




REPORT S2-L2

Piani di trattamento del rischio

Maria Flavia Minotti



Traccia

Un'azienda subisce **6** data breach ogni **2** anni, in cui l'**80%** del contenuto viene esfiltrato per un valore complessivo del dataset di **100.000€**. L'attaccante riesce a portare a termine il data breach nel **90%** dei casi.

Calcolare:

- SLE
- ARO
- ALE
- GL

Per ogni soluzione, valutare:

- mALE
- CBA
- ROSI (con rapporto di mitigazione)
- mv (probabilità di riuscita dopo la mitigazione).

Utilizzare:

- $\lambda = ALE$
- $t = EF$

Valutare se il costo delle contromisure rientra nell'investimento consigliato da Gordon-Loeb

Soluzione	1	2	3	4	5
Mitigation ratio	50%	65%	43%	62%	80%
ACS	63000	70000	60000	69000	100000

Svolgimento

Nel presente report si procede all'analisi costi/benefici (CBA) per valutare la fattibilità e la convenienza economica di potenziali misure di mitigazione del rischio di data breach. Per ottenere la valutazione è necessario prima determinare alcuni valori dettati da metriche quantitative del rischio.

1) SLE (Single Loss Expectancy) = $AV \cdot EF$

Si tratta della perdita stimata per un singolo evento data breach ed è il prodotto dell' AV, il valore complessivo dell'asset, e dell'EF, la percentuale dell'asset esposto, colpito dalla minaccia.

$$Av = 100.000 \times 80\%(0,80) = 80.000€$$

AV (Asset Value) =

EF (Exposure Factor) = 80%

SLE = 80.000

2) ARO (Annualized Rate of Occurrence) = tasso di numero di volte che una minaccia si verifichi in 1 anno.

Numero di data breach ogni 2 anni: 6

Poiché l'ARO è calcolato su base annuale, allora:

ARO = Numero di eventi ÷ periodo di tempo in cui avvengono gli eventi.

$$ARO = 6 \div 2$$

$$ARO = 3$$

3) ALE (Annual Loss Expectancy) = SLE x ARO

L'ALE è perdita attesa (potenziale), su base annua, associata ad una specifica minaccia.

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.

ALE = Perdita monetaria stimata per un singolo evento x numero di volte dell'evento all'anno.

$$ALE = 80.000 \times 3 =$$

$$ALE = 240.000\text{€}$$

4) GL

Gordon-Loeb determina che l'investimento in sicurezza non dovrebbe eccedere il 37% delle perdite potenziali (**d**), mettendo in relazione il valore del sistema (**λ**), quanto i dati o il sistema è a rischio (**t**) e la probabilità di riuscita dell'attacco (**v**).

$$Investment = 0,37 \cdot d$$
$$d = \lambda \cdot t \cdot v$$

Per lo svolgimento del calcolo in esame avremmo dovuto avere il rischio calcolato come prodotto della probabilità di verifica della minaccia per l'impatto, calcolato dal fatturato totale ma non è così.

Quindi, l'esercizio di default afferma che:

$$\lambda = ALE$$

$$t = EF$$

$$v = 90\%$$

$$d = 240.000 \times 80\% (0,80) \times 90\% (0,90)$$

$$d = 172.800 \text{ €}$$

$$Investment = 0,37 (37\%) \times 172.800$$

$$Investment = 63.936\text{€}$$

Secondo Gordone Loeb, con una perdita stimata di 172.800€, l'investimento dell'azienda in sicurezza non dovrebbe superare i **63.936€**.

Ottenuti i dati sopracitati, si procede ad effettuare la valutazione di 5 soluzioni di mitigazione alla luce dei seguenti elementi, di cui si procede a fornire breve descrizione:

5) mALE : Mitigated Annual Loss Expectancy, ovvero la perdita annuale stimata per un evento specifico dopo l'applicazione di misure di mitigazione o di sicurezza. In altre parole, è la perdita attesa per un certo evento una volta che sono state implementate delle contromisure per ridurre il rischio.

Si calcola come prodotto dell' ALE (prior), cioè la perdita annuale stimata per un evento specifico prima delle misure di mitigazione per il complemento del fattore di esposizione (EF).

$$mALE = ALE (prior) \times (1 - MR) \text{ (mitigation ratio?)}$$

6) CBA : analisi costi-benefici utilizzata nella gestione del rischio per valutare la fattibilità e la convenienza economica di potenziali misure di mitigazione del rischio (controlli).

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

ACS: Annualized Cost of Safeguard, costo annuale della salvaguardia.

