativi»[22] e i fornitori di servizi digitali[23].

A seguito di questa prima direttiva, nel 2024, è stata emanata la Direttiva NIS 2[24], che si applica ai soggetti pubblici e privati nel settore dell'alta criticità, alle pubbliche amministrazioni e a ulteriori tipologie di soggetti, quali i servizi di trasporto pubblico locale, gli istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società in house, società partecipate, società a controllo pubblico, ecc. [25]. Le imprese e gli enti soggetti a tale direttiva devono adottare misure in materia di gestione del rischio, in particolare di quello cibernetico. Questo requisito può essere rispettato seguendo le linee guida dello Standard 31000:2018. Per quanto riguarda, invece, i soggetti non menzionati dalla direttiva, l'Unione Europea richiede agli Stati membri di garantire che tali realtà abbiano comunque dei livelli elevati di cybersicurezza e che seguano metodi equivalenti alla gestione del rischio[26].

[19] Direttiva UE 2016/1148, attuata in Italia con il D.lgs. 18 maggio 2018, n. 65.
[20] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 11.
[21] Cfr. *Ibidem*.
[22] *Ivi*, p. 12.
[23] Cfr. *Ibidem*.
[24] Direttiva UE 2022/2555, attuata in Italia con il D.lgs. 4 settembre 2024, n. 138.
[25] Si veda, per informazioni più dettagliate il D.lgs. 4 settembre 2024, n. 138, art. 3 e relativi allegati.
[26] Direttiva UE 2022/2555, Considerando 13.

Anche le norme in materia di protezione dei dati personali[27] e di prevenzione dei reati informatici in azienda[28], richiedono di seguire il metodo della *compliance*, in cui «[…] La legalità dell'impresa viene implementata e garantita attraverso una valorizzazione della struttura organizzativa, pensata attraverso le fasi di valutazione e gestione del rischio aziendale […]»[29]. Per questo motivo è fondamentale predisporre misure tecniche e organizzative adeguate seguendo un approccio basato sul rischio, andando ad analizzare e gestire quest'ultimo, ma anche assegnando responsabilità, formando il personale e migliorando i processi aziendali[30]. Anche in questo caso si fa riferimento, implicitamente, alle Linee guida presenti all'interno dello Standard 31000:2018.

3. ISO 31000 – Principi, quadro e processi di gestione del rischio

Nel 2009 l'organismo di standardizzazione ISO ha introdotto la famiglia di standard 31000, avendo come obiettivo quello di indicare dei principi che, qualora seguiti, possono migliorare l'efficacia del *risk management*[31].

Entrando nello specifico all'interno dello Standard 31000:2018, è possibile notare una suddivisione in tre macro-aree: principi di gestione del rischio, quadro di gestione del rischio e processi di gestione del rischio. L'elemento su cui si basa la gestione del rischio è quello del "*what if…?*". Durante tutte le fasi, infatti, ci si deve chiedere sempre cosa succederebbe se capitasse un certo evento. Inoltre, qualsiasi modifica di un elemento del sistema o nuove introduzioni devono sempre essere precedute da un'attenta analisi e da un controllo della solidità del sistema nel suo insieme[32].

Uno Standard, in generale, cerca di mettere per iscritto una serie di comportamenti condivisi da una comunità di persone nel fare una determinata cosa. In questo contesto, però, i contenuti delle linee guida devono essere adattati al contesto aziendale specifico.

3.1. Principi

Innanzitutto, per poter considerare efficace la gestione del rischio, è necessario che essa

[27] Regolamento (UE) 2016/679.
[28] D.lgs. 8 giugno 2001, n. 231.
[29] Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 22.
[30] Cfr. *Ibidem*.
[31] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 33.
[32] Cfr. *Ivi*, p. 32.

generi valore per l'azienda, concorrendo a raggiungere i traguardi prestabiliti dall'impresa. Deve, inoltre, contribuire all'innovazione e al miglioramento continuo[33].

È fondamentale che la gestione del rischio sia integrata in tutti i processi, aree, progetti, funzioni, attività e livelli organizzativi e che non sia, al contrario, una funzione aziendale separata. L'integrazione, infatti, deve essere sia orizzontale, cioè tra attività e persone all'interno dello stesso processo organizzativo, sia verticale, cioè tra livelli aziendali diversi[34]. È una responsabilità del *management* realizzare tutto questo in modo strutturato[35] e tenendo conto di tutte le informazioni che si hanno a disposizione: più sono, più consentono un alto livello di dettaglio e precisione. Dati conservati dal passato, situazioni già vissute, osservazioni da parte di tutti coloro che si trovano nella realtà imprenditoriale e di esperti esterni, nonché *feedback* sono molto utili a questo scopo[36].

La gestione del rischio deve essere adattata alla realtà imprenditoriale, poiché ogni settore può avere necessità differenti e può contemplare rischi di diverso genere. L'incertezza deve essere affrontata in modo tempestivo, cercando di utilizzare criteri affidabili e che permettono di comparare i risultati ottenuti. L'analisi del contesto interno ed esterno è, infatti, il primo dei processi di gestione del rischio, poiché consente di capire quali sono gli obiettivi da raggiungere, l'ambiente, gli *stakeholder* e i profili di rischio[37].

In questo scenario sono anche da tenere in considerazione i fattori umani e culturali, poiché le abilità e le intenzioni di coloro che sono interni o esterni all'impresa possono avere degli effetti nel quadro complessivo, potendo rappresentare sia un rischio, sia una risorsa.

Complessivamente deve essere un processo dinamico, che consente di essere modificato qualora accadano eventi all'interno o all'esterno di quella specifica realtà[38].

3.2. Quadro

Il quadro di gestione del rischio segue il modello PCDA (Plan-Do-Check-Act)[39],

[33] Cfr. *Ivi*, p. 34.
[34] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 71.
[35] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 34.
[36] Cfr. *Ibidem*.
[37] Cfr. *Ivi*, p. 33.
[38] Cfr. *Ivi*, p. 34.
[39] Cfr. *Ivi*, p. 35.

riscontrabile, in modo più dettagliato, nella Fig.4.

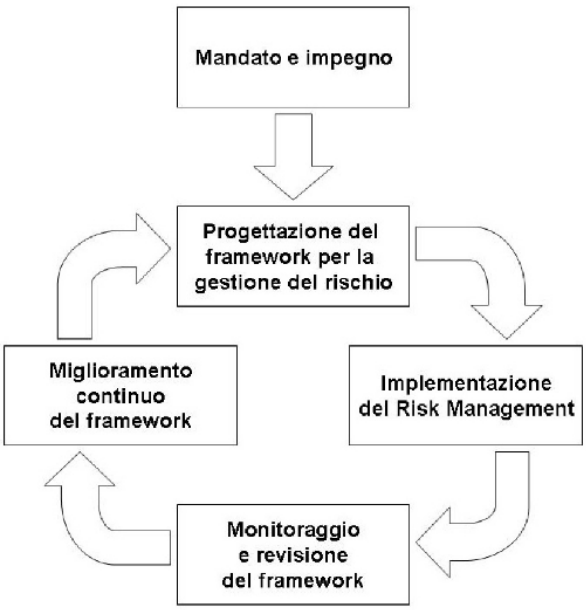

FIG. 4. Security Risk Management 2010, p. 35 - Framework della gestione del rischio.

Come prima cosa è necessario che il *management* aziendale e, a cascata, tutta l'organizzazione, si impegni nella realizzazione del quadro di gestione del rischio. Il *management* deve preparare in modo accurato l'attività creando piani dettagliati, deve definire quali sono le politiche da seguire, individuare gli indicatori da utilizzare durante il procedimento, allineare gli obiettivi aziendali a quelli di gestione del rischio e far rispettare le normative. Anche in riferimento alla protezione dei dati, è necessario stabilire delle linee guida su come essi devono essere gestiti e tutelati. Sotto un profilo più pratico vanno conferite a vari livelli organizzativi responsabilità differenti e adeguate al ruolo svolto e assegnate risorse adeguate, anche dal punto di vista economico[40].

È possibile, a questo punto, progettare il quadro per la gestione del rischio. Va, innanzitutto, analizzato il contesto imprenditoriale in cui ci si trova e gli elementi importanti che incidono nella definizione del quadro. L'analisi del contesto esterno deve tenere in considerazione elementi quali l'ambiente socio-culturale, le norme giuridiche, gli aspetti economici, finanziari e tecnologici e la competitività dell'impresa. L'esame del contesto interno, invece, va ad analizzare la struttura dell'organizzazione, i ruoli, le responsabilità, le risorse, il *know how*, l'infrastruttura informatica, la cultura aziendale e le relazioni tra i soggetti interni, ma anche ulteriori elementi specifici di quella realtà. È necessario, in questa fase, far combaciare le

[40] Cfr. *Ibidem*.

politiche che si vogliono adottare con gli obiettivi dell'impresa e rendere accessibili le risorse economiche affinché l'attività possa proseguire. Deve essere anche deciso chi si occuperà di queste attività; perciò, tra il personale a disposizione, si devono individuare i soggetti che hanno specifiche competenze ed esperienza. Tuttavia, è molto utile coinvolgere più persone possibile al fine di rendere il processo efficiente e di diffondere motivazione a tutti i livelli organizzativi. Per garantire che ci sia una corretta comunicazione, in questa fase e in quelle successive, il protocollo comunicativo deve essere prestabilito. Tutte le procedure e le attività devono essere documentate[41].

Si può passare, poi, a implementare il quadro di gestione del rischio. Devono essere stabiliti tempi e modi per l'implementazione e devono essere applicate tutte le politiche decise nelle fasi precedenti. Le decisioni del *management* devono tenere conto dei risultati del processo di gestione del rischio. Tutto ciò deve essere svolto nel rispetto delle norme giuridiche in vigore. È fondamentale, in questa fase, che ci sia comunicazione e che si svolga un'attività di formazione rivolta a tutti coloro che sono coinvolti nel cambiamento[42].

Il quadro creato, per essere efficace, deve essere costantemente monitorato e rivisto. È necessario misurare periodicamente le *performance* e i progressi rispetto agli indicatori che sono stati stabiliti nelle prime fasi. Anche le deviazioni rispetto al piano concordato devono essere valutate e riviste. Il piano, nel complesso, va controllato e modificato se avvengono dei cambiamenti del contesto o se ci si rende conto che determinate misure non sono efficaci, a differenza di quanto ci si aspettava[43]. Anche i dati e i sistemi hanno la necessità di essere monitorati; in particolare, può essere utile l'analisi delle attività, degli incidenti e delle anomalie relative alla sicurezza dei dati, utilizzando metodi come l'analisi dei *log*, l'*auditing*, i test e così via. Le risposte ad eventuali problemi riscontrati devono avvenire tempestivamente, ad esempio attraverso il contenimento, il recupero dei dati o la mitigazione, a cui segue poi il ripristino dei dati o dei sistemi attraverso tecniche opportune, come il *backup*, il ripristino, il *disaster recovery*[44].

I risultati ottenuti dalla fase precedente devono essere utilizzati per prendere decisioni che

[41] Cfr. *Ivi*, pp. 35-37.
[42] Cfr. *Ivi*, pp. 37-38.
[43] Cfr. *Ivi*, p. 38.
[44] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 22 ottobre 2024), pp. 310-311.

consentano di migliorare sempre più il quadro, le politiche, il piano di gestione del rischio e, di conseguenza, la sicurezza dei dati e quella informatica. Si deve creare e diffondere una vera e propria cultura di gestione del rischio[45].

3.3. Processi

Un buon sistema di gestione del rischio deve essere ben pianificato; per questo motivo, lo Standard indica una serie di processi da seguire per compiere al meglio l'attività di gestione del rischio, come è possibile vedere nella FIG. 5.

