Introduzione al Risk Management (Gestione del Rischio)

La Gestione del Rischio, più comunemente chiamata Risk Management, è un processo strategico che permette alle aziende od organizzazioni di identificare, valutare e trovare modi per limitare i potenziali rischi che potrebbero compromettere le normali operazioni dell'azienda, il raggiungimento di obiettivi, nonché creare danno (d'immagine, monetario, …) alla stessa. Il Risk Management è quindi un processo fondamentale per assicurarsi della robustezza dell'azienda e per poter minimizzare potenziali perdite causate da eventi imprevisti o sfavorevoli. Il Risk Management, essendo un processo strategico, ben organizzato e strutturato, si divide in diverse fasi chiave, ovvero:

1. **Identificazione dei Rischi:** In questa prima, importante e fondamentale fase, l'ente/azienda/organizzazione procede con l'identificare tutti i possibili e potenziali rischi che potrebbero impattare negativamente sulla sua operatività. Questi rischi possono essere di vario tipo, come ad esempio rischi operativi, finanziari, di sicurezza (sia fisica che digitale), legali, ambientali e anche rischi alla reputazione stessa.
2. **Valutazione dei Rischi:** Una volta completata la prima fase ed aver identificato tutti (o quasi, visto la difficoltà del compito) i rischi, è ora necessario valutare sia la probabilità che un determinato rischio abbia luogo, sia quale sarebbe il potenziale impatto per l'azienda. Questo importante processo permette quindi di dare una priorità ai rischi in base alla loro potenziale gravità e alla possibilità che gli stessi si verifichino. In questa fase si usano strumenti che possono includere analisi sia qualitative che quantitative, come ad esempio le matrici di rischio e i modelli di simulazione.
3. **Mitigazione dei Rischi:** Dopo aver effettuato la valutazione dei rischi, l'azienda crea ed implementa delle misure per poter mitigare e ridurre sia la probabilità che un rischio si verifichi (probabilità di accadimento), sia l'impatto che il rischio comporta, o per lo meno uno dei due aspetti, usando la priorità dei rischi calcolata nella fase precedente. Le strategie di mitigazione sono varie, come ad esempio: l'implementazione di controlli di sicurezza, la formazione dei dipendenti, la creazione dei cosiddetti piani di continuità operativa (per garantire il normale funzionamento dell'azienda anche in caso di crisi), e l'adozione di politiche per la gestione delle vulnerabilità.
4. **Monitoraggio e Revisione:** Nonostante le fasi precedenti possano sembrare sufficienti, in realtà il processo di Risk Management, non termina con l'implementazione delle varie misure di mitigazione. È infatti fondamentale un costante monitoraggio dell'efficacia delle varie misure di mitigazione implementate e una revisione periodica del piano di gestione del rischio per potersi adattare ai cambiamenti e alle nuove minacce emergenti. Ciò significa effettuare regolarmente revisioni, test di sicurezza e valutazioni delle vulnerabilità.
5. **Comunicazione e Reporting:** Una parte fondamentale del processo di Risk Management, è la comunicazione trasparente e immediata delle informazioni su potenziali rischi all'interno (o esterno) dell'azienda. Ciò vuol dire, ad esempio, la creazione di rapporti di valutazione del rischio, la condivisione dei risultati delle revisioni periodiche (e/o straordinarie) e l'informare i principali 'stakeholder' sulle azioni intraprese dall'azienda per mitigare i rischi.

La gestione del rischio è quindi un elemento fondamentale per il ‘governo d’impresa’ e per le strategie di sicurezza, che permette all’azienda/ente/organizzazione di affrontare con maggiore sicurezza sfide e opportunità.

Introduzione alla Figura del Risk Manager (Manager del Rischio)

Il Risk Manager, o manager del rischio, è una figura professionale fondamentale all’interno di qualsiasi azienda/ente/organizzazione, che è responsabile di supervisionare e gestire i processi di identificazione, valutazione e mitigazione dei rischi. Questa figura professionale si ritrova quindi a svolgere un ruolo chiave nel garantire che l’azienda sia il più preparata possibile ad affrontare e minimizzare i possibili impatti negativi dovuti ad eventi imprevisti o sfavorevoli, in modo da poter proteggere le risorse dell’azienda e contribuendo al raggiungimento degli obiettivi.

Il Risk Manager si occupa di creare e implementare sia le politiche che le procedure per la gestione dei vari rischi, collaborando a stretto contatto con gli altri dipartimenti dell’azienda, come ad esempio il dipartimento IT, legale, etc.

Il Risk Manager è quindi responsabile del processo di Risk Management sopra descritto. I suoi compiti sono quindi: l’identificazione dei rischi; la valutazione e l’analisi dei rischi; lo sviluppo di strategie di mitigazione; il monitoraggio e la revisione continua; la comunicazione e il reporting. Un’altro compito essenziale del Risk Manager è quello di **Formazione e Sensibilizzazione:** il Risk Manager deve promuovere una ‘cultura’ della gestione del rischio all’interno dell’azienda/ente/organizzazione, organizzando delle sessioni di formazione per il personale, allo scopo di sensibilizzare i dipendenti riguardo l’importanza della sicurezza e della gestione dei rischi.

In conclusione, la figura del Risk Manager è essenziale per poter far fronte ai sempre più crescenti rischi del mondo moderno, che è soggetto a rapidi cambiamenti e da minacce in continua evoluzione. Grazie alla capacità di anticipare, identificare e mitigare i possibili rischi, il Risk Manager contribuisce quindi in modo significativo alla protezione delle risorse dell’azienda, alla sua continuità operativa e al successo sul lungo termine della stessa.

Contesto specifico: Azienda del Settore Informatico

Il Risk Management e la figura del Risk Manager ricoprono un ruolo fondamentale in ogni settore, ma i rischi specifici e le normative variano ampiamente da settore a settore e da paese a paese. Nel settore informatico, le aziende che si occupano di offrire servizi di tipo software e/o hardware, devono affrontare dei rischi particolari. Tra i rischi del settore troviamo rischi legati alla sicurezza delle informazioni, alla protezione dei dati personali, alla conformità alle normative tecnologiche in continua evoluzione (ad esempio il GDPR) e alla rapida crescita ed evoluzione delle minacce informatiche.

