Corso di Laurea Triennale in

Informatica per le aziende digitali L-31

Project Work in privacy e sicurezza aziendale

Sviluppo di un software per la sicurezza aziendale

Sicurezza aziendale: Calcolo e Gestione del Rischio

CANDIDATO:

Latini Leo

MATRICOLA:

0312201763

Anno Accademico

2024/2025

Indice

Introduzione

Negli ultimi anni, la sicurezza informatica è diventata una delle sfide più grandi per governi, aziende e privati. Viviamo in un mondo sempre più digitale, dove ogni giorno vengono generati, trasmessi e archiviati miliardi di dati. Se da un lato questa evoluzione ci ha portato enormi vantaggi, dall'altro ha anche reso le nostre informazioni più esposte a minacce come attacchi hacker, furti di dati e malware.

Ma la sicurezza informatica non riguarda solo la protezione dei dati personali. È una questione di stabilità, continuità operativa e rispetto delle normative. Un cyberattacco può avere conseguenze molto gravi: pensiamo, ad esempio, a un ospedale che non riesce più ad accedere ai suoi sistemi, a una banca bloccata o a una rete elettrica compromessa. È per questo che governi e istituzioni internazionali hanno sviluppato regole precise per proteggere le infrastrutture digitali e ridurre il rischio di incidenti informatici.

L'obiettivo principale di questo Project Work è fornire un'analisi approfondita delle normative sulla sicurezza informatica e delle metodologie di valutazione del rischio, con particolare attenzione al calcolo del fattore di rischio. Con una panoramica completa sulle migliori pratiche del settore e sulle strategie più efficaci per proteggere le infrastrutture digitali.

La guida si propone di:

- Esaminare le principali minacce esistenti.
- Analizzare le normative più rilevanti, come il **GDPR**, la **ISO/IEC 27001, il NIS** e il **NIST**.
- Approfondire le metodologie di valutazione del rischio, confrontando approcci qualitativi e quantitativi.
- Presentare un modello per il calcolo del fattore di rischio e fornire esempi pratici di applicazione.

Oggi più che mai, la gestione del rischio informatico è fondamentale per qualsiasi organizzazione.

Gli attacchi informatici sono sempre più frequenti e complessi, rendendo indispensabile adottare strategie di sicurezza solide e basate su normative affidabili.

Sapere come identificare e misurare il rischio non è solo una questione tecnica, ma un passo essenziale per costruire difese più efficaci, ridurre l'esposizione alle minacce e garantire la continuità delle attività aziendali.

In un mondo sempre più interconnesso, la cybersecurity non è più solo una preoccupazione per gli esperti del settore, ma una priorità globale.

Capitolo 1 – Sicurezza Informatica e Gestione del Rischio

Cosa si intende per rischio informatico?

Il **rischio informatico** può essere definito come la probabilità che eventi dannosi si verifichino e che compromettano la sicurezza, l'integrità, la disponibilità o la riservatezza dei sistemi informativi e dei dati. Può derivare da minacce esterne, come attacchi hacker, o da fattori interni, quali errori umani, vulnerabilità software o guasti infrastrutturali. Anche un'azione apparentemente innocua, come l'apertura di un'email di phishing, può trasformarsi in un problema serio, causando danni economici e di immagine.

Minacce principali e vulnerabilità

Le minacce informatiche, in continuo aumento, rappresentano una sfida costante per le aziende di ogni settore. Di seguito vengono esplorati alcuni dei principali tipi di minacce e vulnerabilità a cui le organizzazioni devono fare fronte:

1. **Malware e Ransomware**

Il **malware** è un termine generico che identifica qualsiasi tipo di software dannoso progettato per infiltrarsi, danneggiare o compromettere il funzionamento dei sistemi informatici. Tra le forme più pericolose di malware troviamo il **ransomware** che si distingue per la sua capacità di bloccare o criptare dati aziendali, rendendoli inaccessibili senza il pagamento di un riscatto. Questo tipo di attacco ha un impatto devastante su organizzazioni di qualsiasi tipo, poiché può paralizzare completamente le operazioni aziendali, impedendo l'accesso a documenti e informazioni cruciali. Oltre alla richiesta di riscatto, gli effetti collaterali di un attacco ransomware includono la perdita di fiducia dei clienti, danni alla reputazione e potenziali sanzioni legali, qualora vengano compromessi i dati sensibili.