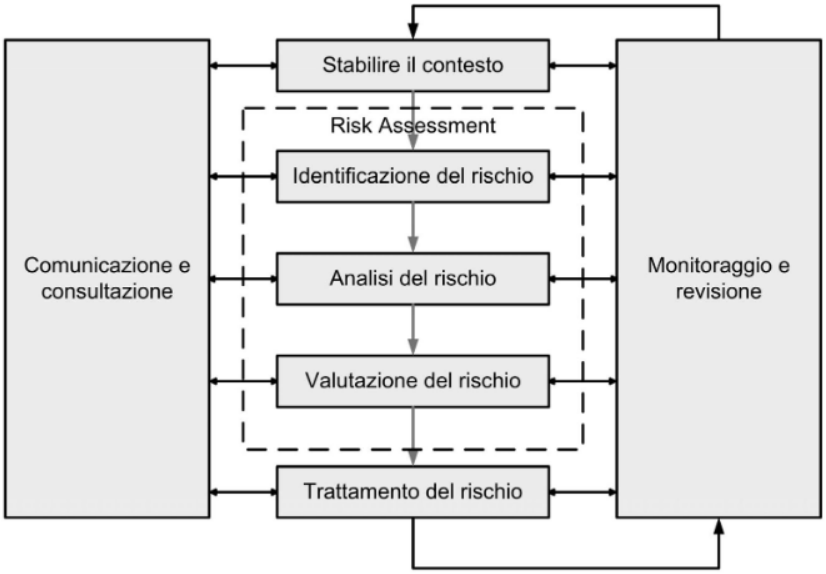

FIG. 5. Security Risk Management 2010, p. 39 – Processi di gestione del rischio.

3.3.1. Stabilire il contesto

L'analisi del contesto interno ed esterno serve all'organizzazione per definire i parametri interni ed esterni e i criteri di rischio da utilizzare. La medesima attività, sebbene in modo più generico, è stata svolta nella fase di progettazione del quadro di gestione del rischio. A differenza di ciò che si è detto prima, in questo contesto i parametri devono essere più dettagliati, poiché va valutata la loro relazione con lo specifico processo di gestione del rischio.

La valutazione del contesto esterno è necessaria per rispondere, quanto più possibile, alle aspettative degli *stakeholder*. Si basa sulla globalità dell'azienda, ma è specifica per rispondere a necessità legali e a quelle dei portatori di interesse[46]. Il contesto esterno è in continua

[45] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 38.
[46] Cfr. *Ivi*, p. 40.

evoluzione, perciò è possibile che in ogni momento possano nascere nuove tipologie di rischio[47]. Con il costante miglioramento delle nuove tecnologie è necessario che all'interno dell'azienda ci sia un'ottima conoscenza degli strumenti informatici, poiché solo in questo modo è possibile sapere a quali rischi l'impresa va incontro[48]. Infatti, «Proprio per la natura trasversale dell'IT […], l'azienda deve partire dal presupposto per cui, se vuole davvero proteggere i suoi dati informatici, deve avere una visione d'insieme dell'intero ambiente organizzativo e costruire una vera e propria mappa che le consente di capire in che modo l'IT è coinvolto nei vari processi […]»[49].

Il contesto interno, invece, è preso in considerazione per allineare i processi di gestione del rischio alla strategia e agli obiettivi aziendali. Si deve analizzare tutto ciò che può influenzare il modo in cui l'organizzazione gestisce i rischi[50].

In questa fase vanno definite le risorse che è possibile utilizzare, le responsabilità e i ruoli. È necessario circoscrivere gli scopi da raggiungere, l'ambito e la dimensione delle attività di gestione del rischio. Tenendo conto dei valori, degli obiettivi, dei requisiti legali e delle risorse disponibili in azienda, devono essere indicati anche i criteri di rischio, che servono a valutare l'importanza di un rischio basandosi sulla sua natura, sulle cause e sulle conseguenze. Le probabilità di accadimento e i livelli di rischio devono essere seguiti da una spiegazione delle modalità in cui essi vengono stabiliti[51].

3.3.2. *Risk Assessment*

Il *risk assessment* è quell'insieme di processi strutturati che, nel contesto della gestione del rischio, serve a determinare e a comprendere quali sono i possibili rischi, le probabilità che essi si verifichino, i motivi per cui essi nascono, quali possono essere le conseguenze, l'adeguatezza e l'efficacia delle misure già predisposte[52]. Il risultato di questa attività è un insieme di informazioni che possono essere utilizzate per prendere le future decisioni aziendali, per esempio in merito al trattamento e alla mitigazione dei rischi[53].

---

[47] Cfr. *Ivi*, p. 31.
[48] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 135.
[49] *Ibidem*.
[50] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 40.
[51] Cfr. *Ivi*, p. 41.
[52] Cfr. *Ivi*, p. 46.
[53] Cfr. *Ivi*, p. 41.

Il primo elemento che va analizzato è il patrimonio aziendale, che consiste in tutti i beni tangibili e intangibili e nelle informazioni che hanno un valore per l'impresa. Un elenco degli *asset* serve a determinare i limiti entro cui viene condotto il *risk assessment* e a stabilire quali contromisure possono essere utilizzate per difendersi dai rischi[54]. «Una contromisura può essere costituita da un'attività, una tecnica o una tecnologia in grado di ridurre le potenziali perdite a un *asset* aziendale, tenendo sempre presente che il costo […] non deve essere maggiore della possibile riduzione nella perdita aziendale […]»[55].

Gli altri elementi da valutare sono le minacce, cioè gli accadimenti che portano conseguenze non volute, e gli agenti di minaccia, cioè le entità che possono scatenare la minaccia[56].

Il *risk assessment* si compone di varie fasi: identificazione dei rischi, analisi e valutazione.

3.3.3. Identificare i rischi

Per identificare un rischio devono essere valutati vari elementi: le fonti di rischio, le minacce effettive, le aree e gli scenari in cui il rischio può verificarsi, la frequenza con cui ciò può accadere, le cause e le conseguenze, sia quelle dirette e più immediate da identificare, sia quelle che ne derivano indirettamente. In questa sede deve essere stilata una lista completa con tutti i rischi a cui l'organizzazione va incontro[57]. È una fase fondamentale, poiché se un rischio non viene indicato in questo momento, è più difficile che venga rilevato in futuro[58].

I rischi sono tanti e possono avere natura diversa, ma possono essere raggruppati in tre categorie. La prima è quella dei rischi prevedibili, cioè quelli interni e controllabili. La categoria successiva è quella dei rischi strategici, cioè quelli che in qualche modo sono necessari alla competitività esterna dell'azienda, poiché sono quelli che portano maggiore crescita. Infine, ci sono i rischi esterni, più difficilmente controllabili dall'organizzazione[59]. Nel caso in cui non sia ben chiaro quali possano essere le fonti o le cause di rischio, è necessario ipotizzarle, al fine di determinare quali possono essere le relative conseguenze[60].

---

[54] Cfr. *Ivi*, p. 51.
[55] *Ibidem*.
[56] Cfr. *Ibidem*.
[57] Cfr. *Ivi*, p. 41.
[58] Cfr. *Ibidem*.
[59] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 79.
[60] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 42.

Anche sotto il profilo della protezione dati devono essere individuati i possibili rischi *privacy*, che possono consistere in distruzione o perdita, anche in modo accidentale, dei dati presenti nei sistemi informatici, in mancanza di disponibilità o di integrità, nell'accesso ai dati da parte di terzi non autorizzati, in trattamenti dati non conformi alle finalità prestabilite nelle informative o nell'impossibilità di garantire i diritti dell'interessato[61].

Le tecniche e gli strumenti per identificare i rischi devono essere quelli più adatti all'impresa, cioè devono aderire agli obiettivi, alle attitudini e al rischio di quella specifica realtà[62]. Nonostante l'esistenza di formule e processi che guidano questa attività, può essere molto difficile considerare tutte le possibilità, a causa della continua evoluzione del contesto e dell'organizzazione stessa[63].

Una tecnica di individuazione dei rischi è quella di utilizzare le *checklist*, cioè "[…] Liste di quelli che sono stati i rischi, individuati o emersi, in passato nella storia dell'azienda e che aiutano nel non tralasciare proprio quei fattori che, sulla base dell'esperienza pregressa, si sono rivelati potenzialmente pericolosi"[64]. Le *checklist* sono molto utili, ma possono indurre a commettere degli errori, perché, se troppo rigide, possono essere un limite all'individuazione di nuovi rischi. Un modo saggio di utilizzarle è quello di servirsene dopo che è già avvenuta un'identificazione preliminare dei rischi. Esse richiedono di essere periodicamente modificate e aggiornate[65].

I rischi possono essere identificati anche grazie a questionari di valutazione dei rischi, creati in modo specifico e trasversale per una specifica realtà organica[66].

Possono, inoltre, essere individuati durante sessioni di *brainstorming* create appositamente per avere un confronto con persone diverse, le quali possono apportare il loro contributo dando idee, proposte e suggerimenti. Questo è d'aiuto per avere una visione più completa del contesto, per definire obiettivi più precisi e ottenere risultati più reali[67].

---

[61] Cfr. Fulvia EMEGIAN, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4], p. 57.
[62] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, pag.42.
[63] Cfr. *Ivi*, p. 33.
[64] Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 85.
[65] Cfr. *Ibidem*.
[66] Cfr. *Ivi*, p. 89.
[67] Cfr. *Ibidem*.

Uno strumento valido per identificare i rischi è la matrice SWOT, che, andando a identificare i punti di forza e di debolezza interni, le opportunità esterne e le minacce esterne, consente di avere una visione globale dell'impresa, di analizzare le zone di intersezione tra il contesto interno ed esterno e di identificare i rischi presenti in entrambi i fronti[68], per avere una migliore visione d'insieme.

3.3.4. Analisi dei rischi

Una volta individuati i rischi è possibile analizzarli, considerando le cause di rischio e le conseguenze, anche multiple, che essi possono comportare, con le rispettive probabilità di accadimento[69].

Nell'analisi delle conseguenze**,** immediate e secondarie, tangibili o intangibili, positive o negative, si va a valutare la natura e l'impatto dell'avverarsi di un evento di rischio[70]. Nel fare ciò si deve tenere conto delle misure di difesa già esistenti nell'organizzazione e della loro efficacia ed efficienza. Le conseguenze e le loro probabilità dipendono dal tipo di rischio, ma anche dalle informazioni che si hanno a disposizione. Per determinare le conseguenze, oltre ai dati disponibili e a quelli storici, si possono utilizzare anche dati sperimentali[71], tecniche predittive, simulazioni statistiche o il parere di esperti. Alla lista delle conseguenze associate a un rischio va aggiunta la descrizione che riporta le probabilità che esse si verifichino e le aree o funzioni aziendali in cui esse probabilmente si manifesteranno.

Sul piano dei sistemi informatici può essere molto semplice identificare le minacce a cui l'organizzazione va incontro, ma può essere più complesso stabilire con quale probabilità esse potrebbero verificarsi e le conseguenze che potrebbero provocare. Le conseguenze, infatti, possono essere molto diverse tra loro e anche il loro grado di severità può essere differente[72]. L'analisi del rischio informatico si basa su alcuni elementi: gli obiettivi della minaccia, la severità dell'attacco e la durata di quest'ultimo, le probabilità di essere esposti alla minaccia, la presenza di contromisure, il *trend* generale e i costi derivanti dall'impatto. L'analisi del rischio *cyber* è fondamentale per orientare gli investimenti dell'impresa e per prevenire il verificarsi di situazioni indesiderate. Tuttavia, gli attacchi informatici sono imprevedibili; essendo sempre

[68] Cfr. *Ivi*, p. 90.
[69] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 42.
[70] Cfr. *Ivi*, p. 56.
[71] Cfr. *Ivi,* p. 42.
[72] Cfr. *Ivi*, p. 31.

nuovi e di diverso tipo, possono verificarsi in modo inaspettato, perciò possono essere di difficile previsione[73].