In questo documento, verrà presa un’azienda generica del settore informatico come caso di studio, allo scopo di analizzare la gestione del rischio e l’applicazione delle normative a questo contesto nello specifico. Verranno quindi esaminate le metodologie per il calcolo del

fattore di rischio, alcune strategie di mitigazione applicabili, nonché le pratiche di monitoraggio e revisione continua, prestando particolare attenzione alle peculiarità del settore informatico. Ciò permette di fornire un quadro completo e dettagliato sul Risk Management all'interno di un'azienda operante in un settore così dinamico e complesso.

Panoramica del Processo di Gestione del Rischio

Per poter calcolare i fattori di rischio, è quindi necessario prendere in considerazione diverse variabili, tra cui le normative di riferimento, le metodologie per il calcolo del rischio e le specifiche strategie di mitigazione necessarie. Si tratta di un processo complesso, che richiede una conoscenza approfondita delle leggi e dei regolamenti del settore in questione, nonché delle metodologie specifiche per analizzare in modo accurato i rischi. Di seguito verranno descritti i principali passaggi per un processo di Risk Management efficiente ed efficace in un'azienda del settore informatico, a partire da un'analisi delle normative di riferimento fino ad arrivare alla pratiche di monitoraggio e revisione continua.

Passo 1: Analisi delle Normative e delle Procedure di Valutazione del Rischio

Introduzione:

La gestione della sicurezza aziendale è fondamentale per tutte le imprese, in particolare per quelle che operano nel settore dell'informatica e che offrono servizi software e/o hardware. L'importanza della sicurezza non può essere sottovalutata: la protezione dei dati dei clienti, dei sistemi e delle informazioni è necessaria per poter garantire la continuità operativa dell'azienda, la fiducia dei clienti che usufruiscono dei servizi offerti e la conformità alle leggi che regolano il settore. Il calcolo del fattore di rischio è quindi fondamentale per poter identificare, valutare e mitigare i potenziali rischi che potrebbero compromettere la sicurezza dell'azienda.

Per poter effettuare il calcolo del rischio bisogna per prima cosa conoscere e analizzare le normative e le procedure di valutazione del rischio specifiche del settore. Le normative di riferimento forniscono un quadro specifico dei regolamenti che l'azienda deve rispettare per poter garantire la conformità e la sicurezza delle operazioni. Queste normative coprono vari aspetti, dalla protezione dei dati, alla sicurezza delle informazioni, e fino alle misure di controllo sia tecnico che organizzativo. È un primo passo fondamentale comprendere queste normative nella loro interezza per poter prendere in considerazione non solo i requisiti obbligatori che l'azienda deve rispettare, ma anche le migliori pratiche da adottare. Di seguito sono riportate le tre principali normative di riferimento che regolano il settore informatico (in un contesto in cui l'azienda caso di studio abbia sede sul suolo Italiano).

Normative di riferimento:

1 - Decreto Legislativo 81/2008 (Testo Unico sulla Sicurezza sul Lavoro, Italiano)

Il **Decreto Legislativo 81/2008** è il testo di riferimento necessario per la gestione della sicurezza sul lavoro in Italia. Il Decreto stabilisce i requisiti chiave per poter garantire la

salute e la sicurezza dei lavoratori in ogni settore, compreso quello informatico. Il Decreto è lungo e complesso, ma tra i principali aspetti coperti dalla normativa troviamo:

- **Valutazione dei Rischi**: Ogni azienda deve condurre una valutazione completa dei rischi presenti nei luoghi di lavoro. Questa valutazione deve includere l'identificazione dei potenziali pericoli, la valutazione della probabilità che l'evento di rischio si verifichi e della gravità potenziale del suddetto pericolo, nonché determinare quali siano le necessarie misure di prevenzione e protezione da adottare.
- **Formazione e Informazione**: I datori di lavoro **devono garantire** che ognuno dei propri lavoratori riceva una formazione adeguata in materia di sicurezza sul lavoro. Questa formazione deve comprendere sia una formazione generale che quella specifica per i rischi legati alle mansioni svolte dal dipendente.
- **Misure di Prevenzione e Protezione**: Il Decreto impone l'adozione di misure sia a livello tecnico che a livello organizzativo per poter prevenire gli incidenti sul lavoro e ridurre al minimo i rischi. Queste misure devono includere l'uso di eventuali dispositivi di protezione individuale o DPI (ad esempio l'elmetto che ogni operaio è tenuto ad indossare all'interno di un cantiere), la manutenzione regolare delle attrezzature (di emergenza e non; è tanto importante la manutenzione di eventuali macchinari usati regolarmente quanto quella dei vari dispositivi di emergenza, come ad esempio gli estintori) e la progettazione di ambienti di lavoro sicuri.

Per un'azienda del settore informatico, questo significa anche assicurarsi che le postazioni di lavoro siano ergonomiche (requisito fondamentale per il benessere fisico dei dipendenti), che tutti sistemi dell'azienda siano protetti da accessi non autorizzati e che siano implementate delle politiche di sicurezza adeguate per proteggere sia i dati aziendali che quelli dei clienti che usufruiscono del servizio offerto.

2 - ISO/IEC 27001 (Gestione della Sicurezza delle Informazioni, Internazionale)

L'**ISO/IEC 27001** è uno standard internazionale che definisce i requisiti necessari per poter stabilire, implementare, mantenere e migliorare un qualsiasi sistema di gestione della sicurezza delle informazioni (ISMS). Questo standard è in particolar modo rilevante per le aziende di informatica per vari motivi, tra cui troviamo:

- **Gestione del Rischio**: Lo standard richiede che si approcci in modo sistematico la gestione dei rischi legati alla sicurezza delle informazioni. Le aziende devono quindi identificare i rischi, valutare la probabilità che tale rischio si verifichi nonché l'eventuale l'impatto, e implementare dei controlli adeguati per poter mitigare suddetti rischi.
- **Controlli di Sicurezza**: Lo standard prevede una serie di controlli di sicurezza che devono e che possono essere implementati per proteggere le informazioni. Questi controlli ricoprono vari ambiti, tra cui la sicurezza a livello fisico (una sicurezza fisica inadeguate rende inutili anche le migliori protezioni a livello software); la sicurezza a livello software; la gestione delle comunicazioni e delle operazioni; il controllo degli accessi alle risorse aziendali (sia fisiche che digitali) e la gestione degli incidenti di sicurezza.