2. **Phishing e Social Engineering**

Gli attacchi di **phishing** rappresentano una delle forme più comuni di "inganno informatico", dove l'attaccante cerca di indurre l'utente a rivelare informazioni sensibili, come credenziali di accesso, numeri di carte di credito o informazioni bancarie. Questi attacchi si presentano solitamente sotto forma di email apparentemente legittime da fonti affidabili, come banche, fornitori di servizi o colleghi, che invitano l'utente a cliccare su link dannosi o a scaricare allegati contenenti malware. Il **social engineering**, che si sovrappone al phishing, sfrutta la psicologia umana per manipolare le persone e ottenere l'accesso non autorizzato ai sistemi aziendali. In questo caso, gli attaccanti possono sfruttare informazioni di contatto o dettagli su una persona o un'organizzazione per guadagnare la fiducia del bersaglio, inducendolo a compiere azioni dannose come la condivisione di password o la concessione di accesso a reti protette.

3. **Attacchi DDoS (Distributed Denial of Service)**

Gli attacchi **DDoS** mirano a sopraffare i sistemi aziendali con un volume straordinario di traffico proveniente da una rete distribuita di dispositivi compromessi (botnet). L'obiettivo principale di un attacco DDoS è quello di rendere i sistemi aziendali, come i siti web o i server, inaccessibili agli utenti legittimi, provocando disservizi che possono durare ore o anche giorni. Gli effetti di un attacco DDoS vanno oltre la semplice interruzione del servizio; possono causare una significativa perdita di fatturato, danni alla reputazione aziendale e, in alcuni casi, compromettere la fiducia dei clienti nel

brand. Le aziende che dipendono da piattaforme online per le loro operazioni quotidiane sono particolarmente vulnerabili a questo tipo di attacco.

4. **Vulnerabilità Software e Configurazioni Errate**

Una delle principali cause di attacchi informatici è rappresentata dalle **vulnerabilità nel software** o dalle **configurazioni errate** nei sistemi aziendali. I software non aggiornati, i bug o le falle di sicurezza non corretti possono essere facilmente sfruttati da attaccanti per accedere a informazioni sensibili o per compromettere l'integrità dei sistemi. Allo stesso modo, una **configurazione errata** dei sistemi, come l'assenza di misure di protezione adeguate (ad esempio, l'uso di password deboli o la mancata applicazione di patch di sicurezza), può lasciare aperte delle "porte" a cui gli hacker possono accedere senza ostacoli. La mancata gestione dei rischi associati a vulnerabilità software e configurazioni errate può compromettere seriamente la sicurezza complessiva dell'infrastruttura aziendale.

5. **Minacce Interne**

Non tutte le minacce provengono dall'esterno. Le **minacce interne** rappresentano un rischio significativo, poiché possono essere causate da dipendenti, collaboratori o partner aziendali. Questi attacchi possono essere sia accidentali, come nel caso di un impiegato che apre involontariamente un'email infetta, sia intenzionali, quando un individuo malintenzionato decide di sottrarre dati aziendali sensibili per fini personali o per venderli a competitor. Le minacce interne sono spesso difficili da rilevare, poiché gli aggressori hanno già accesso ai sistemi aziendali e possono agire senza destare sospetti. Inoltre, dipendenti disattenti o non formati adeguatamente sulla sicurezza informatica possono inconsapevolmente compromettere la sicurezza dei sistemi aziendali, esponendo l'organizzazione a rischi significativi.

Impatto economico e operativo

Le conseguenze derivanti da un attacco informatico si estendono ben oltre la semplice perdita di dati. Esse possono influire gravemente sulle risorse economiche, sulla reputazione e sulla capacità operativa di un'organizzazione.

In elenco le principali aree in cui si concretizzano gli effetti:

1. **Perdite Economiche Dirette e Indirette**

Gli attacchi informatici, come il ransomware, comportano spesso perdite finanziarie dirette significative. I costi relativi al pagamento del riscatto, uniti alle spese per il recupero dei dati, possono ammontare a milioni di euro, con effetti devastanti sui bilanci aziendali. Inoltre, l'interruzione dei servizi può provocare una riduzione dei ricavi a causa della temporanea impossibilità di operare o di accedere a risorse fondamentali. L'impatto può essere ancora più rilevante se il cyber attacco coinvolge informazioni sensibili che richiedono azioni legali per la gestione delle violazioni.