L'analisi del rischio, in generale, può essere più o meno dettagliata, in base allo scopo, alle necessità aziendali, alle informazioni disponibili e ai rischi in questione e può essere di vario tipo: qualitativa, semi-quantitativa, quantitativa, o una combinazione di esse[74]. Facendo un'analisi qualitativa si vanno a definire dei livelli di rischio – alto, medio o basso –, in base alla probabilità che l'evento di rischio si verifichi e alle conseguenze, cioè ai danni, che esso porterà con sé. Nell'analisi quantitativa, invece, si vanno a stimare i rischi a cui l'impresa è esposta utilizzando valori numerici precisi, prestabiliti nella fase di studio del contesto, prima del *risk assessment*[75]. Un'analisi di questo tipo può essere complessa, poiché non sempre sono disponibili informazioni sufficienti. La soluzione è quella di svolgere un'analisi semi-quantitativa, che si avvale di scale di *rating* numeriche per combinare le conseguenze di un rischio e le probabilità, al fine di calcolare il livello di rischio[76].

L'analisi, che contribuisce alla creazione di un *Risk Register*[77], un documento che contiene la lista dei rischi presenti in ordine di priorità, consente all'impresa di prendere decisioni in modo più consapevole nelle fasi successive[78]. All'interno del registro è presente una raccolta numerata dei rischi, che ne garantisce l'identificabilità, con nome e una breve descrizione, ma anche l'indicazione della categoria a cui l'elemento di rischio appartiene, le conseguenze che si prevedono, le azioni predisposte per affrontarlo, il soggetto responsabile e lo status – rischio ancora presente o rischio superato –[79].

L'output di questo processo è un insieme di linee guida per l'impresa che traducono i risultati

---

[73] Cfr. Nicola CIANI, Ingrid SALVADORI, "Rischio Cyber: ecco come quantificarlo nelle aziende", in *Osservatori Digital Innovation del Politecnico di Milano* [sito web], 2024, ultimo aggiornamento luglio 2024, https://www.osservatori.net/cybersecurity-data-protection/insight-rischio-cyber-quantificazione/ (consultato il 26 ottobre 2024).
[74] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 42.
[75] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 109.
[76] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 55.
[77] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 95.
[78] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 42.
[79] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 96.

emersi. L'incertezza, che è stata analizzata con le modalità già esaminate, diventa un elemento importantissimo nello stabilire la strategia aziendale da seguire per rispondere ai rischi[80].

3.3.4.1. La matrice di rischio

La matrice di rischio serve a individuare e a gestire adeguatamente i rischi presenti in un certo ambiente. È una matrice che combina due elementi: le probabilità che un rischio si verifichi e l'impatto, cioè le sue conseguenze. Rappresenta graficamente gli elementi problematici, cioè i rischi potenziali, che devono essere prevenuti o trattati[81].

Grazie a questa matrice, basandoci sulle probabilità e le conseguenze, è possibile distinguere i rischi in quattro categorie: rischi critici, rischi principali, rischi moderati e rischi minori[82]. I rischi critici sono quelli prioritari, per i quali c'è la necessità di intervenire immediatamente con misure specifiche. Sono i primi nella lista delle priorità. Ci sono poi i rischi principali, che sono elevati, ma non estremi; perciò, devono essere presi in considerazione per secondi. Seguono i rischi moderati che, sebbene non siano gravi come i due precedenti, richiedono di essere mitigati o prevenuti, prima che riescano a salire di livello. Per ultimi ci sono i rischi minori, accettabili, ma che vanno comunque gestiti adeguatamente[83].

3.3.5. Valutazione dei rischi

Dopo aver analizzato i possibili rischi presenti in azienda, è finalmente possibile valutarli, per capire quali di essi dovranno essere trattati nella fase successiva e con quale priorità[84].

La valutazione consiste nel confrontare i livelli di rischio stimati nella fase di analisi del rischio con i criteri di rischio predeterminati durante la fase di studio del contesto[85]. Il risultato può essere chiaro, quando c'è una volontà certa di voler gestire il rischio, oppure possono essere necessarie ulteriori valutazioni per prendere una decisione definitiva[86].

I costi e i benefici di trattare un rischio e delle modalità con cui farlo vanno confrontati con i costi e i benefici di mantenere il rischio; è soprattutto in base a questi elementi che si prendono

---

[80] Cfr. *Ivi*, pp. 114-115.
[81] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 13.
[82] Cfr. *Ivi*, p. 14.
[83] Cfr. *Ibidem*.
[84] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, pp. 42-43.
[85] Cfr. *Ivi*, p. 43.
[86] Cfr. *Ibidem*.

le decisioni nelle fasi seguenti[87]. Se, infatti, i costi di mitigazione di un rischio sono superiori a quelli di risposta successiva alle conseguenze e non ci sono ulteriori benefici, non avrà senso mitigare il rischio. Se, al contrario, i costi di mitigazione sono inferiori alle spese per rispondere all'evento di rischio, per avere dei benefici è fondamentale trattare il rischio il prima possibile. Esistono, tuttavia, alcuni rischi che per l'impresa non sono assolutamente tollerabili, perciò devono essere trattati, qualunque ne sia il prezzo[88]. Al contrario, ci possono essere dei rischi talmente bassi o irrilevanti, che non vale la pena mitigarli[89]. Le decisioni di trattare o meno un rischio o quella di perseguire una certa opportunità possono essere influenzate anche da ulteriori elementi, quali le esigenze legali, etiche e finanziarie[90].

La valutazione dei rischi si basa su rischi previsti come possibili in una certa finestra di tempo; perciò, lo stato di valutazione deve essere costantemente aggiornato[91].

3.3.6. Risposta al rischio negativo

Con i rischi che possono portare conseguenze indesiderate, è possibile scegliere di perseguire diverse strade: evitarli, accettarli, mitigarli o trasferirli[92].

In primo luogo, attraverso lo strumento della prevenzione, si può evitare che le fonti di rischio diventino vere e proprie minacce. Ciò richiede di fare dei cambiamenti all'interno dell'organizzazione. Una possibilità per eliminare il rischio è quella di non perseguire o continuare delle attività troppo rischiose. Un'altra soluzione è quella di rimuovere le fonti di rischio. Più si conosce il contesto circostante in cui i rischi si potrebbero verificare, più è possibile che questo rimedio sia efficace[93].

In altri casi, invece, è possibile accettare i rischi in modo consapevole e informato. Per sopportare la possibilità che si concretizzino delle minacce, però, è necessario che sussistano delle condizioni ben precise: il rischio è poco probabile; in azienda ci sono gli strumenti e le competenze adatte per gestirne le conseguenze; i costi di trasferimento a terzi del rischio sono troppo alti[94]. Essendo, questa, una decisione che può avere un serio impatto sull'attività

[87] Cfr. *Ivi,* p. 57.
[88] Cfr. *Ibidem*.
[89] Cfr. *Ibidem*.
[90] Cfr. *Ivi*, p. 57.
[91] Cfr. *Ivi*, p. 31.
[92] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 117.
[93] Cfr. *Ibidem*.
[94] Cfr. *Ivi*, p. 118.

complessiva, la parola finale spetta ai vertici aziendali[95].

Nella maggior parte delle situazioni i rischi vengono mitigati. Si cerca, cioè, di ridurre, fino a raggiungere un livello accettabile per l'impresa, i rischi, le probabilità che essi si verifichino e le loro conseguenze. Per fare ciò è richiesta l'adozione di contromisure[96], procedure e controlli di sicurezza specifici, o il miglioramento di quelli esistenti, formazione del personale in materia di rischio e, in generale, prevenzione in tutti gli ambiti organizzativi[97]. Per ogni rischio, seguendo l'ordine di priorità, è necessario scegliere una specifica modalità di mitigazione, che si ritiene essere ideale in base ai costi e ai benefici e questa deve, poi, essere implementata[98]. Possono anche essere combinate modalità diverse, per avere risultati più completi. Il trattamento di un rischio non si svolge solo una tantum, ma è un processo ciclico di valutazione del trattamento, decisione in merito alla tollerabilità dei rischi residui, attuazione di nuovi trattamenti nel caso in cui quelli presenti siano insufficienti o inefficaci e, di nuovo, valutazione del trattamento[99]. Il trattamento di un rischio, infatti, può comportare la creazione di nuovi rischi, che richiedono a loro volta di essere valutati, trattati, monitorati e revisionati[100]. Tutto ciò deve essere svolto con la consapevolezza che il rischio zero non esiste; perciò, non si può raggiungere un livello di sicurezza totale.[101]

L'ultima possibilità è quella di trasferire il rischio a terzi[102], tramite contratti che definiscono i rischi, gli oneri, le condizioni e i limiti dell'accordo[103]. Sono sempre più diffuse, soprattutto a livello internazionale, coperture assicurative che vanno a tutelare le imprese dai danni conseguenti alla manifestazione di un rischio. Nel caso di rischi informatici esistono delle polizze *di cyber risk insurance* che assicurano l'impresa dai danni, anche non patrimoniali, dai

---

[95] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 44.
[96] "Una contromisura è una tecnica, un'attività, una tecnologia in grado di ridurre il rischio degli asset aziendali". Stefano BONACINA, *Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda*, Wolters Kluwer, Assago (MI) 2010, p. 58.
[97] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 118.
[98] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 43.
[99] Cfr. *Ibidem*.
[100] Cfr. *Ivi*, p. 44.
[101] Cfr. *Ivi*, p. 58.
[102] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 118.
[103] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 44.

danni reputazionali[104] e dalla perdita di dati personali, anche particolari, causati da minacce informatiche[105]. Adottare queste polizze non sostituisce l'adempimento agli obblighi del GDPR, ma è solo una soluzione complementare[106]. Solitamente il trasferimento del rischio viene realizzato per i rischi meno probabili e con una severità medio-bassa; creare delle coperture assicurative per rischi di severità alta, infatti, può essere molto costoso per l'impresa, anche se potrebbe essere un buon investimento[107]. In Italia questo strumento non è sfruttato molto dalle imprese, poiché le tematiche legate al rischio informatico e alle sue conseguenze sono sottovalutate; le polizze, in aggiunta, sono molto costose e ciò non è sostenibile, soprattutto per le imprese di piccole o medie dimensioni. Anche nel caso in cui l'impresa riuscisse a sottoscrivere una polizza di questo tipo, i limiti di copertura del danno possono essere fluidi, per esempio nel caso di minacce informatiche nuove che, non essendo conosciute al momento di sottoscrizione del contratto, non possono essere oggetto di assicurazione[108].

3.3.7. Risposta al rischio positivo

I rischi che, al contrario di quelli appena nominati, non sono visti dall'impresa come una minaccia, bensì come opportunità, possono essere sfruttati, condivisi, valorizzati e accettati[109].

Per un'impresa, sfruttare un rischio significa utilizzare l'opportunità che si è creata, al fine di crearne una risorsa. Per trarne un vantaggio è necessario condividere l'opportunità con team dedicati, aziende partner o con gli *stakeholder*, più in generale[110]. Un rischio può essere valorizzato, aumentando le probabilità che esso si concretizzi e che abbia effetti positivi nell'organizzazione. Anche in questo caso diventerà una vera e propria risorsa per l'impresa[111]. L'azienda può essere anche disposta ad accettare l'opportunità, qualora essa si verifichi, e a

[104] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 59.
[105] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 137.
[106] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 59.
[107] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 118.
[108] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 59.
[109] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 119.
[110] Cfr. *Ibidem*.
[111] Cfr. *Ibidem*.

coglierne gli aspetti positivi, pur senza avervi investito in modo consapevole[112].

3.3.8. Monitoraggio e revisione

«Il […] monitoraggio periodico del rischio e dell'implementazione di adeguate misure correttive forma le basi della gestione del rischio […][113]». Questo procedimento serve a verificare l'efficacia del processo di *risk assessment* in ogni sua componente. Se si vuole che i processi di gestione del rischio portino a risultati ottimali, è necessario migliorare l'attività di *risk assessment*, facendo una serie di controlli sull'efficacia ed efficienza dei processi.

