REPORT S2-L2

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)

Valutare se il costo delle contro misure 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

Scopo del Report

Il presente report analizza il rischio di data breach di un'azienda e valuta le misure di mitigazione in base ai principi di Analisi di Rischio. Sono stati forniti dati relativi alla frequenza degli incidenti, alla quantità di dati esfiltrati e alla probabilità di successo degli attacchi.

Scenario

L'azienda subisce in media 6 data breach ogni 2 anni. Durante tali incidenti, l'80% dei dati viene esfiltrato, con un valore complessivo del dataset di 100.000€. L'attaccante ha una probabilità di successo dell'90%.

Le misure di mitigazione del rischio verranno scelte dopo un analisi di valori finanziari basata sui seguenti parametri:

- **mALE (mitigated Annualized Loss Expectancy):**

L'mALE rappresenta la perdita attesa dopo l'implementazione delle misure di mitigazione.

- **CBA (Costo Beneficio Analisi):**

La CBA confronta il costo delle contromisure con la riduzione della perdita attesa. Se il beneficio supera il costo, l'implementazione è giustificata.

- **ROSI (Return on Security Investment):**

Il ROSI misura il ritorno sull'investimento in sicurezza, confrontando il beneficio netto con il costo delle contromisure.

- **mv (probabilità di riuscita dopo la mitigazione):**

La probabilità di successo dopo l'implementazione delle misure di mitigazione.

Sezione Calcoli

I calcoli sono stati eseguiti secondo i parametri forniti per determinare l'SLE (Single Loss Expectancy), l'ARO (Annualized Rate of Occurrence), l'ALE (Annualized Loss Expectancy) e il GL (Gordon-Loeb Model).

Calcoli:

SLE (Single Loss Expectancy):

L'SLE rappresenta la perdita finanziaria prevista per singolo incidente.

SLE = Valore totale del dataset * Percentuale di dati esfiltrati

SLE = 100.000€ * 80% = 80.000€

ARO (Annualized Rate of Occurrence):

L'ARO rappresenta il numero di incidenti attesi in un anno.

ARO = Numero medio di incidenti / Periodo di tempo in anni

ARO = 6 / 2 = 3 incidenti all'anno

ALE (Annualized Loss Expectancy):

L'ALE rappresenta la perdita finanziaria attesa in un anno.

ALE = SLE * ARO

ALE = 80.000€ * 3 = 240.000€

GL (Gordon-Loeb Model):

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).

$Investment = 0{,}37 \cdot d$

$d = \lambda \cdot t \cdot v$

(d) corrisponde alla perdita stimata

$d = 240.000 * 80\% * 90\% = 172.800€$

$Investment = 0{,}37 * 172.800 = 63.936€$

Valutazione dei casi di mitigazione

L'azienda ha proposto 5 possibili soluzioni di mitigazione del rischio, ognuna delle quali presenta un valore dell'ACS ed un ratio di mitigazione diverso. Per ogni caso si calcoleranno il : mALE, CBA, ROSI e mv(La probabilità di successo dopo l'implementazione delle misure di mitigazione).

Caso 1

ACS = 63.000€

Mitigation ratio = 50%

mALE = ALE * (100%-Mitigation ratio) = 240.000 * 0,5 = 120.000€

CBA (analisi costo-benefici) = ALE – mALE – ACS = 240.000 – 120.000 – 63.000 = 57.000€

ROSI (con mitigation ratio) = (ALE * Mitigation ratio) – ACS / ACS =

= (240.000 * 0,5) – 63.000 / 63.000 = 0,9 = 90%

Mv = ALE * (100% - Mitigation ratio) / ACS = 240.000 * 0,5 / 63.000 = 1,9 = 190%

Caso 2

ACS = 70.000€

Mitigation ratio = 65%

mALE = ALE * (100%-Mitigation ratio) = 240.000 * 0,35 = 84.000€

CBA (analisi costo-benefici) = ALE – mALE – ACS = 240.000 – 84.000 – 70.000 = 86.000€

