

Esercitazione W18D4

Business continuity & disaster recovery

Fabio Benevento - 08/03/2024

Traccia

Ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia.

Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»
- Inondazione sull'asset «edificio primario»
- Terremoto sull'asset «edificio primario»

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Bonus

I modelli proposti possono essere utilizzati come parametri di riferimento per supportare le decisioni in materia di cybersecurity.

Tramite i parametri addizionali seguenti, calcolare gli indici ROSI (Ritorno sull'investimento) e Gordon Loeb (GL) per la definizione del budget ottimale.

	Terremoto	Incendio	Inondazione
ACS	1200€	5000€	300€
Mitigation ratio	60%	85%	30%
v	40%	60%	88%

Implementazione

Per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia è possibile calcolare i seguenti valori:

- SLE (Single Loss Expectation): rappresenta il danno monetario subito al verificarsi dell'evento.
Esso si calcola come **SLE = AV x EF** dove AV è il valore dell'asset mentre EF è la percentuale impattata al verificarsi dell'evento
- ALE (Annualized Loss Expectation): rappresenta il danno monetario annualizzato, ovvero ripartito per la probabilità annuale che esso si verifichi.
Esso si calcola a partire dall'SLE mediante la formula **ALE = SLE x ARO** dove ARO è il numero di volte stimato dell'evento nell'arco di un anno

Per le casistiche citate otteniamo quindi:

- Inondazione sull'asset «edificio secondario»

$$\text{SLE} = 150000\text{€} \times 0,4 = 60000\text{€}$$

$$\text{ALE} = 60000\text{€} \times 0,02 = 1200\text{€/anno}$$

- Terremoto sull'asset «datacenter»

$$\text{SLE} = 100000\text{€} \times 0,95 = 95000\text{€}$$

$$\text{ALE} = 95000\text{€} \times 0,03 = 2850\text{€/anno}$$

- Incendio sull'asset «edificio primario»

$$\text{SLE} = 350000\text{€} \times 0,6 = 210000\text{€}$$

$$\text{ALE} = 210000\text{€} \times 0,05 = 10500\text{€/anno}$$

- Incendio sull'asset «edificio secondario»

$$\text{SLE} = 150000\text{€} \times 0,5 = 75000\text{€}$$

$$\text{ALE} = 75000\text{€} \times 0,05 = 3750\text{€/anno}$$

- Inondazione sull'asset «edificio primario»

$$\text{SLE} = 350000\text{€} \times 0,55 = 192500\text{€}$$

$$\text{ALE} = 192500\text{€} \times 0,02 = 3850\text{€/anno}$$

- Terremoto sull'asset «edificio primario»

$$\text{SLE} = 350000\text{€} \times 0,8 = 280000\text{€}$$

$$\text{ALE} = 280000\text{€} \times 0,03 = 8400\text{€/anno}$$

Bonus

Il ROSI permette di calcolare il beneficio che l'investimento nella sicurezza apporta all'organizzazione.

Per il suo calcolo in primo luogo si determina il mALE (mitigated ALE) o ALE(post) ovvero l'ALE in seguito all'applicazione della mitigazione che è dato dal prodotto dell'ALE pre intervento (ALE (prio)) per il fattore di mitigazione (mitigation ratio)

$$\text{mALE} = \text{ALE}(\text{post}) = \text{ALE}(\text{prio}) * \text{mitigation ratio}$$

Da esso si ottiene il CBA (Analisi costi/benefici in termini monetari) come

$$\text{CBA} = \text{ALE} - \text{mALE} - \text{ACS}$$

dove ACS rappresenta il costo annuale della salvaguardia

Il ROSI sarà quindi calcolato come valore percentuale come rapporto tra il CBA e l'ACS.

$$\text{ROSI} = \text{CBA} / \text{ACS} = \text{ALE} - \text{mALE} - \text{ACS} / \text{ACS}$$

