DIGITAL RISK MANAGER - ALEX FIORILLO

RISK MANAGEMENT
ANALISI DEL RISCHIO

INTRODUZIONE

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/I-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.

ANALISI SEMI-QUANTITATIVA DEL RISCHIO

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 verosimiglianza, impatto e rischio (analisi quantitativa) per poi utilizzare metodi dell'analisi qualitativa per ottenere una relazione con standard e/o regolamentazioni.

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.

ANALISI QUANTITATIVA DEL RISCHIO

L'analisi quantitativa del rischio utilizza valori numerici concreti (oggettivi) e statistiche per calcolare la probabilità e l'impatto di un evento negativo.

Si utilizzano valori monetari, dati statistici e altri elementi quantificabili per comprendere meglio la situazione.

La valutazione quantitativo del rischio segue uno schema ben preciso:

1. **Identificazione delle risorse:** elencare le risorse aziendali (include costo di sostituzione e fattori di esposizione);
2. **Calcolo dell'impatto:** stabilire la perdita potenziale in caso di danno totale o parziale della risorsa;
3. **Valutazione della probabilità:** determinare la possibilità che si verifichi l'evento negativo;
4. **Calcolo del rischio complessivo:** definire il rischio complessivo per l'organizzazione, espresso spesso in valore monetario.

Metriche dell'analisi quantitativa

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

Nel nostro caso siamo già a conoscenza del valore SLE che è pari a 5 milioni di €.
Sappiamo anche che secondo i dati a noi forniti l'evento l'evento occorre due volte l'anno (**ARO**, Annualized Rate of Occurence), quindi da questo possiamo calcolare il valore dell'ALE.

ARO: 2 volte ogni anno = 2 / 1 = **2**

L'ALE è calcolato moltiplicando l'SLE per ARO:

ALE = SLE * ARO
ALE = 5.000.000 * 2 = 10.000.000€

Con questi nuovi dati, conoscendo già il fatturato dell'azienda (200 milioni di €/anno), siamo in grado di calcolare anche l'impatto.

Impatto = ALE / FATTURATO ANNUO = 10.000.000 / 200.000.000 = 0,05

In base a questo calcolo abbiamo stimato che l'impatto equivale al 5% del fatturato annuo.

STIMA DELLA VEROSOMIGLIANZA

Secondo la tabella G-4 del NIST SP 800-30 Rev. 1 il valore semi-quantitativo della verosomiglianza è del 70% e corrisponde al valore quantitativo **moderato**.

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.

STIMA DELL'IMPATTO

Secondo la tabella H-3 del NIST SP 800-30 Rev. 1 il valore qualitativo dell'impatto corrispondente a quello semi-quantitativo (individuato in precedenza, al 5%) ci permette di classificarlo **low**.

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.

STIMA DEL RISCHIO

Combinando le valutazioni quantitative e semi-quantitative della verosomiglianza e dell'impatto siamo in grado di classificare il nostro rischio come **low** (in accordo con la tabella I-2 del NIST SP 800-30 Rev. 1).

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