- **Conformità e Certificazione**: L'adesione a tale standard può essere verificata tramite audit (revisioni) esterni, e le aziende adempienti possono ottenere una certificazione che attesta la conformità allo standard. Questa è una certificazione che è spesso richiesta dai clienti e che può migliorare la reputazione dell'azienda agli occhi di potenziali clienti.

Per un'azienda di informatica, l'implementazione dello standard ISO/IEC 27001 aiuta non solo a proteggere le informazioni sensibili, ma anche a garantire la continuità operativa dell'azienda e a soddisfare i requisiti normativi e/o contrattuali.

3 - GDPR (Regolamento Generale sulla Protezione dei Dati, Europeo)

Il **GDPR (General Data Protection Regulation)** è un regolamento dell'Unione Europea che stabilisce delle norme assai scrupolose per la protezione dei dati personali. Questo è un regolamento fondamentale per le aziende di informatica che devono trattare i dati personali dei clienti. Il documento del regolamento è particolarmente lungo, complesso e preciso, ma i principali requisiti del GDPR includono:

- **Principi di Protezione dei Dati**: Il GDPR stabilisce i principi chiave per il trattamento dei dati personali, tra cui la liceità, la correttezza e la trasparenza sul trattamento dei dati; la limitazione delle finalità di utilizzo dei dati raccolti; la minimizzazione dei dati raccolti; l'esattezza; la limitazione del periodo di conservazione dei dati; l'integrità e la riservatezza dei dati.
- **Diritti degli Interessati**: Il regolamento riconosce vari diritti agli interessati (ovvero le persone fisiche i cui dati vengono trattati), tra cui il diritto di accesso ai propri dati, il diritto alla rettifica (ovvero a poter modificare i propri dati), il diritto alla cancellazione (diritto all'oblio), il diritto alla limitazione del trattamento (il singolo individuo deve poter decidere entro quali limiti i propri dati possano essere usati), il diritto alla portabilità dei dati e il diritto di opposizione.
- **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)**: Per i trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone, il GDPR richiede di condurre una DPIA per valutare l'eventuale impatto delle operazioni di trattamento dei dati e di adottare le misure necessarie per mitigare i rischi.
- **Notifica delle Violazioni dei Dati**: Le aziende devono notificare eventuali violazioni dei dati personali all'autorità di controllo competente entro 72 ore dalla scoperta, a meno che non sia possibile che la violazione comporti un rischio per i diritti e le libertà delle persone.

Per un'azienda di informatica, la conformità al GDPR comporta l'implementazione di misure a livello tecnico e organizzativo adeguate alla protezione dei dati personali dei clienti, la formazione dei dipendenti sia sulle pratiche di protezione dei dati da adottare, sia sulla gestione efficace delle richieste da parte dei clienti o del garante e delle notifiche di violazione al garante.

Conclusione del Passo 1

Comprendere appieno e rispettare le normative di riferimento è un requisito essenziale per garantire la conformità alle stesse nonché la sicurezza operativa di un'azienda del settore informatico. Queste normative non solo proteggono l'azienda da potenziali sanzioni legali,

ma migliorano anche la fiducia dei clienti e la reputazione dell'azienda agli occhi degli stessi. Una volta che si è stabilita una solida base normativa, è possibile procedere al passo successivo, ovvero il calcolo del fattore di rischio, utilizzando le metodologie appropriate per poter identificare e valutare i potenziali rischi.

Passo 2: Metodologie di Calcolo del Fattore di Rischio

Introduzione:

Dopo aver analizzato le normative di riferimento, il passo successivo consiste nell'applicare una delle diverse metodologie di calcolo del fattore di rischio. Queste metodologie permettono di identificare e valutare i rischi specifici dell'azienda, in modo da determinare la probabilità e l'impatto potenziale di ciascun rischio individuato. Esistono diversi strumenti analitici come l'analisi SWOT, le matrici di rischio e i modelli quantitativi, tramite cui è possibile analizzare e stabilire la priorità dei rischi individuati e sviluppare strategie efficaci per poterli mitigare. Il primo passo fondamentale per poter utilizzare uno qualsiasi di questi strumenti è **l'Identificazione dei Rischi** (che variano da azienda ad azienda, da settore a settore, nonché da paese a paese).

Identificazione e Valutazione dei Rischi:

Per un'azienda del settore informatico, che offre servizi software e/o hardware, i vari rischi possono essere principalmente suddivisi in diverse categorie. Alcuni dei principali e più comuni rischi, includono:

- **Rischi Operativi**:
    - Guasti hardware: malfunzionamenti di server, PC, dispositivi di rete o simili.
    - Errori software: bug nei programmi, malfunzionamenti delle applicazioni, etc.
    - Interruzioni del servizio: downtime del sistema, problemi di rete, etc.
- **Rischi di Sicurezza**:
    - Attacchi informatici: hacking, malware, ransomware e simili.
    - Furti di dati: accesso non autorizzato a informazioni sensibili (aziendali o dei clienti).
    - Violazioni di conformità: mancata osservanza delle normative del settore, come ad esempio il GDPR, che comportano sanzioni e anche un possibile danno all'immagine dell'azienda.
- **Rischi Ambientali**:
    - Disastri naturali: incendi, inondazioni, terremoti.
    - Interruzioni di corrente: blackout, instabilità elettrica.

Dopo aver identificato i possibili rischi, è ora necessario svolgere una Valutazione dei Rischi. La valutazione dei rischi comporta principalmente l'analisi delle probabilità che un rischio si verifichi e il calcolo del suo impatto negativo.

Esistono diverse metodologie che possono essere usate per svolgere l'identificazione e la valutazione dei rischi. Di seguito verranno introdotte tre fra le principali metodologie adottate per il settore informatico, ovvero l'analisi SWOT (Strengths Weaknesses Opportunities

Threats, un metodo generico e applicabile a diversi scenari), il metodo NIST (National Institute of Standards and Technology, che si incentra sulla gestione del rischio informatico) e il metodo OWASP (Open Web Application Security Project, che si incentra sulla sicurezza delle applicazioni web).