In questa sede è possibile identificare nuove fonti di rischio, controllare i rischi già individuati per capire se servono ulteriori azioni correttive e concludere la gestione per i rischi non più presenti[114].

Un elemento che va sempre tenuto sotto controllo è il cambiamento del contesto, che segna il perimetro entro cui avviene la gestione del rischio. Una modifica degli elementi di contesto, infatti, può creare nuovi rischi e può riuscire, in alcuni casi, a estinguere alcuni di quelli già analizzati e valutati[115]. Ci possono essere anche altri fattori che, variando nel tempo, richiedono delle modifiche nella gestione del rischio. Essi devono essere individuati e utilizzati per rivedere il *risk assessment*[116].

Anche se non ci sono stati particolari cambiamenti all'interno o all'esterno dell'organizzazione, monitorare l'attività è sempre utile per controllare se ciò che si sta facendo sta portando a risultati positivi o comunque in linea con le previsioni, oppure se è necessario intervenire in altro modo[117].

In ogni caso, questa fase serve a diffondere maggiore consapevolezza e motivazione, poiché va a semplificare la complessità di un ambiente in continua evoluzione[118]. È di per sé anche un'attività di prevenzione, poiché, permettendo di intervenire immediatamente sui problemi e

---

[112] Cfr. *Ibidem*.
[113] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 31.
[114] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 121-122.
[115] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 45.
[116] Cfr. *Ivi*, p. 59.
[117] Cfr. Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 120.
[118] Cfr. *Ibidem*.

sulle vulnerabilità, contribuisce a prevenire i rischi.

3.3.9. Comunicazione e consultazione

«La comunicazione […] è una delle chiavi del successo di ogni iniziativa ma purtroppo la sua importanza viene spesso ignorata perché ritenuta patrimonio consolidato dei rapporti socio-organizzativi, anche nelle aziende»[119]. Essa va svolta sia all'interno, sia all'esterno dell'organizzazione e deve coinvolgere tutti gli *stakeholder*. All'interno essa serve a comunicare informazioni in merito alla gestione del rischio, relativamente al quadro e ai processi, ma anche a comunicarne i risultati[120]. All'esterno, invece, consente lo scambio di informazioni e il rispetto delle norme giuridiche e di *governance*[121].

La comunicazione deve essere presente durante tutta l'attività, poiché, oltre a creare un ambiente di fiducia reciproca, consente di affrontare il tema della gestione del rischio in maniera congiunta. Grazie a questo meccanismo è possibile, per tutti, partecipare all'analisi del contesto, far notare la presenza di rischi, stabilirne le cause e le conseguenze, definire i criteri di rischio, ma anche prendere parte alla decisione su quali siano le contromisure ideali al contesto organizzativo, tenendo in considerazione gli interessi degli *stakeholder*[122]. «La comunicazione e la consultazione devono facilitare uno scambio di informazioni sincero, pertinente, accurato e comprensibile, considerando anche gli aspetti di confidenzialità e di integrità personale»[123].

L'avere dei piani o delle strategie di comunicazione e consultazione ben definiti può essere molto utile anche in contesti emergenziali, durante i quali è necessario che tutti ripongano fiducia nei soggetti al vertice dell'impresa o in chi ne gestisce l'aspetto comunicativo[124].

4. L'importanza delle persone

Un'azienda «[…] È fatta dalle persone che ne fanno parte, quindi, dalle relazioni interpersonali che in essa si sviluppano»[125]. Investire nel fattore umano, significa investire nel futuro[126]. Le persone presenti nell'organizzazione hanno un ruolo fondamentale nel contesto

[119] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 37.
[120] Cfr. *Ibidem*.
[121] Cfr. *Ibidem*.
[122] Cfr. *Ivi*, pp. 38-39.
[123] *Ivi*, pp. 39-40.
[124] Cfr. *Ivi,* p. 37.
[125] Sara GIUSSANI, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024, p. 141.
[126] Cfr. *Ibidem*.

della gestione dal rischio. Da un lato, esse possono essere una risorsa; dall'altro, possono facilmente trasformarsi in una minaccia.

Possono essere una risorsa per l'impresa, non solo perché apportano il loro contributo dal punto di vista lavorativo, ma anche perché, in un contesto di gestione del rischio, collaborano nell'analisi del contesto aziendale, nella ricerca di potenziali rischi e nell'identificazione delle possibili conseguenze. Il loro ruolo è fondamentale, poiché consente di avere una visione complessiva della realtà organizzativa. Le persone possono essere considerate come una risorsa anche nel momento in cui contribuiscono attivamente al rispetto delle procedure e dei processi di gestione del rischio.

Il fattore umano, però, può essere anche un problema. Esso rappresenta, infatti, una delle maggiori cause di rischio[127] per la sicurezza dei dati e dei sistemi informatici. Non solo i dipendenti di un'impresa possono diventare volontariamente dei soggetti malevoli per l'organizzazione; ma, per motivi legati alla negligenza o alla disinformazione, essi possono rappresentare anche un punto debole nell'intero sistema. La minaccia legata al fattore umano può andare a compromettere l'integrità, la disponibilità o la confidenzialità dei dati e delle informazioni presenti nei sistemi informatici[128], perciò è necessario prevenirla e gestirla adeguatamente.

La minaccia interna è uno dei principali rischi che possono concretizzarsi nei confronti dei dati[129]. A riprova di ciò, come si è detto nell'analisi del rapporto Clusit, buona parte delle violazioni di dati avviene utilizzando tecniche di *Social Engineering,* facendo leva sull'elemento umano. Le persone costituiscono ancora l'anello debole dei sistemi di sicurezza informatica[130], poiché gli attaccanti sfruttano la strada che riscontra il minor livello di resistenza al fine di sottrarre e compromettere le credenziali degli utenti[131], che possono essere utilizzate per effettuare un attacco, consentendo di infiltrarsi nei sistemi interni dell'azienda[132].

I soggetti interni possono anche avere intenzioni malevole. Stiamo parlando della categoria

[127] Cfr. *Ivi*, p. 143.
[128] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 68.
[129] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 178.
[130] Cfr. *Ivi*, p. 207.
[131] Cfr. *Ivi*, p. 199.
[132] Cfr. *Ivi*, p. 304.

di minacce più complessa da individuare, dal punto di vista degli strumenti di rilevazione e di gestione del fenomeno[133]. Questi individui vengono definiti *insider*, cioè persone che, lavorando all'interno dell'impresa ed essendo a conoscenza di informazioni, *policy*, tecnologie e procedure relative alle misure di sicurezza, possono usarle impropriamente per scopi illeciti[134]. L'accesso privilegiato[135] a questo tipo di informazioni e l'ottima conoscenza dei sistemi aziendali possono essere utilizzate per danneggiare l'impresa. Scavalcando le misure di sicurezza dall'interno, sfruttando le vulnerabilità di cui sono a conoscenza, infatti, consente loro di neutralizzare l'effetto di *firewall* e dei sistemi di antintrusione[136], progettati in larga parte come barriera di difesa dagli attacchi provenienti dall'esterno. Per tutelarsi dagli *insider*, i vertici aziendali dovrebbero sviluppare una strategia di difesa a diversi livelli che comprenda politiche, procedure e controlli sotto il profilo tecnico-informatico[137], ma anche di *business*, più in generale. Nonostante le minacce interne siano una delle principali vulnerabilità per un'organizzazione, spesso, purtroppo, le aziende si concentrano sulla protezione da attacchi esterni, ignorando il problema[138].

La formazione continua e mirata di tutti i dipendenti, indipendentemente dal loro ruolo, aiuta a colmare il divario tra il rischio percepito, che si basa sulla sensazione di insicurezza, e quello reale, legato a dati oggettivi. Nel complesso, dovrebbe contribuire a diffondere una cultura della sicurezza aziendale[139]. Dovrebbe essere il più possibile coinvolgente; per esempio, potrebbe essere svolta attraverso l'analisi delle minacce più recenti, dimostrazioni pratiche o simulazioni[140]. La formazione sulla sicurezza informatica dovrebbe affrontare il tema della sicurezza delle identità e delle credenziali, ma anche quelli di utilizzo di strumenti per individuare codici maligni e di individuazione di comportamenti di disturbo da parte di altri soggetti interni. Scopo della formazione è anche quello di far conoscere gli strumenti, quali il *whistleblowing*, che consentono di comunicare in modo confidenziale la presenza di

[133] Cfr. *Ivi*, p. 301.
[134] Cfr. *Ivi*, p. 302.
[135] Cfr. *Ibidem*.
[136] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 67.
[137] Cfr. *Ivi*, p. 68.
[138] Cfr. *Ivi*, p. 69.
[139] Cfr. *Ivi*, p. 70.
[140] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 198.

comportamenti o di eventi sospetti[141].

Spesso la formazione non è sufficiente e occorre adottare alcune misure che consentono di ridurre, dal punto di vista informatico, le fonti di rischio. È il caso dell'utilizzo del privilegio minimo, che, limitando i privilegi di ogni utente, diminuisce le possibilità di rischio di compromissione dell'*account*[142]. Autorizzando le persone ad accedere solo alle risorse sufficienti per lo svolgimento delle loro mansioni[143], infatti, è possibile limitare la superficie di attacco, ridurre i danni e diminuire il rischio di perdita di integrità, disponibilità e riservatezza di informazioni e dati confidenziali, poiché si limita la possibilità del soggetto di accedere a funzioni consentite a un altro dipendente con ruolo diverso.

Nel caso di persone il cui rapporto lavorativo con l'impresa è terminato, infine, è necessario disabilitare le possibilità di accesso, sia fisico che telematico[144]. In caso contrario, l'organizzazione rimarrebbe vulnerabile ad accessi non autorizzati[145].

5. La protezione in rete

Proteggersi dai rischi presenti nella rete informatica è fondamentale per le imprese, soprattutto in un periodo storico in cui lo strumento telematico è implicato in tutti gli ambiti e i processi aziendali.

Le minacce informatiche, che possono compromettere i sistemi e i dati, rappresentano i rischi esterni a cui le imprese, oggigiorno, vanno incontro. Le conseguenze non sono solo danni materiali, quali la perdita di dati o la loro alterazione, ma anche danni immateriali, come la violazione di riservatezza dei dati o la distruzione della reputazione dell'organizzazione[146].

È necessario, quindi, ridurre la superficie di attacco, andando a eliminare le fonti di rischio o a trattare i rischi informatici residui. Oltre all'adozione del sistema del privilegio minimo,

---

[141] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 71.
[142] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 183.
[143] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, pp.71-72.
[144] Cfr. *Ivi*, p. 76.
[145] Cfr. *Ivi*, p. 80.
[146] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 301.

che, come si è detto, divide la rete in aree con diversa accessibilità per gli utenti, ci sono altri strumenti che possono essere utili alla salvaguardia della rete informatica aziendale.

Nonostante spesso lo sia dia per scontato, le *password* e le credenziali di accesso a sistemi o applicazioni devono essere gestite correttamente. Per prima cosa, esistono strategie e criteri per creare *password* efficaci e non scontate. Inoltre, sono presenti dei programmi che consentono di archiviare in modo sicuro tutte le *password* dell'utente[147]. Per evitare che le credenziali siano visibili a soggetti non autorizzati dovrebbe essere richiesto ai soggetti interni all'azienda di non lasciarle incustodite su schermi accesi o sulle scrivanie[148]. Per rendere all'utente più semplice la gestione degli account e l'accesso ad applicazioni o programmi, può essere usato lo strumento del *single-sign-on* (SSO), cioè «Un sistema di autenticazione centralizzata che consente a un utente di fornire le proprie credenziali una sola volta e di accedere a molteplici risorse e applicazioni all'interno di una rete locale o della rete Internet»[149].

