INDICE

1. Traccia - Analisi del rischio

Un'azienda di servizi cloud è esposta al rischio di violazione dei dati a causa di vulnerabilità nel software e nelle configurazioni di sicurezza. L'azienda stima che la probabilità di un incidente di questo tipo sia del 70%. Una violazione dei dati potrebbe portare a perdite finanziarie dovute a sanzioni normative, risarcimenti ai clienti e danni reputazionali. Sulla base delle stime, una singola violazione dei dati potrebbe costare all'azienda circa **5 milioni di euro**. Inoltre, l'azienda prevede che un incidente simile possa verificarsi in media **due volte all'anno**. Il fatturato annuale dell'azienda è di 200 milioni di euro.

Svolgere un'**analisi del rischio semi-quantitativa**, utilizzando il processo semplificato visto a lezione, **tabelle G-4/H-3/1-2 NIST SP 800-30 Rev. 1**, Guide for Conducting Risk Assessments, https://csrc.nist.gov/pubs/sp/800/30/r1/final

Creare un report in cui descrivere i passaggi svolti per l'analisi.

2. Analisi semi-quantitativa del rischio

I metodi semi-quantitativi, si basano su metodi quantitativi ma con un approccio semplificato, i dati a disposizione sono quelli rilevati al momento dell'indagine e i parametri di confronto sono determinati da standard o regolamentazioni.
L'analisi del rischio semi-quantitativa è un metodo per valutare i rischi che combina elementi qualitativi e quantitativi. Solitamente si parte da rilevazioni che permettono di definire valori oggettivi di verosomiglianza, impatto e rischio (analisi quantitativa) per poi utilizzare metodi dell'analisi qualitativa per ottenere una relazione con standard e/o regolamentazioni. Come nel nostro caso.
Alternativamente, si possono definire valori numerici di verosomiglianza, impatto e rischio in modo soggettivo, avvicinandosi maggiormente all'analisi qualitativa così da sfruttare metodi matematici per poter effettuare operazioni tra valori (es. valore min/max, media, moltiplicazione, differenza) e trarre conclusioni o relazionarsi sempre con standard e/o regolamentazioni.
Questo metodo combina quindi elementi quantitativi e qualitativi, permettendo una stima più precisa del rischio basata su probabilità di eventi e potenziali impatti finanziari. Sono state utilizzate le tabelle G-4, H-3 e I-2 per classificare e valutare i rischi in maniera strutturata. L'analisi è stata eseguita considerando sia la probabilità di occorrenza degli incidenti di sicurezza sia il loro impatto finanziario sull’organizzazione.

Elementi quantitativi

Calcolo quantitativo del rischio basato sul fatturato annuale dell'azienda

Nell'analisi quantitativa sono utilizzate principalmente due metriche:
SLE (Single Loss Expectancy), rappresenta la perdita stimata per un singolo evento.
ALE (Annual Loss Expectancy), rappresenta la perdita stimata per un evento specifico in un anno.

SLE
AV: Asset Value, valore monetario dell'asset = 5.000.000 €
EF: Exposure Factor, indice che serve a misurare il livello di danno o l'impatto provocato da un evento dannoso su un singolo asset. Questo viene espresso sotto forma di una percentuale, compresa tra 0% e 100% del valore dell'asset colpito dalla minaccia. Il valore 100% indica la distruzione completa dell'asset.
EF (Exposure Factor) = 1

Una singola violazione dei dati comporta per l'azienda un costo di 5 milioni, il quale rappresenta la perdita stimata per la verificazione di un singolo evento, ovvero la Single Loss Expectancy (SLE).
SLE = AV • EF
SLE = 5.000.000 • 1 = 5.000.000€/attacco

Annualized Loss Expectancy (ALE)
ALE è la perdita attesa (potenziale) stimata su base annua, associata ad una specifica minaccia e derivante dalla verificazione della violazione dei dati. Per calcolarlo dobbiamo conoscere SLE e ARO (Annualized Rate of Occurrence).
ARO: Annualized Rate of Occurrence, tasso del numero di volte che una minaccia si verifica nell'arco di un anno.
2 volte all'anno: ARO = 2/1 = 2

A questo punto si calcola:
ALE = SLE·ARO
ALE = 5.000.000 • 2 = 10.000.000€/anno

Fatturato = 200.000.000€/anno

Impatto finanziario (I) = ALE / Fatturato annuo
I = 10.000.000 / 200.000.000 = 0,05

Quindi la perdita economica stimata dovuta alla violazione dei dati è del **5%** rispetto al fatturato annuo dell'azienda.