Gordon Loeb è invece una regola generale per cui l'investimento in sicurezza non dovrebbe eccedere il 37% delle perdite potenziali per essere indicato come conveniente. Esso si calcola quindi come

$$\text{Investment} = 0,37 * d$$

dove d sono le perdite potenziali calcolate come

$$d = \lambda * t * v = AV * EF * v$$

Per le varie casistiche i parametri calcolati sono i seguenti

- Inondazione sull'asset «edificio secondario»

$$ALE = 1200\text{€/anno}$$

$$mALE = ALE - ALE * \text{mitigation rate} = 1200 - 1200 * 0,30 = 840\text{€/anno}$$

$$CBA = ALE - mALE - ACS = 1200 - 840 - 300 = 60\text{€/anno}$$

$$ROSI = CBA / ACS = 60 / 300 = 20\%$$

$$dc = SLE * v = 60000\text{€} * 0,4 = 52800\text{€}$$

$$da = dc * ARO = 52800\text{€} * 0,2 = 10560\text{€/anno}$$

$$lc = 0,37 * dc = 52800\text{€} * 0,37 = 19536\text{€}$$

$$la = 0,37 * da = 10560\text{€} * 0,37 = 3907\text{€/anno}$$

- Terremoto sull'asset «datacenter»

$$ALE = 2850\text{€/anno}$$

$$mALE = ALE - ALE * \text{mitigation rate} = 2850 - 2850 * 0,60 = 1140\text{€/anno}$$

$$CBA = ALE - mALE - ACS = 2850 - 1140 - 1200 = 510\text{€/anno}$$

$$ROSI = CBA / ACS = 510 / 1200 = 42\%$$

$$dc = SLE * v = 95000\text{€} * 0,88 = 24000\text{€}$$

$$da = dc * ARO = 24000\text{€} * 0,33 = 7920\text{€/anno}$$

$$lc = 0,37 * dc = 24000\text{€} * 0,37 = 8880\text{€}$$

$$la = 0,37 * da = 7920\text{€} * 0,37 = 2930\text{€/anno}$$

- Incendio sull'asset «edificio primario»

$$ALE = 10500\text{€/anno}$$

$$mALE = ALE - ALE * \text{mitigation rate} = 10500 - 10500 * 0,85 = 1575\text{€/anno}$$

$$CBA = ALE - mALE - ACS = 10500 - 1575 - 5000 = 3925\text{€/anno}$$

$$ROSI = CBA / ACS = 3925 / 5000 = 78 \%$$

$$dc = SLE * v = 21000\text{€} * 0,6 = 12600\text{€}$$

$da = dc * ARO = 12600€ * 0,5 = 6300€/anno$

$lc = 0,37 * dc = 12600€ * 0,37 = 4462€$

$la = 0,37 * da = 6300€ * 0,37 = 2331€/anno$

- Incendio sull'asset «edificio secondario»

$ALE = 3750€/anno$

$mALE = ALE - ALE * mitigation\ rate = 3750 - 3750 * 0,85 = 312€/anno$

$CBA = ALE - mALE - ACS = 3750 - 312 - 5000 = -1562€/anno$

$ROSI = CBA / ACS = -1562 / 5000 = -31\%$

$dc = SLE * v = 75000€ * 0,6 = 45000€$

$da = dc * ARO = 45000€ * 0,5 = 22500€/anno$

$lc = 0,37 * dc = 45000€ * 0,37 = 16650€$

$la = 0,37 * da = 22500€ * 0,37 = 8325€/anno$

- Inondazione sull'asset «edificio primario»

$ALE = 3850€/anno$

$mALE = ALE - ALE * mitigation\ rate = 3850 - 3850 * 0,30 = 2695€/anno$

$CBA = ALE - mALE - ACS = 3850 - 2695 - 300 = 855€/anno$

$ROSI = CBA / ACS = 855 / 2695 = 31\%$

$dc = SLE * v = 192500€ * 0,4 = 77000€$

$da = dc * ARO = 77000€ * 0,2 = 15400€/anno$

$lc = 0,37 * dc = 77000€ * 0,37 = 28490€$

$la = 0,37 * da = 15400€ * 0,37 = 5698€/anno$

- Terremoto sull'asset «edificio primario»


$ALE = 8400€/anno$

$mALE = ALE - ALE * mitigation\ rate = 8400 - 8400 * 0,60 = 3360€/anno$

$CBA = ALE - mALE - ACS = 8400 - 3360 - 1200 = 3840€/anno$

$ROSI = CBA / ACS = 3840 / 3360 = 114\%$

$dc = SLE * v = 280000€ * 0,88 = 246400€$


$$da = dc * ARO = 246400\text{€} * 0,33 = 81312\text{€/anno}$$

$$lc = 0,37 * dc = 246400\text{€} * 0,37 = 91168\text{€}$$

$$la = 0,37 * da = 81312\text{€} * 0,37 = 30085\text{€/anno}$$