2. **Danni alla reputazione**

Un altro aspetto cruciale degli attacchi informatici è il danno alla reputazione dell'organizzazione. In seguito alla violazione di dati, la fiducia dei clienti e dei partner può essere compromessa irreparabilmente. Le aziende che non riescono a proteggere adeguatamente le informazioni sensibili possono essere abbandonate dai propri clienti, portando a una riduzione delle vendite e della quota di mercato. La ricostruzione della reputazione è un processo lungo e costoso, che spesso non può essere

recuperato nel breve periodo. L’immagine di un’organizzazione che ha subito un attacco informatico può risultare danneggiata anche a livello pubblico, con ripercussioni anche nelle future trattative commerciali.

3. **Implicazioni legali e regolatorie**

Le implicazioni legali degli attacchi informatici sono un'altra area critica per le organizzazioni. In molti casi, la mancata adozione di adeguate misure di sicurezza informatica può comportare sanzioni gravi da parte delle autorità di regolamentazione. Ad esempio, il GDPR (Regolamento Generale sulla Protezione dei Dati) prevede multe che possono raggiungere fino al 4% del fatturato annuale di un'organizzazione, se non vengono rispettati gli obblighi di protezione dei dati sensibili. Le aziende coinvolte in violazioni dei dati sono anche esposte a cause legali da parte dei consumatori danneggiati, con un potenziale aumento dei costi legali e dei risarcimenti.

4. **Interruzione delle attività aziendali**

Gli attacchi informatici possono causare interruzioni significative nelle operazioni quotidiane. Se i sistemi informatici sono compromessi, l'accesso ai dati e alle applicazioni critiche viene bloccato, paralizzando le attività aziendali. In alcuni casi, l’interruzione può durare giorni o addirittura settimane, con effetti disastrosi sulla capacità di servire i clienti e di generare introiti. Inoltre, l'interruzione di servizi fondamentali come il supporto al cliente o l'elaborazione degli ordini può portare a una perdita di fiducia nel brand, che a lungo termine si traduce in un calo delle vendite.

5. **Costi di ripristino e rafforzamento della sicurezza**

Dopo un attacco informatico, è necessario affrontare un lungo processo di recupero. Le organizzazioni devono investire risorse considerevoli in indagini forensi per identificare la causa e l'origine dell'attacco. Una volta compresa la natura della violazione, è essenziale adottare nuove misure di protezione per evitare futuri attacchi, che possono comportare significativi investimenti in software di sicurezza, hardware, e consulenze specializzate. Inoltre, la formazione continua del personale diventa cruciale per sensibilizzare i dipendenti su come riconoscere le minacce e adottare pratiche sicure. L'attuazione di un piano di risposta agli incidenti e di gestione della sicurezza deve essere rapida e decisa, per evitare che il danno diventi sistematico e irreversibile.

Capitolo 2 – Normative di riferimento

1. GDPR e protezione dei dati

Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** è la normativa europea che regola la protezione dei dati personali e la privacy dei cittadini all'interno dell'Unione Europea. È entrato in vigore nel maggio 2018 e ha introdotto cambiamenti significativi nel trattamento dei dati da parte delle aziende.[1]

Principali disposizioni del GDPR:

1. **Licenza per il trattamento dei dati**: le aziende devono trattare i dati solo se hanno una base legale, come il consenso esplicito dell'interessato, l'esecuzione di un contratto, o motivi di interesse legittimo.
2. **Diritti degli interessati**: i cittadini hanno diritti specifici, tra cui il diritto di accesso ai propri dati, il diritto di rettifica, il diritto all'oblio (cancellazione), e il diritto di portabilità dei dati.
3. **Trasparenza**: le aziende devono informare in modo chiaro e comprensibile gli utenti su come e perché i loro dati vengono trattati.
4. **Misure di sicurezza**: le organizzazioni devono adottare adeguate misure tecniche e organizzative per proteggere i dati da rischi di perdita, accesso non autorizzato o divulgazione.
5. **Data Protection Officer (DPO)**: le aziende che trattano grandi quantità di dati personali o dati sensibili devono nominare un responsabile della protezione dei dati.
6. **Sanzioni**: in caso di violazioni, le aziende possono essere multate fino al 4% del loro fatturato annuo globale, o 20 milioni di euro, a seconda di quale sia il valore più alto.

Il GDPR ha come obiettivo quello di proteggere i diritti e le libertà degli individui in relazione al trattamento dei loro dati personali, promuovendo al contempo la fiducia tra utenti e aziende.