Un'altra misura di sicurezza, molto spesso sottovalutata, è il *backup*. Esso dovrebbe essere svolto quotidianamente, meglio se in un ambiente *offline* o nel *cloud*, per evitare di perdere i dati nel caso in cui una minaccia diventasse reale[150]. Se i *backup* utilizzano sistemi di crittografia, inoltre, si rende ancora più difficile agli attaccanti accedere alle informazioni in questione[151]. L'accesso ai sistemi di *backup* dovrebbe essere consentito in base alla strategia del privilegio minimo, per evitare che, nel caso in cui un dispositivo dovesse essere violato, ci possano essere delle compromissioni anche nel sistema di *backup*[152].

L'infrastruttura informatica, per essere più sicura, richiede l'installazione di antivirus e *firewall*, che servono a controllare che le minacce di attacco che provengono dalla rete non riescano ad addentrarsi nel sistema di sicurezza. I *firewall*, in particolare, consentono di analizzare il traffico di rete e di distinguere le reti affidabili da quelle poco sicure; garantiscono un alto livello di protezione, ma non sono infallibili e nemmeno impenetrabili[153]. I *firewall*

[147] Cfr. *Ivi*, p. 178.
[148] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 128.
[149] Pietro LONGO, Single Sign On per applicazioni web. *Bollettino del CILEA* 106, 2007.
[150] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 182.
[151] Cfr. *Ibidem*.
[152] Cfr. *Ivi*, p. 181.
[153] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 96.

possono essere inefficaci in caso di attacchi che provengono dall'interno del perimetro di sicurezza, poiché non sono in grado di reagire ai codici maligni originali provenienti dall'interno e a programmi dannosi installati direttamente sui dispositivi[154]. Possono essere più efficaci, invece, sistemi che individuano le intrusioni, i quali monitorano il traffico di rete e i *log* al fine di individuare le attività sospette e, in caso di riscontro positivo su possibili intrusioni o utilizzi impropri del sistema o della rete, segnalano la violazione tramite un sistema di allarme[155]. Per essere efficace e limitare i danni, la risposta a queste segnalazioni deve essere rapida[156].

I *log* registrano le attività degli utenti e, più in generale, cosa è avvenuto nei sistemi o nelle reti. Fornendo informazioni di vario tipo, come l'autenticazione di un utente, le sue attività e gli attacchi alla rete[157], possono essere utili a ricostruire un evento accaduto all'interno del sistema informatico, come un incidente informatico o una violazione di sicurezza dei dati.

Un altro strumento che può salvaguardare la sicurezza in rete è la navigazione mediante filtri, nella quale agli utenti è consentito compiere solo certe azioni. I filtri possono consistere in restrizioni in base alle fasce orarie, ad esempio dopo l'orario di lavoro, ma anche in restrizioni basate su categorie di lavoratori. Tramite questi filtri è anche possibile limitare i siti visitabili, i programmi utilizzabili, esaminare il traffico di rete e applicare misure di sicurezza selettive, ad esempio nel caso di certi tipi di e-mail[158].

Utile strumento di protezione dei dati e delle informazioni critiche è anche l'autenticazione multifattore (MFA), la quale richiede più forme di verifica per confermare l'identità di un determinato utente che cerca di accedere a un programma o a un sistema[159]. Questa strategia può essere molto efficace nei confronti dei tentativi di *phishing*, poiché, anche se per errore l'utente fornisse la *password*, l'attaccante dovrebbe recuperare altre informazioni per potersi autenticare. Tuttavia, questa tecnica, se usata da sola, può fallire; perciò, è necessario utilizzarla

[154] Cfr. *Ivi*, p. 76.
[155] Cfr. *Ivi*, p. 96.
[156] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), p. 263.
[157] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 153.
[158] Cfr. *Ivi*, pp. 108-109.
[159] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 27 ottobre 2024), pp. 204-205.

all'interno di un sistema di sicurezza a più livelli.

Un approccio sempre più diffuso per proteggere i sistemi informatici è anche quello *zero trust*, che consiste nel non fidarsi mai e nel verificare sempre le informazioni. «In un contesto *Zero Trust*, ogni utente, dispositivo o sistema è trattato come potenzialmente non fidato, richiedendo autenticazione continua e rigorosi controlli di accesso»[160]. In questo modo è possibile garantire una sicurezza continua e dinamica, sia dalle minacce interne, che da quelle esterne.

Più recente è invece la diffusione dell'*Unified Threat Management* (UTM), un'evoluzione del *firewall* che può svolgere ulteriori funzioni: individuazione e prevenzione delle intrusioni, antivirus, anti-spam, VPN, filtro dei contenuti. Invece, quindi, di utilizzare più strumenti per garantire la sicurezza dei sistemi, questa applicazione li rende tutti gestibili da una singola interfaccia. È sicuramente meno costosa rispetto all'adozione di tutti i suoi componenti singoli; inoltre, è più semplice da utilizzare e aggiornare[161]. È l'ideale per le piccole-medie imprese che vogliono tutelarsi.

[160] Cfr. *Ivi*, p. 266.
[161] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 95.

CAPITOLO III – RESILIENZA: L'IMPORTANZA DELLA BUSINESS CONTINUITY PER LE AZIENDE

1. La continuità operativa: minimizzare l'impatto degli incidenti

Non sempre la gestione del rischio porta agli effetti desiderati. Può accadere, infatti, che sorgano nuove minacce inattese, che gli strumenti di mitigazione dei rischi non siano sufficienti o che si verifichino incidenti e disastri non prevedibili.

Gli imprenditori frequentemente sono convinti che, qualora si verificasse un evento inatteso di questo tipo, la loro organizzazione avrebbe tutti i mezzi e le risorse per rispondervi. Tuttavia, molto spesso, non è così, poiché la portata delle conseguenze viene sovente sottovaluta. A testimonianza di ciò, nel Rapporto Clusit[1], che, come si è detto, esamina lo stato della sicurezza informatica in Italia, è possibile riscontrare che, in alcuni ambiti, come quello delle violazioni di dati, «Il 40% [delle imprese coinvolte] ha dovuto affrontare spese non pianificate e circa 1 su 10 ha riportato altre gravi conseguenze, come la perdita del vantaggio competitivo, il calo delle vendite o l'abbandono dei clienti»[2]. Qualora non vengano prese delle precauzioni durante la situazione di normalità, le conseguenze di un evento inaspettato possono essere disastrose, andando dal rallentamento delle normali attività fino al fallimento dell'organizzazione[3].

Un altro dato che a livello internazionale ci permette di confermare la rilevanza del problema da un punto di vista più strettamente economico è che nel 2023, a seguito di una minaccia informatica, «Quasi un'organizzazione su 6 ha riportato danni finanziari pari ad almeno 50.000 dollari […]»[4].

Per sopravvivere a un evento dannoso inaspettato e non subire conseguenze troppo gravi, è necessario che le imprese siano resilienti. Per resilienza si intende «La capacità di un'organizzazione di anticipare, prepararsi, rispondere ed adattarsi al cambiamento

[1] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 30 ottobre 2024).
[2] *Ivi*, p. 176.
[3] Cfr. *Ibidem*.
[4] *Ivi*, p. 177.

incrementale e ad inconvenienti improvvisi, con l'obiettivo di sopravvivere e prosperare»[5]. Per essere resiliente, un'impresa deve integrare la gestione del rischio con la gestione delle emergenze, la *business continuity* e le attività di *recovery*.

Dal punto di vista cibernetico è possibile definire e analizzare il concetto più specifico di "cyber resilienza". Essa consiste nell'unione della resilienza con la cibersicurezza e la *business continuity* e consente alle imprese di poter proseguire il loro operato nonostante il manifestarsi di eventi cibernetici avversi e inaspettati[6].

Qualora le imprese vogliano evitare che eventi inattesi come quelli appena descritti provochino gravi ricadute sull'attività aziendale, possono adottare le Linee guida dello Standard 22301:2019[7], elaborato nel 2011 e aggiornato nel 2019, che si occupa di individuare le qualità necessarie per l'implementazione di un sistema di gestione della *business continuity*[8].

2. ISO 22301- Cosa prevede

Lo Standard 22301 è uno Standard internazionale che aiuta le imprese a riconoscere preventivamente gli eventi che potrebbero interrompere l'attività operativa e ad attuare misure adatte a dimostrare agli *stakeholder* che l'azienda possiede una struttura solida[9]. Queste misure includono la pianificazione, lo sviluppo, il controllo e il riesame del sistema di continuità aziendale[10].

La *business continuity*, nello specifico, vuole assicurare alle aziende la sopravvivenza a seguito di eventi indesiderati, più o meno frequenti e più o meno gravi, che colpiscono l'organizzazione. Ciò viene realizzato attraverso la neutralizzazione degli effetti conseguenti al concretizzarsi di un rischio, ma anche tramite la salvaguardia delle attività critiche dalle possibili conseguenze della minaccia – per assicurare la ripresa delle attività nel minor tempo

[5] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, pp. 50-51.
[6] Cfr. *Ivi*, p. 51.
[7] ISO/TC 292, "ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements", in *ISO* [sito web], 2019[2], ultima modifica nel 2024, https://www.iso.org/standard/75106.html (consultato il 30 ottobre 2024).
[8] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 12.
[9] Cfr. *Ibidem*.
[10] Cfr. *Ibidem*.

possibile[11] – e la creazione di opportunità per l'impresa, anche dal punto di vista competitivo[12]. Partendo dal presupposto che nel 2023 gli attacchi informatici della durata superiore a un giorno che hanno colpito le imprese sono duplicati, investire nella continuità aziendale crea sicuramente dei vantaggi nei confronti della concorrenza[13].

La *business continuity* è molto utile nel contesto informatico, poiché, qualora applicata attraverso misure e procedure ai sistemi e ai dispositivi digitali, consente di assicurare che queste risorse continuino a funzionare nonostante eventi inattesi[14].

La gestione della continuità operativa, come accade nel contesto della gestione del rischio, non è una funzione isolata che ha un inizio e una fine precisi, ma si inserisce ininterrottamente all'interno della *governance* aziendale, andando a contribuire al raggiungimento degli obiettivi aziendali[15].

Si deve fare in modo che le politiche, le procedure e gli strumenti che aiutano l'impresa a gestire l'interruzione dell'attività e la realizzazione della resilienza[16] entrino a far parte della cultura aziendale e dei suoi valori[17]. «Una gestione della continuità di successo si fonda sull'esperienza e le competenze presenti all'interno dell'azienda, su suoi obiettivi, processi e rischi»[18].

La continuità aziendale non è un processo di sola reazione all'evento dannoso, ma anche di prevenzione, poiché avviene prima che la minaccia si verifichi. I piani che preparano le imprese a gestire l'impatto della minaccia e ad affrontarla quando diventa reale vengono preparati in una fase che precede l'evento inatteso e devono, poi, essere applicati quando la minaccia si concretizza. Vengono, infatti, preparate le operazioni, gli strumenti e i processi che dovranno essere seguiti per ritornare a una situazione di normalità[19]. Tuttavia, obiettivo della resilienza

[11] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 181.
[12] Cfr. *Ibidem*.
[13] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 30 ottobre 2024), p. 64.
[14] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 51.
[15] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 181.
[16] Cfr. *Ibidem*.
[17] Cfr. *Ivi*, p. 185.
[18] *Ibidem*.
[19] Cfr. *Ivi*, p. 181.

non è solo quello di far riprendere l'azienda da un attacco, ma anche quello di garantire la continuità delle attività durante l'incidente[20].

Per poter gestire al meglio la continuità operativa è fondamentale che l'azienda abbia strumenti informativi e sistemi di *allert* che segnalano le minacce in grado di impattare sull'attività. Non sono solo gli strumenti tecnici ad essere necessari in questo contesto, ma anche la formazione del personale. È indispensabile che all'interno della realtà aziendale vengano create nuove abilità, competenze e conoscenze che consentano all'impresa di resistere all'evento di rischio[21].