7) ROSI (con rapporto di mitigazione) : Return on Security Investment (ritorno sull'investimento in sicurezza) è l'indicatore per valutare la rendita dell'investimento in sicurezza.

$$\begin{aligned} \text{Rosi} &= (\text{Monetary loss reduction} - \text{Cost of the solution}) \div \text{Cost of the solution} = \\ &= [(ALE(prior) - ALE(post)) - ACS] \div ACS = \mathbf{CBA \div ACS} \end{aligned}$$

8) mv (probabilità di riuscita dopo la mitigazione).

Soluzione	1	2	3	4	5
Mitigation ratio	50%	65%	43%	62%	80%
ACS	63000	70000	60000	69000	100000

Soluzione 1

• mALE

$$mALE = ALE (prior) \times (1 - MR)$$

$$mALE = 240.000 \times (1 - 0.50)$$

$$mALE = 120.000\text{€}$$

Quindi la perdita attesa all'anno, a causa di un data breach, dopo aver la 1° soluzione è di **48.000€**.

• CBA

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

L'ALE dopo l'implementazione delle misure di sicurezza è uguale al mALE, poiché rappresenta la perdita annuale stimata dopo l'applicazione delle misure di mitigazione.

$$ALE (post) = mALE$$

$$CBA = 240.000 - 120.000 - 63.000$$

$$CBA = 57.000$$

- **ROSI**

$$\text{Rosi} = (\text{Monetary loss reduction} - \text{Cost of the solution}) \div \text{Cost of the solution} =$$

$$= [(ALE(prior) - ALE(post)) - ACS] \div ACS = CBA \div ACS$$

$$ROSI = [(240.000 - 120.000) - 63.000] \div 63.000 = 57.000 \div 63.000$$

$$ROSI = 0,90 = 90\%$$

La 1° soluzione di mitigazione restituisce un profitto dall'investimento del 90%. Il Rosi in questo è maggiore di 0 quindi il costo della salvaguardia è minore della perdita annuale, l'investimento è conveniente.

- **mv**

$$mv = v \times (1 - MR)$$

$$mv = 0,90 \times (1 - 0,50)$$

$$mv = 0,45 = 40\%$$

In questo modo, vediamo che la probabilità di riuscita dell'attacco dopo l'applicazione della misura di mitigazione è del **40%**.

Soluzione 2

- **mALE**

$$mALE = ALE (prior) \times (1 - MR)$$

$$mALE = 240.000 \times (1 - 0,65)$$

$$mALE = 84.000\text{€}$$

Quindi la perdita attesa all'anno, a causa di un data breach, dopo aver applicato la 2° soluzione di mitigazione è di **84.000€**.

- **CBA**

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

L'ALE dopo l'implementazione delle misure di sicurezza è uguale al mALE, poiché rappresenta la perdita annuale stimata dopo l'applicazione delle misure di mitigazione.

$$ALE (post) = mALE$$

$$CBA = 240.000 - 84.000 - 70.000$$

$$CBA = 86.000$$

- **ROSI**

Rosi = (Monetary loss reduction – Cost of the solution) ÷ Cost of the solution =

$$= [(ALE(prior) - ALE(post)) - ACS] \div ACS = \mathbf{CBA \div ACS}$$

$$ROSI = [(240.000 - 84.000) - 70.000] \div 70.000 = 86.000 \div 70.000$$

$$\mathbf{ROSI = 1,22 = 122\%}$$

La 2° soluzione di mitigazione restituisce un profitto dall'investimento del 122%. Il Rosi in questo è maggiore di 0 quindi il costo della salvaguardia è minore della perdita annuale, l'investimento è conveniente.

- **Mv (Verosimiglianza mirata)**

$$mv = v \times (1 - MR)$$

$$mv = 0,90 \times (1 - 0,65)$$

$$\mathbf{mv = 0,315 = 31,5\%}$$

In questo modo, vediamo che la probabilità di riuscita dell'attacco dopo l'applicazione della misura di mitigazione è del **31,5%**.

Soluzione 3

- **mALE**

$$mALE = ALE(prior) \times (1 - MR)$$

$$mALE = 240.000 \times (1 - 0.43)$$

$$\mathbf{mALE = 136.800\text{€}}$$

Quindi la perdita attesa all'anno, a causa di un data breach, dopo aver applicato la 3° soluzione di mitigazione è di **136.800€**.