2. ISO/IEC 27001 e standard internazionali

L'**ISO/IEC 27001** è uno degli standard più noti per la gestione della sicurezza delle informazioni, che stabilisce i requisiti per implementare, mantenere e migliorare un **Sistema di Gestione della Sicurezza delle Informazioni** (ISMS). Questo standard aiuta le aziende a **identificare e gestire i rischi legati alla sicurezza delle informazioni**, proteggendo i dati sensibili da accessi non autorizzati, danneggiamenti o perdite.[2]

Gli elementi chiave dell'ISO/IEC 27001 includono:

1. **Identificazione e valutazione dei rischi**: le aziende devono comprendere quali sono i rischi per la sicurezza delle informazioni e stabilire un piano di gestione adeguato.
2. **Politiche di sicurezza**: devono essere sviluppate politiche che definiscono le linee guida per la gestione dei dati e delle informazioni all'interno dell'organizzazione.
3. **Controlli di sicurezza**: devono essere implementati controlli tecnici, fisici e organizzativi per proteggere le informazioni.
4. **Monitoraggio e miglioramento continuo**: l'azienda deve continuamente monitorare l'efficacia del sistema di gestione della sicurezza e migliorarlo, implementando azioni correttive e preventive.
5. **Audit interni**: periodici audit interni sono necessari per garantire che l'ISMS funzioni correttamente e sia conforme agli standard.

[1] GDPR (Regolamento UE 2016/679)

Oltre all'ISO/IEC 27001, esistono altre normative internazionali correlate, come l'ISO/IEC 27002, che fornisce linee guida per i controlli di sicurezza, e l'ISO/IEC 27005, che si concentra sulla gestione del rischio in ambito IT.[3]

3. **Direttiva NIS2 e regolamenti di settore**

La **Direttiva NIS2** (Network and Information Systems Directive) è un aggiornamento della precedente Direttiva NIS, adottata dalla Commissione Europea nel dicembre 2020, che mira a migliorare la sicurezza dei **sistemi informativi e delle reti** in tutta l'UE. La NIS2 stabilisce requisiti più stringenti per le **organizzazioni che gestiscono servizi essenziali** o forniscono **infrastrutture critiche**, come l'energia, i trasporti, la sanità, e i servizi digitali.[4]

I punti principali della Direttiva NIS2 includono:

1. **Maggiori obblighi di sicurezza**: le organizzazioni devono adottare misure di sicurezza avanzate per proteggere le proprie infrastrutture critiche.
2. **Segnalazione obbligatoria degli incidenti**: qualsiasi incidente grave che influenzi la sicurezza dei sistemi deve essere segnalato alle autorità competenti entro 24 ore.
3. **Gestione del rischio**: le organizzazioni devono identificare e mitigare i rischi legati alla sicurezza informatica attraverso strategie e politiche adeguate.
4. **Cooperazione tra stati membri**: la NIS2 promuove la cooperazione tra i paesi dell'UE, assicurando che le risorse e le informazioni sulla sicurezza siano condivise.
5. **Sanzioni per inadempimento**: le aziende che non rispettano i requisiti della Direttiva NIS2 possono essere soggette a sanzioni severe.

Oltre alla Direttiva NIS2, vari settori specifici hanno regolamenti dedicati per la sicurezza informatica. Ad esempio, nel settore bancario e finanziario, c'è la direttiva PSD2, che riguarda la sicurezza dei pagamenti elettronici, mentre nel settore sanitario ci sono normative come l'Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti, che regolano la protezione dei dati sanitari sensibili.

4. **NIST**

Il NIST (National Institute of Standards and Technology) è un'agenzia federale statunitense, essa fa parte del Dipartimento del Commercio, che si occupa di sviluppare e promuovere standard, tecnologie, metodologie e pratiche migliori in numerosi settori industriali e scientifici. Fondata nel 1901, la sua missione è quella di migliorare la qualità e la competitività dei prodotti e dei servizi negli Stati Uniti e a livello globale, garantendo al contempo la sicurezza e la protezione dei dati, dei sistemi e delle infrastrutture critiche.