1 - Analisi SWOT

L'analisi SWOT è uno strumento di analisi che viene utilizzato per identificare e valutare i punti di forza (Strengths), le debolezze (Weaknesses), le opportunità (Opportunities) e le minacce (Threats) di un azienda/ente/organizzazione o addirittura di un singolo progetto. Questo metodo fornisce una visione d'insieme riguardo alla posizione attuale e futura dell'azienda/ente/organizzazione o del progetto, facilitando la pianificazione necessaria e la gestione del rischio. L'analisi SWOT prende in considerazione:

- **Strengths (Punti di Forza)**: Questi sono gli aspetti interni positivi che conferiscono qualunque un vantaggio all'azienda o al progetto. In un contesto aziendale questi punti di forza possono ad esempio includere delle risorse uniche, delle competenze chiave, ma anche una buona e salda reputazione o anche un'ampia base di clienti.
- **Weaknesses (Debolezze)**: Sono gli aspetti interni negativi che possono ostacolare in diversi modi il successo dell'azienda. Queste debolezze sono varie e possono ad esempio riguardare un problema di risorse limitate, una carenza nelle competenze del personale, ma anche dei processi aziendali inefficaci o una scarsa presenza sul mercato.
- **Opportunities (Opportunità)**: Questi sono i fattori esterni che l'azienda può sfruttare per migliorare la sua posizione e crescere. Le opportunità possono ad esempio essere rappresentate da cambiamenti nel mercato, da innovazioni tecnologiche, ma anche da cambiamenti normativi favorevoli o nuove tendenze di consumo.
- **Threats (Minacce)**: Sono i fattori esterni che potrebbero rappresentare un rischio o un ostacolo per l'azienda. Le minacce possono includere ad esempio la concorrenza crescente, dei cambiamenti nelle normative sfavorevoli all'azienda, così come un'instabilità economica o un'evoluzione tecnologica che potrebbe rendere obsoleti i prodotti e/o servizi offerti dall'azienda.

L'analisi SWOT consente all'azienda/ente/organizzazione di sviluppare delle strategie che siano in grado di massimizzare i punti di forza e le opportunità, mentre puntino a minimizzare le debolezze e le minacce che potrebbero presentarsi. L'Analisi SWOT è uno strumento versatile e semplice da usare, che può essere adattato a varie situazioni e a vari settori. Per un Risk Manager, l'analisi SWOT è uno strumento particolarmente utile per poter valutare il 'panorama' dei rischi e riuscire ad elaborare dei piani di mitigazione efficaci.

2 - Metodo NIST (National Institute of Standards and Technology)

Il **metodo NIST** fornisce una guida più specifica per la gestione del rischio informatico e si suddivide nelle seguenti fasi:

- **Identificazione dei Rischi**: Si analizzano e catalogano tutti i rischi potenziali.
- **Analisi dei Rischi**: Si valuta la probabilità (frequenza) e l'impatto (gravità) di ciascun rischio.

- **Mitigazione dei Rischi**: Si studiano, sviluppano e implementano delle misure di controllo per poter ridurre la probabilità e/o l'impatto dei rischi analizzati.
- **Monitoraggio dei Rischi**: Si procede ad un monitoraggio continuo dei rischi e delle misure di controllo e mitigazione intraprese per poterne garantire l'efficacia nel tempo.

3 - Metodo OWASP (Open Web Application Security Project)

Il **metodo OWASP** si concentra più specificatamente sulla sicurezza delle applicazioni web e si suddivide nelle seguenti fasi:

- **Identificazione delle Minacce**: Si utilizza un modello di una minaccia per poter essere in grado di identificare potenziali attacchi.
- **Analisi delle Vulnerabilità**: Si esamina il codice dell'applicazione e le sue diverse configurazioni per poter identificare le possibili vulnerabilità.
- **Valutazione del Rischio**: Si determina la probabilità di exploit, attacchi informatici, virus e simili e il loro impatto potenziale.
- **Implementazione dei Controlli**: Si applicano le necessarie misure di sicurezza per mitigare le vulnerabilità che sono state riscontrate.

Per poter completare la valutazione dei rischi, è necessario essere in grado di calcolare il **Fattore di Rischio** per ogni rischio che si è identificato, in modo tale da poter applicare le necessarie misure di mitigazione del rischio.

Calcolo del Fattore di Rischio:

Il calcolo del fattore di rischio è un passo fondamentale per la mitigazione dei rischi. Il fattore di rischio viene calcolato semplicemente combinando la probabilità che un evento si verifichi con il suo possibile impatto. La formula standard è:

Fattore di Rischio = Probabilità x Impatto

Dove:

- **Probabilità**: E' la possibilità che un rischio si verifichi (valutata su una scala da 1 a 5).
- **Impatto**: Sono le conseguenze o l'effetto di un rischio nel caso in cui lo stesso si verifichi (valutato su una scala da 1 a 5).

Questa scala di valutazione è solitamente soggettiva da azienda ad azienda (le probabilità che un'evento si verifichi sono diverse da azienda ad azienda, così come l'eventuale impatto), ma generalmente la scala di valutazione più usata è la seguente:

- **Probabilità**:
    - 1: Molto bassa (meno del 5%)
    - 2: Bassa (5-20%)
    - 3: Moderata (21-50%)
    - 4: Alta (51-80%)
    - 5: Molto alta (oltre l'80%)
- **Impatto**:

- 1: Insignificante (l’evento ha un impatto minimo sull'operatività aziendale)
- 2: Minore (l’evento ha un impatto limitato e facilmente gestibile dall’azienda)
- 3: Moderato (l’evento ha un impatto significativo, richiede interventi da parte dell’azienda)
- 4: Maggiore (l’evento ha un impatto grave, richiede azioni immediate per garantire la continuità dell’operatività aziendale)
- 5: Catastrofico (l’evento ha un impatto critico, compromette l'operatività aziendale per un periodo di tempo indeterminato)

Esempi Pratici di Calcolo del Fattore di Rischio:

Scenario 1: Cyber attacco a un server

- **Probabilità**: Alta (4) - E’ presente un’elevata frequenza di attacchi informatici (soggettivo all’azienda).
- **Impatto**: Maggiore (4) - Esiste il rischio di una possibile compromissione di dati sensibili e un’interruzione dei servizi.