Adottare questo Standard significa prefissare, prima che l'evento dannoso si concretizzi, obiettivi chiari, osservabili e misurabili, al fine di assicurare la continuità aziendale. È necessario stabilire uno o più soggetti responsabili della gestione dell'incidente, i mezzi tramite cui contattarli, le risorse da destinare a queste attività, i criteri per misurare e valutare i risultati[22] e la finestra temporale massima di interruzione delle attività che l'azienda può sopportare, cioè il periodo di tempo massimo che l'impresa ha per ritornare alla situazione ordinaria[23].

All'interno dello Standard vengono esaminati anche i modi di tenuta e di conservazione dei piani e dei documenti di *business continuity*. Gestire in modo attento la documentazione, infatti, permette alle imprese di ripristinare in poco tempo le normali attività[24].

Nel complesso, se si vuole che la gestione della situazione critica sia il più possibile efficiente, è necessario mantenere un ottimo livello della comunicazione proveniente dai vertici aziendali – che possiedono la *leadership* – e diretta verso dipendenti, clienti e autorità regolatorie[25].

---

[20] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 51.
[21] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 13.
[22] Cfr. *Ivi*, p. 15.
[23] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 181.
[24] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 15.
[25] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 30 ottobre 2024), p. 263.

2.1. Casi di obbligatorietà

Anche in questo caso ci troviamo di fronte a uno Standard e non a una norma con natura obbligatoria. Tuttavia, come nel caso del *risk management*, esistono alcune norme che, in vario modo, richiamano le linee guida contenute all'interno dello Standard.

La più importante è sicuramente la Direttiva NIS 2[26], la quale richiede alle imprese di saper gestire la continuità operativa per garantire il proseguimento delle attività, senza interruzioni significative, nel momento in cui si verifica un incidente[27]. L'art. 24 del Decreto attuativo richiede ai soggetti essenziali – grandi imprese, soggetti critici, fornitori di servizi di comunicazione elettronica, Pubbliche Amministrazioni, ecc. – e ai soggetti importanti[28] di adottare «[…] Misure tecniche, operative e organizzative adeguate e proporzionate […] per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi»[29]. Tra queste misure rientrano la gestione degli incidenti e la continuità operativa. I soggetti sopra elencati devono adottare delle *policy* per la sicurezza dei dati e delle informazioni, ma anche sistemi di valutazione dell'impatto di un potenziale attacco nei confronti dell'organizzazione e strumenti di analisi delle vulnerabilità[30]. In un contesto di continuità, inoltre, è necessario avere un piano specifico che indichi come reagire a un attacco e un piano di ripristino dei sistemi, al fine di minimizzare i tempi di interruzione dell'attività.

In precedenza, questi obblighi di continuità erano inseriti all'interno della Direttiva NIS[31] e dovevano essere soddisfatti, in modo simile, dagli operatori di servizi essenziali e dai fornitori di servizi digitali. Si richiedeva, anche in quel caso, di adottare misure per prevenire e minimizzare l'impatto degli incidenti ai sistemi informatici e di notificare al CSIRT gli incidenti rilevanti[32].

---

[26] Direttiva UE 2022/2555, attuata in Italia con il D.lgs. 4 settembre 2024, n. 138.
[27] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 4 novembre 2024), p. 162.
[28] Sono i soggetti di cui all'art. 3 del D.lgs. 138 del 2024 che non sono considerati essenziali ai sensi dei commi 1 e 2 del medesimo articolo.
[29] D.lgs. 138 del 2024, Art. 24, comma 1.
[30] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 4 novembre 2024), p. 251.
[31] Direttiva UE 2016/1148, attuata in Italia con il D.lgs. 18 maggio 2018, n. 65.
[32] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020, p. 30.

2.2. *Business Impact Analysis* e *Business Continuity Plan*

Per poter gestire la continuità operativa di un'organizzazione è necessario analizzare il contesto e lo stato delle attività. Si devono individuare, anche grazie all'analisi dei rischi e alla documentazione disponibile, i processi critici – cioè quei processi fondamentali per raggiungere gli obiettivi aziendali – e le loro relative attività, risorse, interdipendenze[33] e classifiche di priorità[34]. Queste ultime sono stilate sulla base dell'importanza del processo per il raggiungimento degli obiettivi aziendali[35]. La comunicazione interna tra i vertici aziendali e gli *stakeholder* è fondamentale per avere un quadro completo ed esaustivo della situazione.

Solo a questo punto è possibile esaminare l'impatto operativo e finanziario di un incidente sulle attività aziendali e le conseguenze di una sospensione o interruzione del *business*[36]. Per farlo si può utilizzare la *Business Impact Analysis* (BIA); essa, infatti, consente «[…] Di capire in che misura le varie funzioni aziendali si affidano a sistemi, applicazioni e dati per operare efficacemente»[37]. Questa analisi aiuta anche ad individuare le potenziali opportunità che possono nascere da un evento imprevisto[38].

È fondamentale, in questo contesto, stabilire la parentesi temporale massima di interruzione delle attività che l'impresa è in grado di sopportare. Per fissarla, è possibile fare dei tentativi con periodi di tempo differenti e capire quale si adatta di più alla situazione specifica[39].

Si devono, poi, definire, più nello specifico, l'RTO e l'RPO. Per **RPO** si intende *Recovery Point Objective*, cioè il momento precedente all'interruzione, a partire dal quale si devono ripristinare i dati[40]. L'**RTO**, o *Recovery Time Objective*, invece, indica la finestra temporale massima per cui, dopo l'evento inatteso, l'infrastruttura e i sistemi informatici possono essere indisponibili[41], quindi i tempi entro cui deve avvenire il ripristino dei servizi dopo

[33] C'è una relazione di interdipendenza quando un processo è l'*input* o l'*output* di un altro processo. Se il primo è considerato critico, anche il secondo dovrà essere gestito come tale.
[34] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 190.
[35] Cfr. *Ivi*, pp. 188-189.
[36] Cfr. *Ivi*, p. 188.
[37] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 4 novembre 2024), p. 162.
[38] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 191.
[39] Cfr. *Ibidem*.
[40] Cfr. *Ibidem*.
[41] Cfr. Beatrice PANATTONI, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters

l'interruzione. Qualora le tempistiche per ripristinare l'infrastruttura informatica siano superiori a quelle tollerabili dall'organizzazione, è necessario che l'impresa trovi delle alternative per continuare a fornire il servizio durante quel periodo di tempo[42]. È fondamentale per l'organizzazione anche essere in grado di riallocare le risorse disponibili per consentire la rapida ripresa delle attività[43].

Successivamente alla realizzazione della BIA è necessario valutare se i sistemi informatici presenti sono adatti a soddisfare i requisiti individuati nell'analisi[44]. La valutazione è svolta in termini di resilienza dell'infrastruttura, di capacità dell'organizzazione di recuperare dati e informazioni e di presenza di piani di *business continuity* e di *disaster recovery* appropriati.

Il piano di continuità aziendale, o *Business Continuity Plan*, consiste in una serie di procedure «[…] Basate su trattamenti di ripristino approvati e attività e risorse alternative ben identificate»[45] che l'impresa deve seguire dopo un incidente per riportare la continuità operativa a una soglia minima accettabile[46]. Per essere efficace, deve essere in grado di realizzare la resilienza, di fornire delle direttive su come assicurare la sopravvivenza dell'azienda davanti a un evento imprevisto e di permettere il recupero delle informazioni e dei sistemi nel minor tempo possibile[47].

Il piano di continuità operativa è diverso per ogni organizzazione, poiché dipende dal suo livello di complessità[48], deve essere coerente con gli obiettivi aziendali e stimolare la crescita del *business*. «[…]Per un'organizzazione di dimensioni ridotte può essere più congeniale implementare un unico documento che consideri solamente le funzioni più rilevanti o i principali processi di gestione, mentre per un'impresa di notevoli dimensioni […] può essere giustificato sviluppare una pluralità di piani, indicizzati per singoli *output*, per unità operative

Kluwer, Milano 2020, p. 52.

[42] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 191.

[43] Cfr. *Ivi*, p. 193.

[44] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 4 novembre 2024), p. 162.

[45] Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 197.

[46] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 20.

[47] Cfr. *Ivi*, p. 22.

[48] Cfr. *Ivi*, p. 20.

o per aree strategiche d'affari»[49]. Può accadere, nei casi di imprese di grandi dimensioni o di imprese che hanno una struttura complessa, che la gestione durante la fase dell'interruzione sia affidata a un *team*. È fondamentale, in questo caso, che la squadra abbia un piano che indichi come procedere e un elenco di contatti[50]. Le diverse aree aziendali, in contesti di grandi dimensioni, dovranno avere un loro piano di ripristino, correlato da una serie di soggetti responsabili, risorse disponibili, tempi di azione e obiettivi da raggiungere in ordine di priorità[51].

Solitamente il piano si compone di più fasi. Si inizia con la pianificazione e programmazione della strategia di *business continuity*, la quale deve tenere conto dei costi e dei benefici che ne deriveranno. La continuità operativa deve essere, poi, integrata nelle normali attività dell'organizzazione. È possibile, a questo punto, passare all'individuazione e valutazione delle minacce che possono interrompere l'attività operativa. C'è, poi, la fase di progettazione vera e propria, in cui devono essere scelte le strategie, le tattiche e le modalità per raggiungere gli obiettivi di continuità prefissati e per ripristinare le attività dopo che la fase di interruzione è terminata[52]. In questo contesto vanno pianificate le procedure da seguire per salvaguardare le risorse e i processi più critici. Si deve, poi, implementare il piano stabilendo strategie, obiettivi, responsabilità e risorse. Successivamente si devono sviluppare gli indirizzi direzionali e gestionali per l'organizzazione, sulla base delle *policy* stabilite. Per ultimo, se necessario, il piano va modificato; infine, convalidato[53].

È necessario stabilire concretamente dei criteri che abilitano l'attivazione del piano e prevedere degli strumenti in grado di stimare la durata e lo stato dell'interruzione. È anche utile conservare le registrazioni degli eventi accaduti, in modo da poter analizzare a posteriori come è stata gestita la situazione[54]. Solo in questo modo un'impresa è in grado di migliorarsi.

Affinché il piano di continuità sia considerato all'altezza, è necessario che esso sia facilmente accessibile agli *stakeholder*, che sia sintetico, efficiente, chiaro, semplice, integrato

---

[49] *Ibidem*.
[50] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 197.
[51] Cfr. *Ibidem*.
[52] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 21.
[53] Cfr. *Ibidem*.
[54] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 197.

con gli altri piani, flessibile e rispettoso delle misure di sicurezza[55].

Ogni volta che ci sono modifiche del contesto, delle infrastrutture, dei profili di rischio, dei processi o di altri elementi interni ed esterni all'organizzazione, il piano di continuità e la B*usiness Impact Analysis* devono essere rivalutati[56].

Anche se non avvengono cambiamenti particolari all'interno dell'organizzazione, affinché il piano di continuità sia efficace, è necessario revisionarlo e migliorarlo periodicamente; a questo proposito possono essere utili fasi di test ed esercitazioni[57], ma anche la conservazione di tutta la documentazione e la formazione del personale. Nel caso in cui un piano dovesse subire delle modifiche, è necessario svolgere nuovamente la *Business Impact Analysis* per controllare se gli effetti che ne derivano sono stati sufficientemente presi in considerazione.

Nel momento in cui cessa definitivamente l'interruzione dell'attività operativa, l'impresa ritorna a una situazione di normalità e l'utilizzo del piano di continuità può cessare[58].

Per concludere, se l'azienda che vuole adottare questo Standard tratta dati personali, l'*audit* in ambito *privacy* deve andare a verificare i contenuti e le procedure inserite nel piano di continuità, attraverso l'analisi dei documenti disponibili, per controllare che le normative in merito alla protezione dati siano state tenute in considerazione. È, inoltre, necessario accertarsi che i soggetti *privacy* – quali ad esempio il Titolare e il Responsabile del Trattamento – siano contemplati all'interno del piano e che altri soggetti come, ad esempio, gli Amministratori di Sistema siano autorizzati sulla base di solide procedure[59].