I principali ambiti di Intervento del NIST sono:

1. Sicurezza Informatica

Il NIST ha un ruolo fondamentale nella sicurezza informatica e nella gestione dei rischi tecnologici. Una delle sue principali iniziative è il Cybersecurity Framework, creato per aiutare le organizzazioni a identificare, proteggere, rilevare, rispondere e recuperare in caso di minacce informatiche. Questo framework è utilizzato sia a livello pubblico che privato, ed è ampiamente adottato da enti governativi, aziende e istituzioni. Il NIST sviluppa anche numerosi documenti e linee guida, tra cui la serie SP 800, che copre aspetti cruciali come la gestione dei rischi, la protezione dei dati e la conformità agli standard di sicurezza.

[3] Sicurezza delle informazioni - Edizione 2022: Gestione del rischio - I sistemi di gestione - La ISO/IEC 27001:2022 - I controlli della ISO/IEC 27002:2022 - Cesare Gallotti.
[4] NIS2

Tra le pubblicazioni più rilevanti c'è SP 800-53, che fornisce un set completo di controlli di sicurezza per proteggere i sistemi informatici, e SP 800-171, che definisce i requisiti di sicurezza per proteggere le informazioni sensibili non classificate in ambienti federali.

2. **Metrologia e Standard di Misura**

Un altro ambito di intervento cruciale del NIST riguarda la metrologia, ovvero la scienza delle misurazioni. Il NIST è responsabile della definizione degli standard di misura negli Stati Uniti e gioca un ruolo centrale nel Sistema Internazionale di Unità (SI), garantendo la precisione e l'affidabilità delle misurazioni scientifiche e industriali. Questo implica la calibrazione di strumenti di misura, l'adozione di metodi per ridurre gli errori di misurazione e la gestione di laboratori di riferimento.

3. **Tecnologia e Innovazione**

Il NIST svolge un ruolo chiave anche nello sviluppo e nell'adozione di tecnologie emergenti. Collabora con l'industria e la comunità scientifica per promuovere l'innovazione in vari settori tecnologici. Tra le aree di ricerca di punta vi sono la computazione quantistica, l'intelligenza artificiale (IA), e le reti 5G. Il NIST supporta la creazione di standard per queste tecnologie emergenti, cercando di garantire la loro sicurezza e l'efficienza operativa.

4. **Certificazione e Conformità**

Il NIST è anche un punto di riferimento per la certificazione di sistemi e conformità agli standard di sicurezza. Le sue pubblicazioni, come i FIPS (Federal Information Processing Standards), stabiliscono requisiti minimi di sicurezza per i sistemi informatici utilizzati dalle agenzie federali degli Stati Uniti, ma sono anche adottate da organizzazioni private e internazionali. Ad esempio, i FIPS sono fondamentali per la gestione delle chiavi crittografiche e la protezione dei dati sensibili.

Il NIST offre anche linee guida su come implementare controlli di sicurezza, migliorare la resilienza dei sistemi e proteggere le infrastrutture critiche da attacchi informatici e disastri naturali.

Gli standard e le linee guida del NIST vengono adottati da organizzazioni e governi di tutto il mondo. Per esempio, il NIST Cybersecurity Framework è diventato uno degli standard più diffusi per la gestione dei rischi informatici, non solo negli Stati Uniti, ma anche in Europa e in Asia.[5]

[5] NIST

Capitolo 3 - Calcolo del Fattore di Rischio

Importanza del calcolo del rischio

Il calcolo del **fattore di rischio** è essenziale per garantire una gestione efficace della sicurezza e ridurre al minimo le potenziali minacce, esso si basa su due fattori principali: la probabilità che una minaccia si verifichi e l'impatto che potrebbe avere nel caso si concretizzi. L'obiettivo è ottenere un valore numerico che aiuti a capire quali rischi meritano maggiore attenzione. In questo modo, si possono allocare le risorse di sicurezza in modo più mirato, affrontando prima le minacce più gravi e urgenti.[6]

1. Formule e metodologie di analisi

Formula del Rischio

Il calcolo del rischio può essere eseguito utilizzando la seguente formula:

$$R = P \times I \times V$$

Dove:

- R è il rischio informatico.
- P è la probabilità che una minaccia si verifichi.
- I è l'impatto di tale minaccia.
- V è la vulnerabilità dei sistemi.

2. Metodologie di Calcolo del Rischio

Metodologia OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) è una metodologia di gestione del rischio che si concentra sull'identificazione e sulla gestione dei rischi relativi agli asset critici, alle minacce e alle vulnerabilità di un'organizzazione. Questo approccio qualitativo consente di valutare in modo sistematico il rischio, considerando gli aspetti operativi e la sicurezza informatica.