  Fattore di Rischio = 4 x 4 = 16

Scenario 2: Guasto hardware critico

- **Probabilità**: Moderata (3) - I guasti hardware non sono frequenti ma sono comunque possibili (soggettivo all’azienda).
- **Impatto**: Maggiore (4) - L’eventuale guasto comporterebbe un interruzione significativa del servizio (soggettivo all’azienda).

  Fattore di Rischio = 3 x 4 = 12

Scenario 3: Violazione dei dati personali (GDPR)

- **Probabilità**: Moderata (3) - C’è un possibile rischio di violazioni di sicurezza riguardanti i dati dei clienti.
- **Impatto**: Catastrofico (5) - Nel caso in cui l’evento si verifichi, l’azienda è sottoposta a sanzioni severe e anche ad un possibile danno alla sua reputazione.

  Fattore di Rischio = 3 x 5 = 15

Conclusione del Passo 2

Dopo aver applicato una o più delle diverse metodologie per il calcolo del fattore di rischio, è possibile comprendere come ogni rischio possa essere quantificato e prioritizzato in base alla sua probabilità di verificarsi ed al suo possibile impatto. Questo processo, quindi, non solo identifica i rischi potenziali, ma fornisce anche una solida base di partenza per poter prendere decisioni informate su come poterli affrontare. Una volta ottenuta una più approfondita consapevolezza dei rischi specifici e la loro valutazione dettagliata, il prossimo

passo è naturalmente lo sviluppo delle strategie di mitigazione. Queste strategie sono essenziali per poter ridurre al minimo l'impatto dei rischi che si sono identificati e per garantire che l'azienda possa affrontare al meglio le sfide che si presentano.

Nel passo successivo, verranno prese in considerazione le diverse strategie di mitigazione del rischio che possono essere implementate per proteggere le risorse dell'azienda e per poter assicurare la continuità operativa della stessa.

Passo 3: Sviluppo delle Strategie di Mitigazione

Introduzione

Una volta che si sono identificati e valutati i rischi specifici per l'azienda, il passo successivo è quello di sviluppare delle strategie di mitigazione per poter gestire efficacemente i suddetti rischi. L'obiettivo delle strategie di mitigazione è quello di ridurre la probabilità che un rischio si verifichi e, nel caso, fare il possibile per minimizzarne l'impatto potenziale. Essendo che i rischi potenziali sono molti e diversificati, non esistono prettamente delle strategie di mitigazione uniche. Un passo tuttavia fondamentale è quello di stabilire delle "Politiche di Sicurezza", uniche da settore a settore e da azienda ad azienda.

Le **Politiche di Sicurezza** sono un passo importante nello sviluppo delle strategie di mitigazione poiché servono come guida per le azioni e i comportamenti dei dipendenti. Queste politiche devono essere ben definite e applicate il più rigorosamente possibile, in modo da garantire la protezione delle informazioni aziendali. Di seguito sono elencate alcune delle principali politiche di sicurezza generali ad un'azienda del settore informatico:

- **Gestione delle Password:** Un aspetto fondamentale della sicurezza informatica è la gestione delle password. Le politiche di sicurezza dovrebbero includere l'obbligo per i dipendenti di utilizzare password complesse e, possibilmente, che siano anche cambiate regolarmente. Inoltre, l'autenticazione a due fattori (2FA) dovrebbe essere implementata per l'accesso ai sistemi critici, in modo da garantire un livello di protezione aggiuntivo.
- **Controllo degli Accessi:** Per proteggere i dati sensibili, è essenziale limitare e monitorare l'accesso a questi dati. Solo il personale autorizzato dovrebbe averne l'accesso, e ogni accesso deve essere tracciato per poter identificare potenziali abusi o eventuali accessi non autorizzati.
- **Gestione delle Vulnerabilità:** La sicurezza delle informazioni richiede una gestione attiva delle vulnerabilità. E' necessario effettuare delle scansioni periodiche del sistema per poter identificare e correggere in modo tempestivo delle eventuali vulnerabilità. Questo processo serve a garantire che le misure di sicurezza siano sempre aggiornate ed efficaci.

Esempi Pratici:
Illustreremo ora alcune misure di mitigazione possibili basandosi su degli scenari di potenziali rischi per un'azienda di informatica.

Scenario 1: Cyber attacco ad un server

Descrizione del Rischio: Un attacco informatico mirato ad un server aziendale ha la possibilità di compromettere dei dati sensibili, causare dei downtime dei servizi offerti e anche di danneggiare la reputazione dell'azienda.

Valutazione del Rischio:

- **Probabilità**: Alta (4) - Gli attacchi informatici sono frequenti e i server sono degli obiettivi primari.
- **Impatto**: Maggiore (4) - Possibile compromissione di dati sensibili, interruzione dei servizi e anche danno alla reputazione.

  Fattore di Rischio = 4 x 4 = 16

Misure di Mitigazione:

1. **Implementazione di firewall e sistemi di rilevamento delle intrusioni (IDS/IPS)**: Per monitorare e prevenire accessi non autorizzati.
2. **Aggiornamento regolare dei software e delle patch di sicurezza**: Per ridurre le vulnerabilità.
3. **Formazione dei dipendenti**: Sensibilizzazione sui rischi di phishing e social engineering.
4. **Backup regolari dei dati**: Per garantire il ripristino rapido in caso di attacco.

Scenario 2: Guasto ad un hardware critico

Descrizione del Rischio: Un guasto ad un hardware critico, come il malfunzionamento di un server principale, può causare un'interruzione significativa dei servizi offerti dall'azienda.

Valutazione del Rischio:

- **Probabilità**: Moderata (3) - I guasti hardware sono meno frequenti ma pur sempre possibili.
- **Impatto**: Maggiore (4) - Interruzione significativa dei servizi, perdita temporanea di dati e produttività.

  Fattore di Rischio = 3 x 4 = 12

Misure di Mitigazione:

1. **Implementazione di un sistema di monitoraggio dell'hardware**: Per rilevare e prevenire guasti imminenti.
2. **Piani di manutenzione preventiva**: Per garantire che tutto l'hardware sia mantenuto in buone condizioni.
3. **Utilizzo di soluzioni di ridondanza**: Come server di backup e storage ridondante per garantire la continuità.