2.3. Gestione delle emergenze e *Disaster Recovery*

Nel contesto della *business continuity* vengono compiute altre due attività: la gestione delle emergenze e il *disaster recovery*. Questi concetti, pur essendo strettamente correlati, non sono sostitutivi l'uno dell'altro. Nelle aziende di grandi dimensioni, inoltre, queste attività potrebbero essere separate, mentre in quelle più piccole e strutturalmente più semplici è possibile che i ruoli coesistano.

La continuità aziendale, come già ampiamente detto, serve a evitare che un evento

[55] Cfr. *Ivi*, p. 198.
[56] Cfr. *Ivi*, p. 186.
[57] Cfr. *Ivi*, p. 199.
[58] Cfr. *Ibidem*.
[59] Cfr. Fulvia EMEGIAN, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4], pp. 383-384.

imprevisto possa interrompere per un periodo di tempo prolungato l'attività produttiva dell'organizzazione e arrecare un danno.

La gestione dell'emergenza, invece, è la fase che scatta immediatamente quando si viene a conoscenza del verificarsi dell'incidente. La situazione che si è creata deve essere gestita in modo tattico. Ci si deve occupare di gestire le persone, di raccogliere più informazioni possibili su quanto avvenuto, di capire se la situazione può ancora peggiorare, di stimare i danni materiali e immateriali e di segnalare l'incidente alle autorità[60]. Fondamentale, anche in questo caso, è la comunicazione con gli *stakeholder*. Le procedure di emergenza devono essere predisposte da coloro che sono soggetti alla Direttiva NIS 2; esse «[…] Devono essere documentate in modo accurato, testate regolarmente e includere un chiaro percorso di *escalation* per il processo decisionale»[61]. Possono essere create, specialmente nelle realtà imprenditoriali di grandi dimensioni, vere e proprie squadre di risposta alla crisi, composte da soggetti esperti di incidenti informatici[62]. Queste squadre devono andare a valutare l'entità dell'incidente informatico e procedere a trattarlo, per neutralizzarne gli effetti. All'interno del *team* è necessario definire un soggetto *leader* e un suo sostituto. Le mansioni e i diversi gradi di responsabilità dei soggetti interni al *team* devono essere documentati. I membri possono essere scelti sulla base della loro posizione nella gerarchia organizzativa o in base alle loro caratteristiche personali e professionali[63].

Il *disaster recovery*, infine, indica l'insieme di procedure operative che devono essere seguite per ripristinare i dati, i sistemi e le reti informatiche dopo che l'evento si è verificato[64] e riportarli ad uno stato di normalità. Anche in questo caso è necessario fissare una strategia da seguire per recuperare le risorse e stabilire il personale che si occuperà di queste attività[65]. Al fine di misurare l'efficacia e l'efficienza dei meccanismi di *disaster recovery* devono essere rispettati il *Recovery Point Objective* e il *Recovery Time Objective* fissati in precedenza.

Sulla base della Direttiva NIS 2, per rispondere agli incidenti nel minor tempo possibile e

---

[60] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 184.
[61] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 4 novembre 2024), p. 252.
[62] Cfr. *Ibidem*.
[63] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 196.
[64] Cfr. *Ivi*, p. 183.
[65] Cfr. *Ibidem*.

proteggere le risorse, le imprese devono predisporre dei sistemi di *backup*. Il *backup* è uno strumento utile per realizzare la resilienza da un punto di vista informatico, poiché garantisce tempi inferiori e procedure automatizzate per il recupero dei dati e dei sistemi necessari a continuare l'attività. Se non venisse adoperato, le imprese impiegherebbero moltissimo tempo a riacquisire tutte le informazioni necessarie alla normale operatività. I *backup*, per essere utili, dovrebbero essere svolti e testati frequentemente, dovrebbero garantire la sicurezza dei dati trattati, essere gestiti con accessi basati suoi ruoli e funzionare attraverso la creazione di copie multiple sotto la responsabilità di soggetti differenti[66].

Oltre agli strumenti di *backup* può essere utile archiviare la documentazione necessaria, come i piani di continuità e altri materiali importanti, in supporti fisici sicuri, quali le chiavette USB protette, che ne consentono una facile accessibilità, pur garantendo un buon livello di sicurezza[67].

Le procedure che permettono all'impresa di ripartire dopo un evento inatteso possono essere molto costose, ma l'investimento risulta essere direttamente proporzionale alla velocità con cui le attività vengono ripristinate. Più si investe nella fase di *recovery*, più l'impresa ha la sicurezza di ritornare alla normale operatività in tempi brevi.

2.3.1. Disaster Recovery Plan

Il *Disaster Recovery Plan* è una componente essenziale del piano di continuità aziendale e contiene «[…] Procedure, risorse ed infrastrutture volte a garantire il ripristino dei dati dell'Organizzazione o dei processi informatici in caso di calamità»[68]. Esso consente di ridurre i tempi e i costi di ripristino dell'attività operativa e dei processi critici. All'interno del piano devono essere definite le fasi da seguire per ripristinare dati e sistemi. Per semplificare questo lavoro possono essere molto utili degli strumenti che consentono di analizzare le criticità, di controllare l'integrità dei dati e delle informazioni e di verificare e circoscrivere la compromissione delle infrastrutture[69].

Gli *asset* aziendali, in questo contesto, vengono classificati in critici, vitali, delicati o non

[66] Cfr. *Ivi*, p. 82.
[67] Cfr. *Ivi*, p. 196.
[68] Fulvia EMEGIAN, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4], pag.382.
[69] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 6 novembre 2024), p. 182.

critici[70] in base alla loro rilevanza per l'impresa, cioè al ruolo che essi svolgono per l'organizzazione. Gli *asset* critici sono quelli che non possono essere sostituiti in altro modo e una loro indisponibilità, anche breve, può avere effetti gravi sull'organizzazione[71]; è necessario, perciò, gestirli per primi. Quelli non critici, al contrario, anche se risultano indisponibili per un certo periodo di tempo, non hanno un grave impatto sull'organizzazione[72], perciò possono essere ripristinati per ultimi. Sulla base di questa categorizzazione si stabilisce l'ordine di priorità con cui essi devono essere recuperati.

Un'altra distinzione deve essere fatta relativamente ai dati trattati dall'azienda attraverso gli strumenti informatici. Chi si occupa dell'*audit privacy* deve controllare se i dati sono stati classificati in modo corretto, per esempio distinguendo i dati personali "normali" da quelli particolari, oppure da quelli biometrici, se la loro conservazione e il loro trattamento sono congrui e se essi vengono adeguatamente considerati e salvaguardati all'interno delle procedure di ripristino contenute nel piano[73].

Affinché un *Disaster recovery plan* funzioni in modo efficiente, è fondamentale svolgere periodicamente dei test e delle simulazioni. Solo in questo modo il personale sarà in grado di reagire in modo tempestivo e adeguato qualora si verificasse l'incidente[74].

2.4. *Cyber Insurance*

Così come si è detto per la gestione del rischio, anche nel contesto di continuità aziendale, qualora si preveda l'impossibilità o la difficoltà per l'organizzazione di ripristinare i sistemi in tempi brevi, è possibile esternalizzare una parte delle conseguenze economiche a un ente assicurativo. Non esistono polizze assicurative in grado di garantire un ripristino dei dati o dei sistemi aziendali, ma, sottoscrivendo un'assicurazione ordinaria, è possibile che il risarcimento del danno derivante dall'incidente riesca a coprire buona parte dei danni economici o a

[70] Cfr. Fulvia EMEGIAN, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4], p. 383.
[71] Cfr. Agostino CORTESI et alt., "Validazione di Piani di Disaster Recovery mediante Simulatore", in *Emergency Sim: Realtà Virtuale, Serious Games e Simulazione per la Gestione delle Emergenze e dei Disastri*, Venezia 2009, p. 1.
[72] Cfr. *Ibidem*.
[73] Cfr. Fulvia EMEGIAN, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4], p. 383.
[74] Cfr. Agostino CORTESI et alt., "Validazione di Piani di Disaster Recovery mediante Simulatore", in *Emergency Sim: Realtà Virtuale, Serious Games e Simulazione per la Gestione delle Emergenze e dei Disastri*, Venezia 2009, p. 1.

prevenire addirittura il fallimento dell'organizzazione[75].

Questa è una strategia molto popolare a livello internazionale, poiché il 44% delle imprese ha un'assicurazione di questo tipo e un ulteriore 15% ha dichiarato che vorrebbe sottoscriverla entro un anno[76]. A livello nazionale, invece, ci sono ancora molte perplessità sull'efficacia dello strumento. Esso, infatti, risulta essere scarsamente utilizzato e molto sottovalutato.

2.5. Costi e benefici

Utilizzare un sistema di continuità aziendale può implicare numerosi vantaggi, anche dal punto di vista competitivo, per l'impresa, ma può comportare altrettanti costi.

Uno degli aspetti positivi derivanti dall'adozione dello Standard 22301 è certamente la limitazione degli effetti negativi che potrebbero essere causati dall'interruzione dell'operatività dell'impresa[77]. Oltre a ciò, l'impresa può garantire ai clienti l'offerta di servizi in ogni momento, senza necessità di sospenderla a seguito di incidenti, realizzando, così, l'obiettivo della resilienza[78]. Si rende possibile, inoltre, individuare preventivamente le conseguenze di un'interruzione e predisporre mezzi adeguati a ridurne i danni economici[79]. Grazie alla continuità operativa la ripresa della normale operatività può essere velocizzata[80].

Considerando, inoltre, che i costi di una violazione di dati o di un attacco ai sistemi informatici possono essere molto elevati, in molti casi l'adozione di misure preventive può limitare la portata delle passività che andrebbero ad impattare all'interno dei bilanci aziendali. Nel caso più estremo, l'utilizzo di questi Standard potrebbe riuscire a garantire la sopravvivenza dell'impresa e ad evitarne il fallimento.

Alcuni esempi di costi associati ad eventi di rischio a cui le imprese potrebbero andare incontro sono illustrati nella Tabella che segue:

---

[75] Cfr. Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 6 novembre 2024), p. 188.
[76] Cfr. *Ibidem*.
[77] Cfr. Stefano BONACINA, Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010, p. 182.
[78] Cfr. *Ibidem*.
[79] Cfr. *Ibidem*.
[80] Cfr. *Ibidem*.

EVENTO DI RISCHIO[81]	PROBABILITÀ	COSTO INDICATIVO
Interruzione delle attività	Alta	Dipende dalle dimensioni aziendali e dal tipo di attività
Data Breach	Alta	4,88 milioni di Dollari[82] (in Italia 3,55 milioni di Euro)
Attacco alle infrastrutture critiche	Alta	5,04 milioni di Dollari[83] (circa 4,75 milioni di Euro)
Attacco informatico es. malware o ransomware	Alta	5,24 milioni di dollari[84] (circa 4,94 milioni di Euro)
Attacco con *insider*	Alta	4,99 milioni di Dollari[85] (circa 4,70 milioni di Euro)
Violazioni in più ambienti	Medio-Alta	4,75 milioni di dollari[86] (circa 4,47 milioni di Euro)
Attacchi informatici distruttivi (scopo generale di arrecare un danno)	Medio-Alta	5,13 milioni di dollari[87] (circa 4,83 milioni di Euro)
Perdita della reputazione	Media	Dipende da molti fattori (dimensione azienda, quantità e tipo di *stakeholder*…)

TABELLA 1. Costi derivanti dal verificarsi di alcuni eventi di rischio.

