REPORT S1-L4

ANALISI DEL RISCHIO

Maria Flavia Minotti

Sommario

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.

Risk Analysis semi-quantitativa

La Skynet, azienda di servizi in cloud, richiede l'analisi semi-quantitativa del rischio di violazione dei dati cui è esposta a causa di vulnerabilità, debolezze, che affliggono il software e le configurazioni del sistema aziendale.
Si procede quindi alla suddetta analisi specificando che la metodologia semi-quantitativa consiste nel combinare un approccio quantitativo, basato su valori numeri concreti e oggettivi, e un approccio qualitativo, basato su valori soggettivi quali l'esperienza, conoscenza di settore, e fattori interni ed esterni nel rapporto con standard e regolamentazioni.
Questa tipologia di analisi consente di valutare in modo olistico il rischio della violazione dei dati poiché permette di integrare nel processo elementi difficilmente quantificabile come la reputazione dell'azienda lesa dall'evento dannoso.

Dati forniti dall'azienda

La Skynet fornisce una serie di informazioni preliminari che costituiranno la base dell'analisi:

- **Minaccia** = violazione dei dati
- **Vulnerabilità** = del software e della configurazione del sistema
- **Probabilità verificazione evento** = 70%
- **Costo di una singola violazione** = 5.000.000 € = **SLE**
- **Volte dell'evento in 1 anno** = 2 = **ARO**
- **Fatturato annuale azienda** = 200.000.000 €

Metriche Quantitative

I dati forniti dall'azienda rappresentano valori numerici concreti per cui si procede all'applicazione delle metriche dell'analisi quantitativa per effettuare, in seguito, le valutazioni qualitative.

Lo scopo è di determinare il livello di rischio cui è sottoposta l'azienda.
Il rischio è il risultato del calcolo della probabilità che l'evento/minaccia si verifichi (**P**) per l'impatto (danno) negativo che avrebbe su Skynet (**I**).
Di seguito una rappresentazione come formula:

$$\text{R (Rischio)} = \text{P (probabilità)} \cdot \text{I (Impatto)}$$

- L'azienda ci ha fornito la probabilità del 70% che la violazione dei dati si verifichi.
  Quindi, si può dire che:

  P = 70%

- Per quanto attiene al calcolo dell'impatto finanziario, si procede ad analizzare i dati ulteriormente forniti alla luce delle metriche quantitative.
  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). Quindi:

  $$\textbf{SLE} \text{ (Single Loss Expectancy)} = \textbf{AV} \cdot \textbf{EF}$$

  Laddove:

  AV (Asset Value) = 5.000.000 €

  EF (Exposure Factor) = 1

  SLE = 5.000.000€

- Procedendo nello stesso modo, l'azienda ha calcolato che tale violazione dei dati possa verificarsi 2 volte all'anno. Questo dato corrisponde al tasso del numero di volte che una minaccia si verifica nell'arco di un anno, ovvero l'Annualized Rate of Occurence (ARO). Quindi:

ARO (Annualized Rate of Occurence) = 2

- A questo punto si calcola l'ALE o Annual Loss Expectancy, ovvero la perdita potenziale stimata su base annua derivante dalla verificazione della violazione dei dati.
  Questa perdita è il prodotto del costo associato alla minaccia per il numero di volte in cui si prevede che la minaccia si verifichi in un anno. Quindi:

$$\mathrm{ALE} = \mathrm{SLE} \cdot \mathrm{ARO}$$

$$\mathrm{ALE} = 5.000.000€ \cdot 2$$

$$\mathbf{ALE = 10.000.000€}$$

In questo modo è possibile calcolare l'impatto finanziario sulla Skynet rapportando l'ALE, la perdita annuale associata all'evento dannoso, con il fatturato annuo della società di 200.000.000 €.
In questo modo si avrà:

