PHANTOM SRL

2024 PIANI DEL RISCHIO

Prepared By :

PIGNATELLO GIUSEPPE
D'OTTAVIO ALESSIO
IANNONE LUCA

Presented To :

EPICODE

TRACCIA

EPICODE

Risk management
Esercizio

Un'azienda subisce 6 data breach ogni 2 anni, in cui l'80% del contenuto viene esfiltrato per una 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

DATI FORNITI:

Data breach ogni 2 anni **(ARO = 3)**
80% del contenuto esfiltrato **(SLE = 100,000 €)**
Attaccante riesce a portare a termine il data breach nel 90% dei casi **(Mitigation ratio senza contromisure = 0.1)**

PER CALCOLARE I VALORI RICHIESTI, UTILIZZIAMO LE SEGUENTI DEFINIZIONI:

SLE (Single Loss Expectancy): Il valore atteso di una singola perdita, calcolato moltiplicando l'importo della perdita per la probabilità che si verifichi.

ARO (Annualized Rate of Occurrence): Il tasso annuale di occorrenza delle perdite, indicante quante volte ci si aspetta che si verifichi una perdita in un anno.

λ**=ALE (Annualized Loss Expectancy):** La perdita annuale prevista dovuta a una particolare minaccia, calcolata moltiplicando l'SLE per l'ARO.

GL (Gordon-Loeb): È il limite superiore dell'investimento per mitigare il rischio, calcolato come ALE moltiplicato per il rapporto tra il livello di mitigazione desiderato e il livello di mitigazione attuale.

mALE: Acronimo di **"Maximum Annual Loss Expectancy"**. Si tratta di una metrica utilizzata nell'analisi del rischio per stimare la massima perdita finanziaria che un'organizzazione potrebbe subire in un anno a causa di un particolare tipo di minaccia o evento dannoso.

CBA: Acronimo di **"Cost-Benefit Analysis"** (Analisi costi-benefici). È una procedura utilizzata per valutare e confrontare i costi previsti e i benefici attesi di un progetto, decisione o investimento. In termini di sicurezza informatica, può essere utilizzato per valutare se l'implementazione di contromisure o misure di sicurezza sia conveniente rispetto al potenziale danno finanziario causato da un incidente o una violazione della sicurezza.

ROSI: Acronimo di "Return on Security Investment" (Ritorno sull'investimento in sicurezza). È una metrica utilizzata per valutare l'efficacia degli investimenti in sicurezza informatica. Calcola il valore dei benefici ottenuti da un investimento in sicurezza rispetto al costo totale dell'implementazione e della gestione delle misure di sicurezza.

mv (probabilità di riuscita dopo la mitigazione): Questo rappresenta la probabilità che una minaccia riesca a sfruttare una vulnerabilità dopo che sono state implementate le misure di mitigazione. Questa metrica è importante perché fornisce un'indicazione dell'efficacia delle contromisure adottate nel ridurre il rischio associato alla minaccia.

t = EF: t è il simbolo usato per rappresentare il "Tempo" e EF sta per **"Exposure Factor"** (Fattore di esposizione). L'EF indica la percentuale di perdita di un asset in caso di violazione della sicurezza. Ad esempio, se un'azienda subisce una violazione che porta alla perdita del 50% dei dati sensibili, allora l'EF sarà del 50%. Il tempo (t) può essere qualsiasi unità di misura temporale appropriata utilizzata per valutare l'intervallo di tempo durante il quale un asset è esposto a una minaccia o a un potenziale danno.

CALCOLI EFFETTUATI

	A	B	C	D	E	F
1	SLE =	100.000				
2	ARO =	3				
3	ALE =	300.000				
4	GL =	79.920				
5	CBA(1) =	87.000	ROSI(1) =	138%	mALE(1) =	150.000
6	CBA(2) =	80.000	ROSI(2) =	50%	mALE(2) =	195.000
7	CBA(3) =	90.000	ROSI(3) =	115%	mALE(3) =	129.000
8	CBA(4) =	81.000	ROSI(4) =	170%	mALE(4) =	186.000
9	CBA(5) =	50.000	ROSI(5) =	140%	mALE(5) =	240.000
10	mv(1) =	40%				
11	mv(1) =	25%				
12	mv(1) =	47%				
13	mv(1) =	28%				
14	mv(1) =	10%				

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

formula per il calcolo di GL

$$ROSI_1 = \frac{(ALE \cdot mitigation\_ratio_1) - ACS_1}{ACS_1}$$

formula per il calcolo di ROSI

$$CBA_1 = ALE(prior) - ALE(post_1) - ACS_1$$

formula per il calcolo del CBA

$$mitigation\ ratio = \frac{ALE(prior) - ALE(post)}{ALE(prior)}$$

formula utilizzata per risalire a mALE

PHANTOM SRL

2024 GRAZIE

Prepared By :

PIGNATELLO GIUSEPPE
D'OTTAVIO ALESSIO
IANNONE LUCA

Presented To :

EPICODE