4. **Disaster Recovery Plan (DRP)**: Un piano dettagliato per il ripristino rapido dei servizi in caso di guasto hardware.

Scenario 3: Violazione dei dati personali (GDPR)

Descrizione del Rischio: Un'eventuale violazione dei dati personali potrebbe comportare delle severe sanzioni secondo il GDPR, oltre che a causare dei danni alla reputazione e alla fiducia dei clienti.

Valutazione del Rischio:

- **Probabilità**: Moderata (3) - Il rischio di incidenti di sicurezza dei dati è presente, soprattutto se non sono adottate misure adeguate.
- **Impatto**: Catastrofico (5) - Sanzioni severe, danni alla reputazione e perdita di fiducia dei clienti.

  Fattore di Rischio = 3 x 5 = 15

Misure di Mitigazione:

1. **Implementazione di politiche di sicurezza dei dati**: Assicurare che i dati personali siano trattati in conformità con il GDPR.
2. **Crittografia dei dati**: Proteggere i dati personali con crittografia per ridurre il rischio di accesso non autorizzato.
3. **Formazione dei dipendenti**: Sensibilizzare i dipendenti sull'importanza della protezione dei dati e delle normative GDPR.
4. **Audit regolari e valutazioni d'impatto sulla protezione dei dati (DPIA)**: Per identificare e mitigare i rischi relativi ai dati personali.
5. **Piani di risposta agli incidenti**: Procedure chiare per la gestione e la notifica delle violazioni dei dati personali.

Conclusione del Passo 3

L'implementazione delle strategie di mitigazione è quindi fondamentale per poter ridurre al minimo l'impatto dei rischi che si sono identificati e poter garantire la resistenza dell'azienda. Tuttavia, il rischio è una realtà dinamica, in continuo mutamento. Perciò, è essenziale non solo sviluppare e mettere in atto delle strategie di mitigazione, ma è anche necessario monitorare costantemente l'efficacia delle misure adottate e, se necessario, adattarle alle nuove minacce e vulnerabilità che possono emergere. Nel prossimo passo infatti, andremo a prendere in esame l'importanza del monitoraggio continuo e della revisione periodica dei rischi, in modo tale da poter mantenere nel tempo un livello di sicurezza alto e la conformità alle normative di legge.

Passo 4: Monitoraggio e Revisione Continua

Introduzione:

Il monitoraggio continuo e la revisione periodica sono dei componenti essenziali all'interno di un sistema di gestione del rischio efficace. Questi processi servono ad assicurarsi che le misure di mitigazione continuino ad essere efficaci e che l'azienda sia pronta ad affrontare i nuovi rischi che potrebbero emergere. Esploreremo quindi passo per passo le pratiche e gli strumenti che sono necessari per mantenere un controllo costante sui rischi e come adattare le strategie di mitigazione in maniera tempestiva.

Integrazione del Sistema di Gestione dei Rischi:

Passo 1: Identificazione e Valutazione dei Rischi

1. **Creare un Team di Gestione dei Rischi**:
    - E' necessario costituire un team dedicato alla gestione dei rischi composto da membri chiave dell'azienda, inclusi rappresentanti del reparto IT, della sicurezza, del reparto legale e anche quello amministrativo e di gestione.
2. **Condurre un'Analisi dei Rischi**:
    - Bisogna identificare i rischi potenziali utilizzando strumenti come checklist, interviste e brainstorming.
    - Una volta identificati, si procede a classificare i rischi in base alla loro natura (operativi, di sicurezza, ambientali, ecc.).
3. **Valutare i Rischi**:
    - Si assegna un punteggio di probabilità e di impatto a ciascun rischio identificato.
    - Si calcola il fattore di rischio per ciascun rischio utilizzando la formula già vista in precedenza:

      Fattore di Rischio = Probabilità x Impatto

Passo 2: Pianificazione delle Misure di Mitigazione

1. **Sviluppare un Piano di Mitigazione dei Rischi**:
    - Si definiscono le misure preventive e correttive per poter ridurre la probabilità e l'impatto dei rischi.
    - Si assegnano delle responsabilità specifiche per l'implementazione delle misure di mitigazione.
2. **Implementare Controlli di Sicurezza**:
    - Si implementano firewall, IDS/IPS, crittografia, backup regolari e altre misure di sicurezza tecnica necessarie.
    - Si stabiliscono le politiche di sicurezza dei dati e le procedure necessarie per conformarsi alle normative di legge (ISO/IEC 27001, GDPR, ecc.).

Passo 3: Monitoraggio e Revisione dei Rischi

1. **Monitorare Continuamente i Rischi**:
    - Si utilizzano degli strumenti di monitoraggio per rilevare e rispondere il più rapidamente possibile ai nuovi rischi o a dei cambiamenti nei rischi esistenti.
    - Si conducono degli audit regolari e delle valutazioni d'impatto riguardanti la protezione dei dati (DPIA).
2. **Revisione Periodica del Sistema di Gestione dei Rischi**:

- Si rivede e, se necessario, si aggiorna periodicamente il piano di gestione dei rischi in base ai risultati del monitoraggio e agli audit.
- Si effettuano dei test di penetrazione e delle valutazioni di vulnerabilità per poter verificare l'efficacia delle misure di sicurezza adottate.

Monitoraggio e Revisione Periodica

1. **Audit e Verifiche di Conformità**:
   - Si conducono degli audit interni ed esterni per assicurarsi che il sistema di gestione dei rischi sia conforme agli standard e alle normative vigenti.
   - Si verifica regolarmente che le politiche e le procedure di sicurezza siano seguite e applicate correttamente.
2. **Valutazioni di Vulnerabilità**:
   - Bisogna effettuare delle valutazioni regolari delle vulnerabilità del sistema per poter identificare e correggere degli eventuali punti deboli.
   - E' necessario utilizzare degli strumenti di scansione automatica e dei test di penetrazione manuali per poter garantire una copertura completa.
3. **Rafforzamento Continuo**:
   - E' fondamentale aggiornare continuamente le misure di sicurezza in risposta ai nuovi rischi e alle nuove minacce.
   - Bisogna investire in tecnologie avanzate e corsi di formazione continua per poter mantenere un alto livello di sicurezza e di protezione dei dati.