$$\text{Impatto finanziario} = \mathrm{ALE} \div \text{Fatturato annuo}$$

$$\text{Impatto finanziario} = 10.000.000 \div 200.000.000$$

$$\mathbf{\text{Impatto finanziario} = 0{,}05}$$

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

Calcolo Quantitativo del rischio

Una volta determinato l'impatto finanziario, è possibile procedere al calcolo del rischio associato alla minaccia:

$$\mathbf{R\ (Rischio) = P\ (probabilità) \cdot I\ (Impatto)}$$

$$\mathrm{R} = (70\%) \cdot (5\%)$$

$$\mathrm{R} = 0{,}7 \cdot 0{,}05$$

$$\mathbf{R = 0{,}035}$$

In definitiva, il rischio che la minaccia si verifichi e provochi una perdita del 5% del fatturato annuo è stimato al **3,5%**.
Si tratta di una percentuale ridotta rispetto al fatturato annuale della Skynet ma, nonostante il rischio sia basso/moderato è necessario considerare il danno reputazionale e la perdita di fiducia che la notizia dell'inefficacia della protezione dei dati potrebbe generare in acquirenti e stakeholder.
La suddetta considerazione è sostenuta dalla considerazione del settore nel quale opera l'azienda, che in quanto vendor di servizi in cloud, potrebbe avere importanti ricadute a medio e lungo termini sulla competitività aziendale.

Metriche Qualitative

Una volta stimata la percentuale di rischio quantitativa si procede ad utilizzare metodi dell'analisi qualitativa per ottenere una relazione con standard e/o regolamentazioni.
Avendo già ottenuto il calcolo della probabilità (P), l'impatto finanziario (I) e il Rischio si procede ad applicare lo standard del **NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments,** facendo riferimento alle seguenti tabelle:

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

Contiene la scala di valori semi quantitativi rapportati a valori qualitativi per la valutazione della probabilità che un evento avverso intenzionale determini impatti avversi, diversi rispetto a quelli aspettati in quanto negativi.

N.B. I seguenti valori sono identici anche per le minacce che abbiano carattere **non-adversarial**, ovvero che non abbiano natura intenzionale come errori umani, incidenti o eventi naturali.

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

Contiene la scala di valori semi quantitativi rapportati a valori qualitativi per la valutazione della gravità degli impatti che si attendono dalla verificazione delle minacce.

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK

Combina le scale dei valori qualitativi della probabilità che l'evento si verifichi e determini un impatto avverso e con i valori della gravità dell'impatto per individuare il livello del rischio qualitativo, la cui descrizione si rintraccia nella **TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK.**

Valutazione della probabilità

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 che la minaccia dell'evento comporti impatti avversi nell'analisi semi-quantitativa è del 70%, di conseguenza in base alla tabella in figura il valore qualitativo è "**Moderate**": se la minaccia è inizializzata o si verifica è abbastanza probabile avere impatti avversi.

Valutazione dell'impatto

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.

L'impatto negativo che la violazione dei dati comporta per la Skynet è stato individuato con le metriche quantitative al 5% del fatturato annuale.
In base alla tabella di cui sopra il corrispondente valore qualitativo dell'impatto è "**Low**": Nonostante la Skynet perda, sulla base delle stime quantitative, 10.000.000 l'anno si tratta di un effetto avverso di portata limitata da un punto di vista finanziario.

Valutazione 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

La combinazione della probabilità, identificata come moderate, e l'impatto, identificato come low, fornisce un livello quantitativo del rischio a **"Low".**

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.

Il valore del rischio individuato con le metriche quantitative, di 3,5%, non corrisponde al livello del rischio individuato con le metriche qualitative.
Infatti secondo il metodo qualitativo il livello di rischio è basso, ha limitati impatti negativi e corrisponde ai valori da 5 a 20 del metodo semi-quantitativo. Diversamente il valore semi-qualitativo rientra tra 0 e 4, per cui dovrebbe corrispondere al livello "Very Low".

La discordanza potrebbe risiedere nell'errore a monte sui dati forniti dall'azienda oppure in un errore della traccia.