Analisi del rischio

Traccia

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.

1. Svolgere un'analisi del rischio semi-quantitativa, utilizzando il processo semplificato visto a lezione, tabelle G-4/H-3/I-2 NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, https://csrc.nist.gov/pubs/sp/800/30/r1/final
2. Creare un report in cui descrivere i passaggi svolti per l'analisi.

Traccia 1

SLE = 5.000.000€

ARO = 2

ALE = 5.000.000€ * 2 = 10.000.000€

Fatturato Annuale = 200.000.000€

I = 10.000.000 / 200.000.000 = 0,05

V = 70%

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.

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.

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

Traccia 2

1. Prendiamo la SLE (Single Loss Expectancy), ovvero la perdita stimata per un singolo evento, fornitaci nella traccia, equivalente a 5.000.000€
2. Prendiamo l'ARO (Annualized Rate of Occurrence), ovvero il numero delle volte che una minaccia si verifica durante l'anno, fornitaci nella traccia, equivalente a 2
3. Calcoliamo l'ALE (Annualized Loss Expectancy), ovvero la potenziale perdita attesa su base annua associata ad una specifica minaccia, moltiplicando la SLE per l'ARO
4. Prendiamo il fatturato annuo, fornitoci nella traccia, equivalente a 200.000.000€
5. Calcoliamo l'I (Impatto) dividendo l'ALE per il fatturato annuo
6. Prendiamo la V (Verosomiglianza) che ci viene fornita nella traccia, equivalente al 70%
7. Prendiamo il valore corrispondente alla V nella tabella G-4 del NIST SP 800-30 Rev. 1, equivalente a Moderate
8. Prendiamo il valore corrispondente alla I nella tabella H-3 4 del NIST SP 800-30 Rev. 1, equivalente a Very Low
9. Incrociamo i valori trovati precedentemente nella tabella I-2 del NIST SP 800-30 Rev.1 e otteniamo il livello di rischio finale che equivale a Very Low