Conclusione del Passo 4

Il monitoraggio continuo e la revisione periodica sono i pilastri fondamentali per un sistema di gestione del rischio efficace. Se si mantiene un controllo costante sui rischi e si adattano tempestivamente le strategie di mitigazione, le aziende possono assicurarsi che le loro difese rimangano robuste e aggiornate di fronte a delle nuove minacce. Questo approccio proattivo non serve solo a ridurre il potenziale impatto dei rischi, ma serve anche a rafforzare la resistenza complessiva dell'azienda. Una volta che si è messo in atto un solido sistema di monitoraggio e revisione, il prossimo passo cruciale è quello di garantire che tutti i dipendenti dell'azienda abbiano ricevuto una formazione adeguata e che siano stati sensibilizzati sui rischi e sulle pratiche di sicurezza che bisogna necessariamente adottare.

Passo 5: Formazione e Sensibilizzazione

Introduzione:

La formazione e la sensibilizzazione dei dipendenti sono degli elementi essenziali per una gestione del rischio efficace. Un'azienda può anche avere le migliori tecnologie e le più elevate procedure di sicurezza in atto, ma se il personale della stessa non è adeguatamente informato e formato, i rischi di sicurezza possono comunque emergere. Osserveremo quindi le strategie necessarie per poter sviluppare un programma di formazione e sensibilizzazione che coinvolga tutti i livelli dell'azienda. L'obiettivo infatti è quello di creare un organico aziendale che sia consapevole dei rischi, dove ogni singolo dipendente è in grado di comprendere l'importanza della sicurezza e quale sia il proprio ruolo nel mantenere l'azienda protetta.

I programmi di **Formazione e Sensibilizzazione** sono variegati, e si possono a grandi linee dividere in:

Programmi di Formazione

1. **Formazione Generale per Tutti i Dipendenti:**
    - **Sessioni di Formazione Periodiche:** Si organizzano dei corsi regolari che siano in grado di coprire i fondamenti della sicurezza informatica, le migliori pratiche che è necessario adottare per proteggere dati e sistemi e le principali normative di legge rilevanti come ad esempio il GDPR.
    - **E-learning e Moduli Online:** E' possibile fornire l'accesso a piattaforme di apprendimento online, dove i dipendenti possono completare i moduli di formazione necessari secondo il loro ritmo.
    - **Workshop Interattivi:** Si possono anche creare dei workshop pratici che possano simulare degli scenari di rischio e che permettano ai dipendenti di applicare le conoscenze apprese in situazioni reali.
2. **Formazione Specializzata per il Personale Tecnico:**
    - **Tecniche di Difesa Avanzate:** E' fondamentale formare il personale IT su tecniche avanzate di difesa contro gli attacchi informatici, inclusi firewall, intrusion detection systems (IDS), intrusion prevention systems (IPS) e crittografia.
    - **Gestione degli Incidenti di Sicurezza:** Bisogna inoltre addestrare i team tecnici a riconoscere, rispondere e recuperare in maniera tempestiva dagli incidenti di sicurezza, possibilmente usando anche delle simulazioni di scenari di crisi.

Sensibilizzazione

1. **Campagne di Sensibilizzazione:**
    - **Poster Informativi e Newsletter:** Si distribuisce regolarmente del materiale informativo che evidenzia dei consigli di sicurezza, delle storie di incidenti recenti e eventuali aggiornamenti sulle politiche di sicurezza aziendali.
    - **Eventi e Seminari:** Si possono organizzare degli eventi aziendali dedicati alla sicurezza informatica, con la partecipazione di esperti del settore che possano condividere le loro esperienze ed eventuali raccomandazioni.
2. **Simulazioni di Attacchi:**
    - **Test di Phishing:** Si possono condurre delle simulazioni di attacchi di phishing per poter valutare la consapevolezza dei dipendenti e fornire un feedback immediato su come si possa riconoscere e rispondere a tali minacce.
    - **Esercitazioni di Sicurezza:** Si pianificano delle esercitazioni periodiche che simulino vari tipi di attacchi informatici, in modo tale da poter testare la prontezza e la reattività dei team.
3. **Creazione di una Cultura della Sicurezza:**
    - **Incoraggiare il Feedback:** Si creano dei canali di comunicazione attraverso i quali i dipendenti possono segnalare problemi di sicurezza o fare domande sulle migliori pratiche di sicurezza da adottare.

- **Riconoscimento e Incentivi:** E’ buona pratica premiare i dipendenti che dimostrano un impegno eccezionale nel promuovere sia la sicurezza informatica che il rispetto delle politiche aziendali.

Conclusione del Passo 5

Un programma di formazione e sensibilizzazione ben strutturato è fondamentale per poter rafforzare la sicurezza complessiva dell'azienda. Attraverso un programma di formazione continua e la promozione di una cultura della sicurezza, i dipendenti diventano così la prima linea di difesa contro le minacce informatiche. Una volta implementato questo programma, è fondamentale una comunicazione e un monitoraggio costante dei progressi e dei risultati ottenuti. Adesso ci andremo quindi a concentrare sull'importanza della comunicazione efficace e del reporting, in modo tale da poter garantire che le informazioni critiche sulla sicurezza siano condivise il più rapidamente possibile e che le decisioni da intraprendere si basino su dei dati accurati.

Passo 6: Comunicazione e Reporting

Introduzione:

La comunicazione trasparente ed il reporting accurato, sono i componenti chiave per una gestione del rischio efficace. Andremo quindi ad esaminare quali siano le migliori pratiche per potersi assicurare che le informazioni sui rischi siano comunicate in modo rapido ed efficiente e come i rapporti dettagliati possano aiutare nelle decisioni e nell'adeguamento delle misure di sicurezza. Tratteremo quindi dei rapporti di valutazione e dei test del sistema di gestione dei rischi.

Rapporto di Valutazione e Test

Obiettivi del Test

Gli obiettivi principali di un test del sistema di gestione dei rischi per un'azienda di informatica sono i seguenti:

1. **Verificare l'efficacia del sistema di gestione dei rischi** nel rilevare, valutare e mitigare i rischi identificati.
2. **Valutare la conformità alle normative di legge e agli standard** di sicurezza informatica applicabili (es. ISO/IEC 27001, GDPR).
3. **Identificare eventuali lacune** nel sistema di gestione dei rischi e apportare le modifiche che si ritengono necessarie.
4. **Assicurare la preparazione dell'azienda** nel rispondere a incidenti di sicurezza e a possibili violazioni dei dati.

