Davide Andreozzi

BCC – Risk Management

S01 – L04

Esercizio – 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.

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.

Agenda

1) Identificazione e stime quantitative di un potenziale rischio
2) Stima della verosomiglianza
3) Stima dell’impatto
4) Stima del rischio
5) Descrizione del rischio

1) Identificazione e stime quantitative di un potenziale rischio

- V = 70%
- Fatturato Annuo = **€ 200.000.000**
- SLE = **€ 5.000.000**
  - La SLE è la singola perdita dovuta al verificarsi di una determinata minaccia
- ARO = 2/1 = **2 attacchi/Anno**
  - L'ARO è la media con cui la minaccia si verifica annualmente
- ALE = 5MLN * 2 = **€ 10.000.000/Anno**
  - L'ALE è la perdita stimata annualmente al verificarsi delle minacce
- Impatto = 10.000.000/200.000.000*100 = **5 %**
  - L'impatto è il valore che identifica in termini economici quanto la minaccia incide sul fatturato annuo, possono essere quantificati anche ulteriori dati come il danno al brand, perdita di investitori, calo vendite, ecc.

2) Stima della verosomiglianza

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.

La probabilità del verificarsi dell'evento è del 70 % e presentiamo un rischio «Moderato», come indicato dalla tabella G-4

3) Stima dell'impatto

Il danno economico che gli eventi causerebbero all'azienda è di 10Mln, quindi il 5% del fatturato annuo.

Questo valore si classifica come «**Basso**» sulla scala di valutazione dell'impatto che hanno le minacce

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.

4) Stima del rischio

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

Il livello di rischio è dato dalla combinazione del livello di impatto e la probabilità che l'impatto si verifichi (verosimiglianza).
Ricapitolando, i valori per la nostra azienda sono:

- Verosimiglianza = *Moderate*
- Impatto = *Low*

Il livello di rischio dato dalla combinazione dei due valori precedenti sarà di «***Low***»

Successivamente andremo a vedere più nel dettaglio a cosa corrisponde il valore e come viene percepito.

5) Descrizione del rischio

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a 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	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

5) Descrizione del rischio

Dato il livello di rischio finale che abbiamo potuto vedere nella precedente slide come («**Low**»).

*Ci si può aspettare che un evento minaccioso abbia un effetto negativo **limitato** sulle operazioni organizzative, sugli asset organizzativi, sugli individui, su altre organizzazioni o sulla nazione.*

Questo suggerisce che le eventuali misure di sicurezza attuate hanno efficacemente mitigato il rischio, riducendo la probabilità e/o le conseguenze di eventi dannosi a un livello accettabile per l'azienda.

Tuttavia, è importante mantenere un monitoraggio alto per identificare eventuali cambiamenti nelle minacce o nelle vulnerabilità che potrebbero influenzare il livello di rischio.
Ad esempio fattori esterni, oppure valutare in maniera oggettiva il rischio che un determinato evento abbia sull'immagine dell'azienda.

La perdita di informazioni critiche in un'azienda che si occupa di servizi Cloud è fondamentalmente pericoloso per la sua reputazione in quanto l'asset esposto a minaccia è un **Asset principale** che riguarda il core business dell'azienda.