ROSI (con mitigation ratio) = (ALE * Mitigation ratio) – ACS / ACS =

= (240.000 * 0,65) – 70.000 / 70.000 = 1,22 = 122%

Mv = ALE * (100% - Mitigation ratio) / ACS = 240.000 * 0,65 / 70.000 = 1,2 = 120%

Caso 3

ACS = 60.000€

Mitigation ratio = 43%

mALE = ALE * (100%-Mitigation ratio) = 240.000 * 0,57 = 136.800€

CBA (analisi costo-benefici) = ALE – mALE – ACS = 240.000 – 136.800 – 60.000 = 43.200€

ROSI (con mitigation ratio) = (ALE * Mitigation ratio) – ACS / ACS =

= (240.000 * 0,43) – 60.000 / 60.000 = 0,72 = 72%

Mv = ALE * (100% - Mitigation ratio) / ACS = 240.000 * 0,57 / 60.000 = 2,28 = 228%

Caso 4

ACS = 69.000€

Mitigation ratio = 62%

mALE = ALE * (100%-Mitigation ratio) = 240.000 * 0,38 = 91.200€

CBA (analisi costo-benefici) = ALE – mALE – ACS = 240.000 – 91.200 – 69.000 = 79.800€

ROSI (con mitigation ratio) = (ALE * Mitigation ratio) – ACS / ACS =

= (240.000 * 0,62) – 69.000 / 69.000 = 1,15 = 115%

Mv = ALE * (100% - Mitigation ratio) / ACS = 240.000 * 0,38 / 69.000 = 1,32 = 132%

Caso 5

ACS = 100.000€

Mitigation ratio = 80%

mALE = ALE * (100%-Mitigation ratio) = 240.000 * 0,2 = 48.000€

CBA (analisi costo-benefici) = ALE – mALE – ACS = 240.000 – 48.000 – 100.000 = 92.000€

ROSI (con mitigation ratio) = (ALE * Mitigation ratio) – ACS / ACS =

= (240.000 * 0,8) – 100.000 / 100.000 = 0,92 = 92%

Mv = ALE * (100% - Mitigation ratio) / ACS = 240.000 * 0,2 / 100.000 = 0,48 = 48%

Considerazioni dei Risultati Ottenuti

Per determinare quale dei casi fornisce il miglior equilibrio per rientrare nel modello di Gordon-Loeb, dobbiamo considerare il costo delle contromisure (ACS) e confrontarlo con la perdita attesa (d) secondo la formula:

$Investment = 0{,}37 \cdot d$

Per rientrare nel modello di Gordon-Loeb, l'investimento in sicurezza non dovrebbe superare il 37% della perdita attesa. Quindi, dovremmo cercare il caso in cui l'ACS sia più vicino possibile al 37% della perdita attesa (d), ma non superiore ad esso.

Dopo aver effettuato i calcoli, è stato determinato che il Caso 1 potrebbe fornire il miglior equilibrio per rientrare nel modello di Gordon-Loeb, poiché l'ACS è di poco più basso rispetto al 37% della perdita attesa (d), mantenendo un buon livello di mitigazione del rischio.

Infatti, il caso 1 presenta un ROSI (calcolato con il mitigation ratio) del 90% quindi l'investimento è conveniente ed un mv (probabilità che l'attacco non si ripeta) del 190%.

Conclusione

Dopo aver valutato i casi proposti in base al modello di Gordon-Loeb, che stabilisce che l'investimento in sicurezza non dovrebbe superare il 37% della perdita attesa (d), abbiamo concluso che il Caso 1 sembra fornire il miglior equilibrio per rientrare nel modello. Il Caso 1 ha un ROSI (Return on Security Investment) del 90%, calcolato utilizzando il mitigation ratio, il che indica che l'investimento è conveniente. Inoltre, il Caso 1 ha una probabilità di successo dopo l'implementazione delle misure di mitigazione (mv) del 190%, il che suggerisce un alto grado di efficacia delle contromisure.

Pertanto, il Caso 1 fornisce il miglior equilibrio complessivo per rientrare nel modello di Gordon-Loeb e garantire una buona mitigazione del rischio di data breach.