- **CBA**

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

L'ALE dopo l'implementazione delle misure di sicurezza è uguale al mALE, poiché rappresenta la perdita annuale stimata dopo l'applicazione delle misure di mitigazione.

$$ALE(post) = mALE$$

$$CBA = 240.000 - 136.800 - 60.000$$

$$\mathbf{CBA = 43.200}$$

- **ROSI**

Rosi = (Monetary loss reduction – Cost of the solution) ÷ Cost of the solution =

$$= [(ALE(prior) - ALE(post)) - ACS] \div ACS = \mathbf{CBA \div ACS}$$

$$ROSI = [(240.000 - 136.800) - 60.000] \div 60.000 = 43.200 \div 60.000$$

$$\mathbf{ROSI = 0,72 = 72\%}$$

La 3° soluzione di mitigazione restituisce un profitto dall'investimento del 72%. Il Rosi in questo è maggiore di 0 quindi il costo della salvaguardia è minore della perdita annuale, l'investimento è conveniente.

- **Mv (Verosimiglianza mitigata)**

$$mv = v \times (1 - MR)$$

$$mv = 0,90 \times (1 - 0,43)$$

$$mv = 0,513 = 51,3\%$$

In questo modo, vediamo che la probabilità di riuscita dell'attacco dopo l'applicazione della misura di mitigazione è del **51,3%**.

Soluzione 4

- **mALE**

$$mALE = ALE(prior) \times (1 - MR)$$

$$mALE = 240.000 \times (1 - 0.62)$$

$$mALE = 91.200\text{€}$$

Quindi la perdita attesa all'anno, a causa di un data breach, dopo aver applicato la 1° soluzione di mitigazione è di **91.200€**.

- **CBA**

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

L'ALE dopo l'implementazione delle misure di sicurezza è uguale al mALE, poiché rappresenta la perdita annuale stimata dopo l'applicazione delle misure di mitigazione.

$$ALE(post) = mALE$$

$$CBA = 240.000 - 91.200 - 69.000$$

$$CBA = 79.800\text{€}$$

- **ROSI**

$$Rosi = (Monetary\ loss\ reduction - Cost\ of\ the\ solution) \div Cost\ of\ the\ solution =$$

$$= [(ALE(prior) - ALE(post)) - ACS] \div ACS = CBA \div ACS$$

$$ROSI = [(240.000 - 91.200) - 69.000] \div 69.000 = 79.800 \div 69.000$$

$$ROSI = 1,15 = 115\%$$

La 4° soluzione di mitigazione restituisce un profitto dall'investimento del 115%. Il Rosi in questo è maggiore di 0 quindi il costo della salvaguardia è minore della perdita annuale, l'investimento è conveniente.

- **Mv (Verosimiglianza mitigata)**

$$mv = v \times (1 - MR)$$

$$mv = 0,90 \times (1 - 0,62)$$

$$mv = 0,513 = 34,2\%$$

In questo modo, vediamo che la probabilità di riuscita dell'attacco dopo l'applicazione della misura di mitigazione è del **34,2%**.

Soluzione 5

• mALE

$$mALE = ALE (prior) \times (1 - MR)$$

$$mALE = 240.000 \times (1 - 0.80)$$

$$mALE = 48.000\text{€}$$

Quindi la perdita attesa all'anno, a causa di un data breach, dopo aver applicato la 1° soluzione di mitigazione è di **48.000€**.

• CBA

$$CBA = ALE_{prior} - ALE_{post} - ACS$$

L'ALE dopo l'implementazione delle misure di sicurezza è uguale al mALE, poiché rappresenta la perdita annuale stimata dopo l'applicazione delle misure di mitigazione.

$$ALE (post) = mALE$$

$$CBA = 240.000 - 48.000 - 100.000$$

$$CBA = 92.000\text{€}$$

• ROSI

$$Rosi = (Monetary\ loss\ reduction - Cost\ of\ the\ solution) \div Cost\ of\ the\ solution =$$

$$= [(ALE(prior) - ALE(post)) - ACS] \div ACS = CBA \div ACS$$

$$ROSI = [(240.000 - 48.000) - 100.000] \div 100.000 = 92.000 \div 100.000$$

$$ROSI = 0,92 = 92\%$$

La 5° soluzione di mitigazione restituisce un profitto dall'investimento del 115%. Il Rosi in questo è maggiore di 0 quindi il costo della salvaguardia è minore della perdita annuale, l'investimento è conveniente.

• Mv (Verosimiglianza mitigata)

$$mv = v \times (1 - MR)$$

$$mv = 0,90 \times (1 - 0,80)$$

$$mv = 0,18 = 18\%$$

In questo modo, vediamo che la probabilità di riuscita dell'attacco dopo l'applicazione della misura di mitigazione è del **18%**.