Elementi qualitativi

L'analisi qualitativa del rischio si concentra su valutazioni soggettive, anche in assenza di dati quantitativi accurati. Utile quando i fattori di rischio sono difficilmente quantificabili come il danno reputazionale o la perdita di fiducia dei clienti). Si basa quindi su esperienza, conoscenza di settore, e fattori interni ed esterni. Richiede meno risorse rispetto all'analisi quantitativa.

Per l'analisi qualitativa possono essere utilizzati:
- Scale di valutazione (es.: Bassa, Media, Alta)
- Sondaggi e raccolta di opinioni di esperti
- Analisi di trend storici

Scale di valutazione qualitative
Si possono usare scale come quella di Likert (da 1=Molto Basso a 5=Molto Alto). E' importante definire la relazione tra i valori qualitativi assegnati.
Il rischio è stimato come relazione tra la **stima della verosomiglianza** e la **stima dell'impatto.**
Solitamente si utilizzano standard o framework come riferimento.

Calcoliamo il rischio associato alla minaccia:
R (Rischio) = P (probabilità) · I (Impatto)
P = 70%
R = 0,7 • 0.05 = **0,035**

Per l'analisi del rischio, è stato adottato un approccio semi-quantitativo seguendo le linee guida del **NIST SP 800-30 Rev. 1**., Guide for Conducting Risk Assessments e utilizzando le seguenti tabelle per categorizzare e valutare i rischi:
- tabella G-4: viene utilizzata per valutare la verosomiglianza di un evento rischioso basandosi su dati storici e scenari ipotetici.
- tabella H-3: aiuta a determinare l'impatto finanziario di una violazione dei dati, considerando vari fattori come perdite dirette, sanzioni e danni reputazionali.
- tabella I-2: utilizzata per combinare le informazioni di probabilità e impatto per arrivare a una valutazione complessiva del rischio.

Valutazione della probabilità/verosomiglianza
TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Questa tabella fornisce una scala di valutazione per determinare la probabilità che un evento avverso possa provocare impatti negativi sull'organizzazione. Questa scala aiuta a quantificare la verosomiglianza di un evento minaccioso che si traduce in conseguenze avverse. Consideriamo quindi, il valore di verosomiglianza dell'evento nel nostro caso:
V = 70%

Valutazione dell'impatto
TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

La tabella contiene una scala di valutazione per determinare l'impatto degli eventi minacciosi sull'organizzazione. Questa scala aiuta a valutare la **gravità delle conseguenze** di un evento avverso, consentendo di comprendere l'entità degli impatti che potrebbero verificarsi. Consideriamo il valore dell'Impatto calcolato precedentemente:
I = 5%

Valutazione del Rischio
TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

La tabella fornisce una scala di valutazione per determinare il livello complessivo di rischio associato a un particolare evento avverso. Questa scala combina le scale dei valori qualitativi della probabilità che l'evento si verifichi e determini un impatto avverso (Likelihood) con i valori della gravità dell'impatto (Impact) per individuare il livello del **rischio qualitativo**.

3. Conclusioni

La perdita economica stimata dovuta alla violazione dei dati è del **5%** rispetto al fatturato annuo dell'azienda. Inoltre dopo l'analisi semi-quantitativa svolta abbiamo identificato il rischio qualitativo come "Low" ma è necessario considerare anche altri fattori come il danno reputazionale, la perdita di fiducia o engagement che l'inefficacia della protezione dei dati potrebbe creare in acquirenti e stakeholder.