Le fasi principali di OCTAVE sono:

1. **Identificazione degli asset critici**: Determinare quali sono i beni aziendali più rilevanti da proteggere.
2. **Identificazione delle minacce**: Elencare le minacce che potrebbero compromettere gli asset identificati.
3. **Analisi delle vulnerabilità**: Rilevare le debolezze presenti nei sistemi che potrebbero essere sfruttate dalle minacce.
4. **Valutazione del rischio**: Combinare la probabilità e l'impatto delle minacce e vulnerabilità per determinare il livello di rischio.[7]

Metodologia FAIR

FAIR (Factor Analysis of Information Risk) è un framework quantitativo che consente di valutare il rischio finanziario, piuttosto che solo il rischio operativo. Questa metodologia si basa su calcoli

6 Sicurezza delle informazioni - Edizione 2022 - Cesare Gallotti
[7]OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

statistici per determinare la probabilità e l'impatto, in particolare in termini economici, di un evento dannoso.

Le fasi di FAIR comprendono:

1. **Identificazione del rischio**: Determinare la natura della minaccia e della vulnerabilità.
2. **Quantificazione del rischio**: Stimare la probabilità dell'evento dannoso e la perdita economica potenziale.
3. **Calcolo della perdita attesa**: Moltiplicare la probabilità dell'evento per la perdita economica media per determinare il rischio finanziario complessivo.[8]

ISO 31000:2018

ISO 31000 è uno standard internazionale che fornisce linee guida generali per la gestione del rischio in qualsiasi contesto. In ambito informatico, la gestione del rischio include l'identificazione, la valutazione, e la risposta ai rischi.

Le fasi di gestione del rischio secondo ISO 31000 sono:

a. **Contesto**: Definizione del contesto in cui si opera.
b. **Identificazione**: Identificazione delle minacce e vulnerabilità.
c. **Valutazione**: Calcolo della probabilità e dell'impatto.
d. **Trattamento del rischio**: Definizione di misure di mitigazione.
e. **Monitoraggio**: Controllo continuo delle vulnerabilità.

3. Applicazione Pratica del Calcolo del Rischio

L'esecuzione di un'analisi di rischio pratica richiede l'impiego di metodologie e strumenti tecnici avanzati. In questa sezione, verrà illustrato il processo passo dopo passo, applicandolo a casi reali per dimostrare in modo concreto come viene eseguita la valutazione completa del rischio.

Fase 1: Identificazione degli Asset

Il primo passo è identificare gli **asset** critici dell'organizzazione, che potrebbero includere dati sensibili, infrastrutture tecnologiche, applicazioni aziendali e risorse umane. Un'azienda che gestisce dati finanziari, ad esempio, dovrà concentrare l'analisi sul rischio di violazione della privacy di questi dati.

Fase 2: Identificazione delle Minacce

Le minacce rappresentano eventi esterni o interni che potrebbero compromettere gli asset aziendali. Le minacce comuni includono:

- **Attacchi informatici** (phishing, ransomware, hacking)
- **Errori umani** (incidenti causati da disattenzione o negligenza)
- **Malfunzionamenti tecnici** (guasti hardware o software)

[8] FAIR (Factor Analysis of Information Risk)

Fase 3: Valutazione della Probabilità e dell'Impatto

Dopo aver identificato le minacce, è necessario valutare la **probabilità** che si verifichino e l'**impatto** che causerebbero. In questa fase, la metodologia **FAIR** è molto utile, poiché permette di stimare quantitativamente la probabilità e l'impatto delle minacce.

- **Probabilità**: Quanto è probabile che una minaccia si realizzi? Ad esempio, un attacco ransomware potrebbe essere considerato ad alta probabilità se i sistemi non sono aggiornati.
- **Impatto**: Quanto grave sarebbe l'evento? La perdita di dati sensibili, per esempio, potrebbe comportare danni legali e reputazionali gravi.

Fase 4: Applicazione nel caso reale

Dopo aver identificato gli asset, le minacce, e aver valutato la probabilità e l'impatto, possiamo applicare la metodologia di calcolo del rischio a dei casi di aziende reali.