In base al Report di IBM, che analizza i costi derivanti da una violazione di dati, è possibile affermare che le aziende che decidono di adottare misure di prevenzione – anche sfruttando l'Intelligenza Artificiale – sono in grado di ridurre di 2.2 milioni di Dollari i costi derivanti da

[81] Dati di ALLIANZ TRADE "Barometro Allianz: i principali rischi aziendali per il 2024", in *Allianz Trade* [sito web], 2024, ultimo aggiornamento 16 gennaio 2024, https://www.allianz-trade.com/it_IT/news-e-approfondimenti/studi-economici/pubblicazioni-economiche/barometro-rischi.html (consultato il 12 novembre 2024).
[82] Dati di IBM "Report Cost of a Data Breach 2024", in *IBM* [sito web], Segrate (MI) 2024, https://www.ibm.com/reports/data-breach (consultato il 12 novembre 2024).
[83] Cfr. Federica Maria Rita LIVELLI, "Ma quanto ci costano i data breach? Facciamo un po' di conti", in *Cybersecurity 360* [sito web], 2024, https://www.cybersecurity360.it/outlook/ma-quanto-ci-costano-i-data-breach-facciamo-un-po-di-conti/ (consultato il 12 novembre 2024).
[84] Il pagamento del riscatto a seguito di un attacco ransomware, tuttavia, non assicura la risoluzione del problema. Pagare per riottenere la disponibilità dai dati, inoltre, finanzia l'economia degli illeciti informatici: ogni riscatto pagato si stima possa finanziare altri nove attacchi della stessa tipologia. Cfr. Federica Maria Rita LIVELLI, "Ma quanto ci costano i data breach? Facciamo un po' di conti", in *Cybersecurity 360* [sito web], 2024, https://www.cybersecurity360.it/outlook/ma-quanto-ci-costano-i-data-breach-facciamo-un-po-di-conti/ (consultato il 12 novembre 2024).
[85] Dati di IBM "Report Cost of a Data Breach 2024", in *IBM* [sito web], Segrate (MI) 2024, https://www.ibm.com/reports/data-breach (consultato il 12 novembre 2024).
[86] Cfr. Federica Maria Rita LIVELLI, "Ma quanto ci costano i data breach? Facciamo un po' di conti", in *Cybersecurity 360* [sito web], 2024, https://www.cybersecurity360.it/outlook/ma-quanto-ci-costano-i-data-breach-facciamo-un-po-di-conti/ (consultato il 12 novembre 2024).
[87] Cfr. *Ibidem*.

un evento di questa portata[88]; costi che sono particolarmente aumentati in riferimento al settore industriale. L'incremento rispetto al 2023 è stato circa gli 830.000 Dollari per ogni singola violazione. Si conferma, quindi, la necessità di predisporre misure adeguate che garantiscano alle organizzazioni una reazione rapida nel caso in cui avvenga un incidente, in modo da limitare i danni causati da un *data breach*[89].

Lo stesso Report fornisce un altro dato importante: i costi di una violazione sono aumentati del 75% rispetto all'anno precedente non solo a causa del protrarsi del periodo di inattività conseguente a un attacco, ma anche a causa della perdita dei clienti e dei loro ordini[90].

Adottare le linee guida di questo Standard, infine, può servire a migliorare l'immagine aziendale nei confronti degli *stakeholder* e può aiutare le imprese ad essere maggiormente credibili[91].

Queste attività di prevenzione, d'altro canto, comportano dei costi non indifferenti e direttamente proporzionali alla velocità di ripresa del *business* e dell'infrastruttura informatica[92].

Un costo importante, innanzitutto, è collegato alla formazione del personale; questa è, tuttavia, un'attività fondamentale per far comprendere i concetti di continuità a coloro che lavorano con o per l'impresa[93]. Se l'impresa vuole evitare che i lavoratori si ritrovino impreparati nel momento in cui è necessario reagire all'evento avverso, è necessario che venga diffusa una buona consapevolezza della materia. Il personale, in particolare, deve essere istruito adeguatamente sulle mansioni e responsabilità attribuite nel contesto della *business continuity.*

Altri costi, poi, sono legati al rafforzamento dell'infrastruttura informatica e alla sua messa in sicurezza, alla predisposizione di processi e attività alternativi per garantire i servizi anche durante l'evento imprevisto e all'implementazione di metodi comunicativi più efficaci.

---

[88] Cfr. IBM "Report Cost of a Data Breach 2024", in *IBM* [sito web], Segrate (MI) 2024, https://www.ibm.com/reports/data-breach (consultato il 12 novembre 2024).
[89] Cfr. *Ibidem*.
[90] Cfr. *Ibidem*.
[91] Cfr. Stefano BONACINA, *Security Risk Management. Progettare e implementare un'efficace sicurezza delle informazioni in azienda*, Wolters Kluwer, Assago (MI) 2010, p. 182.
[92] Cfr. *Ibidem*.
[93] Cfr. *Ivi*, p. 187.

La *business continuity* nel suo complesso è costosa. Per le imprese, molto spesso, è considerata una spesa inutile e una perdita di tempo e di risorse[94].

Al di fuori, quindi, degli obblighi legali che impongono ad alcune categorie di imprese di seguire queste linee guida, è difficile che altre aziende siano propense ad aderirvi volontariamente. Tuttavia, questa potrebbe essere una scelta strategica molto proficua.

[94] Cfr. Pierluigi RAUSEI, Marco BARBIZZI, Management, *Business continuity, going concern. Fare crescere l'impresa oltre la crisi*, Wolters Kluwer, Milano 2020, p. 9.

CONCLUSIONE

Le riflessioni svolte all'interno di questo elaborato hanno permesso di illustrare due importanti strumenti di prevenzione, lo Standard 31000:2018 relativo al *risk management* e lo Standard 22301:2019 riguardante la *business continuity*, entrambi essenziali per quelle aziende che vogliono evitare che un attacco informatico possa arrecare danni gravi ai dati e ai sistemi aziendali.

A confermare l'importanza dell'argomento sono i dati analizzati sullo stato della sicurezza informatica nel nostro Paese[95], i quali non appaiono rassicuranti. Gli attacchi informatici nei confronti delle imprese italiane, come si è visto nel Capitolo I, risultano essere sempre più insistenti e sono favoriti, in modo particolare, dalla scarsa prevenzione che contraddistingue la nostra cultura.

Per questo motivo, c'è la forte necessità di formare gli imprenditori sugli strumenti a loro disposizione per gestire i rischi aziendali e per garantire la continuità dell'attività operativa anche nel caso in cui si verificasse un incidente.

Sarebbe ideale riuscire a persuadere le imprese ad adottare su base volontaria gli Standard illustrati, poiché è solo grazie a questi strumenti che le organizzazioni possono proteggere sé stesse, i dati – anche personali – trattati e gli *stakeholder* che su quella determinata organizzazione hanno riposto la loro fiducia.

I costi di implementazione di queste strategie e di questi processi, come si è visto, possono essere talvolta molto elevati e ciò non è d'aiuto nel convincere i vertici aziendali a perseguire questa scelta. La decisione, però, dovrebbe essere presa confrontando le spese da sostenere con i benefici e i vantaggi, economici e reputazionali, che ne potrebbero derivare. Tuttavia, è molto più probabile che siano le grandi imprese ad adottare tali strumenti. Le piccole imprese, infatti, potrebbero non avere le risorse economiche necessarie.

Sulla base di queste considerazioni, sarebbe ottimale prevedere a livello pubblico delle agevolazioni o degli incentivi che ne favoriscano l'utilizzo. Assicurare che un'impresa si protegga adeguatamente da possibili attacchi informatici, infatti, è vantaggioso per tutta la rete

[95] Claude BAZZUCCHI et alt., "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia", in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/ (consultato il 13 novembre 2024).

di coloro che con quell'organizzazione si interfacciano quotidianamente.

Solo favorendo una cultura della prevenzione di questo tipo sarebbe possibile raggiungere l'alto livello di cibersicurezza all'interno dell'Unione tanto auspicato dalla Direttiva NIS 2[96] recentemente entrata in vigore.

[96] Direttiva UE 2022/2555, attuata in Italia con il D.lgs. 4 settembre 2024, n. 138.

BIBLIOGRAFIA

Tutti gli URL presenti di seguito sono aggiornati al 12 novembre 2024.

ADRIAN David et alt., “An Update on the Lock Icon”, in *Chromium Blog* [sito web], 2023, ultimo aggiornamento 2 maggio 2023, https://blog.chromium.org/2023/05/an-update-on-lock-icon.html.

ALLIANZ TRADE, “Barometro Allianz: i principali rischi aziendali per il 2024”, in *Allianz Trade* [sito web], 2024, ultimo aggiornamento 16 gennaio 2024, https://www.allianz-trade.com/it_IT/news-e-approfondimenti/studi-economici/pubblicazioni-economiche/barometro-rischi.html

BAZZUCCHI Claude et alt., “Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia”, in *Clusit – Associazione Italiana per la Sicurezza Informatica* [sito web], Milano 2024, 376 pagine [PDF], https://clusit.it/rapporto-clusit/.

BONACINA Stefano, Security Risk Management. Progettare e implementare un’efficace sicurezza delle informazioni in azienda, Wolters Kluwer, Assago (MI) 2010.

CADOPPI Alberto et alt., *Cybercrime*, UTET Giuridica, Milano 2019.

CASTELLS Manuel, *Galassia internet,* Feltrinelli, Milano 2006 [Traduzione di Stefano VIVIANI].

CIANI Nicola, SALVADORI Ingrid, “Rischio Cyber: ecco come quantificarlo nelle aziende”, in *Osservatori Digital Innovation del Politecnico di Milano* [sito web], 2024, ultimo aggiornamento luglio 2024, https://www.osservatori.net/cybersecurity-data-protection/insight-rischio-cyber-quantificazione/.

CORTESI Agostino et alt., "Validazione di Piani di Disaster Recovery mediante Simulatore", in *Emergency Sim: Realtà Virtuale, Serious Games e Simulazione per la Gestione delle Emergenze e dei Disastri*, Venezia 2009.

Direttiva UE 2016/1148, “NIS 1”, attuata in Italia con il D.lgs. 18 maggio 2018, n. 65.

Direttiva UE 2022/2555, “NIS 2”, attuata in Italia con il D.lgs. 4 settembre 2024, n. 138.

EMEGIAN Fulvia, Monica PEREGO, *Privacy & Audit*, Wolters Kluwer, Milano 2019[4].

FARCI Manolo et al., “Media digitali e tecnoculture maschili”, in *Media digitali, genere e sessualità*, Mondadori Education, 2022.

GIUSSANI Sara, *Risk Management. Massimo rendimento a rischio ridotto*, Wolters Kluwer, Milano 2024.

IBM “Report Cost of a Data Breach 2024”, in *IBM* [sito web], Segrate (MI) 2024, https://www.ibm.com/reports/data-breach.

ISO/TC 262, “ISO 31000:2018 Risk management - Guidelines”, in *ISO* [sito web], 2018[2], ultimo aggiornamento nel 2023, https://www.iso.org/standard/65694.html.

ISO/TC 292, “ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements”, in *ISO* [sito web], 2019[2], ultima modifica nel 2024, https://www.iso.org/standard/75106.html.

LIVELLI Federica Maria Rita, “Ma quanto ci costano i data breach? Facciamo un po’ di conti”, in *Cybersecurity 360* [sito web], 2024, https://www.cybersecurity360.it/outlook/ma-quanto-ci-costano-i-data-breach-facciamo-un-po-di-conti/.

LONGO Pietro, Single Sign On per applicazioni web. *Bollettino del CILEA* 106, 2007.

LUCCHINI Alessandro, *Intranet - Teoria e pratica*. Apogeo Editore, Milano 2004.

MEZZALAMA Marco et alt., “Anatomia del malware” in *Mondo Digitale*, AICA, 2013.

PANATTONI Beatrice, *Compliance, Cybersecurity e sicurezza dei dati personali*, Wolters Kluwer, Milano 2020.

RAUSEI Pierluigi, BARBIZZI Marco, Management, *Business continuity, going concern. Fare crescere l’impresa oltre la crisi*, Wolters Kluwer, Milano 2020.

Regolamento (UE) 2016/679

STANZIONE Pasquale et alt., “Relazione annuale 2023”, in *Garante Privacy* [sito web], Roma 2024, 279 pagine [PDF], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10032003.