Metodologia di Test

La metodologia di test comprende i seguenti passaggi:

1. **Pianificazione del Test**:

    - Si definisce un piano di test, compresi gli obiettivi, l'ambito e le risorse necessarie.
    - Si identificano gli scenari di rischio da testare (ad esempio attacchi informatici, guasti hardware, violazioni dei dati, etc.).
2. **Preparazione del Test**:
    - Si configura l'ambiente di test per poter simulare delle condizioni operative reali.
    - Si creano degli script di test e degli strumenti di monitoraggio per poter raccogliere i dati necessari durante il test.
3. **Esecuzione del Test**:
    - Si simulano degli scenari di rischio che si sono identificati, utilizzando tecniche di test come il penetration testing, il vulnerability scanning e gli attacchi di phishing simulati.
    - Si effettua un monitoraggio dei sistemi e si effettua una raccolta dei dati relativi alle prestazioni del sistema di gestione dei rischi.
4. **Analisi dei Risultati**:
    - Bisogna ora effettuare una valutazione dei risultati del test per poter determinare l'efficacia delle misure di mitigazione e dei controlli di sicurezza.
    - Si identificano le eventuali aree in cui è possibile effettuare un miglioramento e le eventuali lacune presenti nel sistema.

Risultati del Test

Ecco un esempio di come potrebbero essere presentati i risultati di un test, prendendo in considerazione gli scenari possibili già trattati in precedenza:

Scenario 1: Cyber attacco ad un server

- **Descrizione**: Simulazione di un attacco DDoS e tentativi di accesso non autorizzato ad un server aziendale.
- **Risultati**:
    - **Probabilità stimata**: Alta (4)
    - **Impatto stimato**: Maggiore (4)
    - **Fattore di Rischio**: 16
    - **Misure di mitigazione**: Firewall e IDS/IPS hanno rilevato e bloccato l'attacco. I tempi di risposta sono stati adeguati, ma si è evidenziata la necessità di migliorare la capacità di gestione del traffico.

Scenario 2: Guasto ad un hardware critico

- **Descrizione**: Simulazione del guasto di un server principale.
- **Risultati**:
    - **Probabilità stimata**: Moderata (3)
    - **Impatto stimato**: Maggiore (4)
    - **Fattore di Rischio**: 12
    - **Misure di mitigazione**: Il sistema di backup e ripristino ha funzionato correttamente, ma i tempi di ripristino potrebbero essere migliorati con ulteriori misure di ridondanza.

Scenario 3: Violazione dei dati personali (GDPR)

- **Descrizione**: Simulazione di un attacco phishing e furto di dati personali.
- **Risultati**:
    - **Probabilità stimata**: Moderata (3)
    - **Impatto stimato**: Catastrofico (5)
    - **Fattore di Rischio**: 15
    - **Misure di mitigazione**: Le politiche di sicurezza dei dati e la crittografia si sono dimostrate efficaci, ma è necessaria una maggiore formazione dei dipendenti per migliorare la rilevazione degli attacchi phishing.

Valutazione dei Risultati

E' ora necessario effettuare un'analisi dei risultati ottenuti dai test (in questo caso degli scenari di esempio) effettuati per poter evidenziare le eventuali lacune o le eventuali azioni da intraprendere per il miglioramento del sistema.

1. **Efficacia delle Misure di Mitigazione**:
    - Le misure di mitigazione implementate hanno mostrato un buon livello di efficacia nella gestione dei rischi. Tuttavia, sono state identificate alcune aree in cui è possibile un miglioramento, come ad esempio la gestione del traffico durante gli attacchi DDoS e i tempi di ripristino dei sistemi.
2. **Conformità alle Normative**:
    - Il sistema di gestione dei rischi è risultato conforme alle normative di legge e agli standard di sicurezza applicabili.
    - Le politiche di sicurezza dei dati e le procedure di risposta agli incidenti sono state adeguatamente testate e si sono dimostrate efficaci.
3. **Lacune e Aree di Miglioramento**:
    - È necessaria una maggiore formazione dei dipendenti per la rilevazione e la gestione degli attacchi di phishing.
    - I tempi di ripristino dei sistemi possono essere migliorati con delle ulteriori misure di ridondanza e di ottimizzazione dei processi di backup.

Raccomandazioni e Azioni Correttive

Se sono state trovate delle lacune che richiedono delle azioni correttive o sono possibili dei miglioramenti, è necessario aggiungere queste informazioni al report. Prendendo come riferimento gli esempi precedenti, potremmo ad esempio dire che sarebbe necessario:

1. **Migliorare la Capacità di Gestione del Traffico**:
    - Bisogna implementare delle soluzioni di gestione del traffico più avanzate per poter migliorare la capacità di risposta durante degli attacchi DDoS.
2. **Ottimizzare i Tempi di Ripristino**:
    - Sarebbe opportuno investire in ulteriori misure di ridondanza e di ottimizzazione dei processi di backup per poter ridurre i tempi di ripristino in caso di un guasto hardware.
3. **Aumentare la Formazione dei Dipendenti**:
    - E' necessario organizzare delle sessioni di formazione regolari per i dipendenti sulla rilevazione e sulla gestione degli attacchi di phishing.

    - Sarebbe opportuno promuovere una cultura della sicurezza attraverso delle campagne di sensibilizzazione e delle simulazioni di attacchi.
4. **Aggiornare Regolarmente le Misure di Sicurezza**:
    - E’ fondamentale rivedere e aggiornare periodicamente le politiche di sicurezza e le misure di mitigazione in risposta ai nuovi rischi e alle minacce emergenti.

Conclusione del Passo 6:

Il rapporto di valutazione e test fornisce quindi una panoramica completa riguardo l'efficacia del sistema di gestione dei rischi implementato da un'azienda. Identificando le aree di miglioramento e proponendo eventuali azioni correttive, l'azienda può in tal modo rafforzare ulteriormente la sua capacità di gestione dei rischi e protezione delle risorse aziendali.