Primo caso Fastweb - Attacco DDoS (Distributed Denial of Service)

Fastweb, uno dei principali operatori di telecomunicazioni in Italia, potrebbe dunque essere vulnerabile agli attacchi **DDoS** (Denial of Service), che mirano a sovraccaricare i server dell'azienda con un grande volume di traffico internet, impedendo agli utenti legittimi di accedere ai servizi.[9]

Applicazione della Formula del Rischio

- **Probabilità (P)**: Gli attacchi DDoS sono molto comuni nel settore delle telecomunicazioni. L'esperienza e i dati storici suggeriscono che Fastweb ha una probabilità del 70-80% di essere attaccata ogni anno. Pertanto, **P = 0.8**.
- **Impatto (I)**: L'impatto di un attacco DDoS su Fastweb include l'interruzione dei servizi, la perdita temporanea di clienti, il danno alla reputazione e l'eventuale perdita di ricavi. Poiché la disponibilità dei servizi è fondamentale per Fastweb, l'impatto potrebbe essere significativo, ma non catastrofico se l'azienda è pronta con misure di backup. Pertanto, **I = 0.7**.
- **Vulnerabilità (V)**: La vulnerabilità di Fastweb dipende dalla capacità dei suoi sistemi di resistere a un attacco DDoS. Se Fastweb non ha implementato misure di difesa adeguate, la vulnerabilità potrebbe essere alta. Se, tuttavia, sono in atto misure di difesa come l'uso di soluzioni anti-DDoS, la vulnerabilità potrebbe essere bassa. Supponiamo che Fastweb abbia una vulnerabilità media, **V = 0.6**.

$$R = P \times I \times V = 0.8 \times 0.7 \times 0.6 = 0.336$$

Il rischio calcolato è **0.336**, che indica un rischio **moderato-alto**. Questo significa che Fastweb deve prendere provvedimenti per ridurre il rischio, ad esempio aumentando la capacità di difesa contro gli attacchi DDoS e potenziando la resilienza dei suoi servizi.

Misure di Mitigazione

- **Mitigazione della probabilità (P)**: Migliorare i sistemi di rilevamento degli attacchi in tempo reale e diversificare le risorse di rete.
- **Mitigazione dell'impatto (I)**: Investire in **backup ridondanti** e infrastrutture scalabili per garantire che i servizi possano rimanere online anche durante gli attacchi.

[9] Fastweb

- **Mitigazione della vulnerabilità (V)**: Aumentare la protezione dei server con tecnologie avanzate di **anti-DDoS** e **content delivery network (CDN)**.

La probabilità di attacchi DDoS è alta per un'azienda come Fastweb, e l'impatto di tali attacchi potrebbe essere significativo. Utilizzando **FAIR**, possiamo calcolare con maggiore precisione la probabilità di incorrere in un attacco DDoS e l'entità della perdita economica in caso di disservizio.

OCTAVE aiuta a valutare l'importanza degli asset critici (come le reti e i dati degli utenti) e ad analizzare le vulnerabilità interne ed esterne, come l'accesso non autorizzato o le interruzioni di servizio.

Applicazione delle normative

Le normative e i framework sono essenziali per gestire i rischi in modo conforme alle leggi e agli standard internazionali. Per Fastweb, i principali riferimenti da seguire sono:

1. **GDPR (General Data Protection Regulation)**: Fastweb deve trattare i dati personali degli utenti rispettando il GDPR, usando misure come la crittografia e la gestione dei consensi per proteggere i dati sensibili.
2. **ISO/IEC 27001**: Fastweb deve seguire questa norma per gestire la sicurezza delle informazioni. Ciò significa adottare un sistema per proteggere i dati e fare controlli regolari per identificare e ridurre i rischi informatici.
3. **NIST (National Institute of Standards and Technology)**: Questo framework aiuta Fastweb a strutturare la gestione dei rischi informatici, migliorando la protezione dei dati e la risposta agli attacchi.
4. **Direttiva NIS2**: Essendo un operatore di infrastrutture critiche, Fastweb deve seguire la direttiva NIS2, che richiede misure di sicurezza più forti e una risposta rapida in caso di incidenti informatici per proteggere i sistemi cruciali.

Adottare queste normative e framework aiuta Fastweb a gestire i rischi e a garantire la sicurezza dei dati e delle informazioni.

Secondo caso UniCredit - Attacco Ransomware

UniCredit, una delle principali banche in Italia e in Europa, potrebbe essere colpita da un attacco **ransomware**, dove i criminali informatici bloccano l'accesso ai dati sensibili della banca e chiedono un riscatto per il rilascio.[10]

Applicazione della Formula del Rischio

- **Probabilità (P)**: Gli attacchi ransomware sono comuni nel settore bancario e la probabilità che UniCredit sia attaccata è abbastanza alta. Poiché l'industria bancaria è un obiettivo primario per i criminali informatici, supponiamo che la probabilità di attacco sia **P = 0.7**.
- **Impatto (I)**: L'impatto di un attacco ransomware per una banca è elevato. La perdita di dati sensibili dei clienti, la sospensione dei servizi bancari, il danno economico e la possibile multa per violazione della sicurezza sono tutte conseguenze gravi. Pertanto, l'impatto sarà valutato come **I = 0.9**.
- **Vulnerabilità (V)**: UniCredit ha probabilmente una vulnerabilità relativamente bassa, poiché la banca utilizza misure avanzate di protezione come crittografia dei dati e soluzioni antivirus. Tuttavia, la vulnerabilità potrebbe essere aumentata dalla possibilità di attacchi tramite **phishing** o altri vettori non tecnici. Pertanto, la vulnerabilità potrebbe essere **V = 0.7**.

[10] Unicredit

$$R = P \times I \times V = 0.7 \times 0.9 \times 0.7 = 0.441$$

Il rischio calcolato è **0.441**, che rappresenta un rischio **alto**. Questo significa che UniCredit deve investire maggiormente nella protezione contro gli attacchi ransomware.

- **Mitigazione della probabilità (P)**: Sensibilizzare i dipendenti sui rischi di **phishing** e implementare filtri avanzati per le email.
- **Mitigazione dell'impatto (I)**: Implementare sistemi di **backup regolari** e **disaster recovery** per recuperare rapidamente i dati critici.
- **Mitigazione della vulnerabilità (V)**: Aumentare la protezione contro l'accesso non autorizzato e migliorare la formazione dei dipendenti sulla sicurezza informatica.

Applicazione delle Metodologie

Con **FAIR** in Unicredit, si potrebbe calcolare la probabilità di attacchi ransomware, analizzando quante volte questo tipo di attacco si verifica nel settore bancario e quale potrebbe essere l'impatto economico (inclusi i costi per il recupero dei dati e le perdite reputazionali).

Utilizzando **OCTAVE**, è possibile determinare le minacce più rilevanti, come attacchi ransomware e frodi bancarie, e definire le misure di protezione necessarie per evitare che queste minacce compromettano la sicurezza dei dati bancari e la continuità dei servizi.

Applicazione delle normative

L'applicazione delle normative e dei framework è essenziale per garantire una gestione adeguata del rischio e la protezione delle informazioni. Per UniCredit, le principali normative di riferimento sono:

1. **GDPR**: UniCredit deve trattare i dati personali in conformità con il GDPR, implementando misure di protezione come la crittografia e politiche di gestione dei consensi per prevenire la perdita o il furto di dati sensibili.
2. **ISO/IEC 27001**: L'adozione di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) consente a UniCredit di gestire efficacemente i rischi informatici e proteggere le informazioni, attraverso controlli specifici e audit periodici.
3. **NIST**: Il framework NIST fornisce una guida strutturata per la gestione del rischio informatico, che UniCredit può applicare per migliorare le proprie capacità di protezione, rilevamento e risposta agli incidenti.
4. **Direttiva NIS2**: UniCredit, in quanto fornitore di servizi essenziali, è obbligata a seguire le disposizioni della NIS2 per garantire la sicurezza dei propri sistemi bancari, notificando tempestivamente agli enti competenti in caso di incidenti informatici.

L'adozione di queste normative assicura a UniCredit una gestione conforme e sicura dei dati, riducendo il rischio di incidenti informatici e migliorando la resilienza operativa.

Conclusioni

L'obiettivo della guida è fornire una comprensione approfondita del calcolo del fattore di rischio, esaminando il quadro normativo e proponendo metodologie pratiche e applicabili.

Il metodo adottato integra parametri quantitativi e qualitativi, offrendo una valutazione rigorosa ma adattabile. Durante lo sviluppo, si è puntato sulla chiarezza e usabilità, bilanciando precisione tecnica e semplicità d'uso per garantire un supporto efficace.

Per il download del documento è stata realizzata una pagina web utilizzando HTML e CSS.

In futuro, il modello potrebbe evolversi con strumenti automatici per l'analisi dei dati e una piattaforma interattiva.

La sicurezza non deve essere considerata come un traguardo finale, ma come un processo che si evolve all'evolversi delle minacce.

Security is a process, not a product *– Bruce Schneier*