

VALUTAZIONE DEL RISCHIO E PERDITA ANNUALE

Introduzione

In questo esercizio ho simulato un'attività di **risk assessment quantitativo** su alcuni asset aziendali, con l'obiettivo di calcolare la perdita economica annuale che una compagnia potrebbe subire in caso di determinati eventi disastrosi.

Per effettuare i calcoli ho utilizzato i concetti fondamentali di:

- SLE (Single Loss Expectancy)
- ARO (Annual Rate of Occurrence)
- ALE (Annual Loss Expectancy)

Questo approccio permette di stimare in modo concreto l'impatto economico dei rischi e supportare eventuali decisioni di sicurezza.

Metodologia di calcolo

SLE – Single Loss Expectancy

Rappresenta la perdita economica nel caso in cui l'evento si verifichi una singola volta.

Formula:

$$\text{SLE} = \text{Valore asset} \times \text{Exposure Factor}$$

ARO – Annual Rate of Occurrence

Indica ogni quanto si verifica l'evento.

Esempi:

- 1 volta ogni 20 anni = 0,05
- 1 volta ogni 50 anni = 0,02

ALE – Annual Loss Expectancy

Rappresenta la perdita economica annua stimata.

Formula:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

Calcolo perdita annuale per scenario

1. Inondazione sull'edificio secondario

Valore asset: 150.000€

Exposure factor: 40%

ARO inondazione: 1/50 = 0,02

$$\text{SLE} = 150.000 \times 0,40 = 60.000\text{€}$$

$$\text{ALE} = 60.000 \times 0,02 = \mathbf{1.200\text{€ annui}}$$

2. Terremoto sul datacenter

Valore asset: 100.000€

Exposure factor: 95%

ARO terremoto: 1/30 ≈ 0,033

$$\text{SLE} = 100.000 \times 0,95 = 95.000\text{€}$$

$$\text{ALE} = 95.000 \times 0,033 \approx \mathbf{3.135\text{€ annui}}$$

3. Incendio sull'edificio primario

Valore asset: 350.000€

Exposure factor: 60%

ARO incendio: 1/20 = 0,05

$$\text{SLE} = 350.000 \times 0,60 = 210.000\text{€}$$

$$\text{ALE} = 210.000 \times 0,05 = \mathbf{10.500\text{€ annui}}$$

4. Incendio sull'edificio secondario

Valore asset: 150.000€

Exposure factor: 50%

ARO incendio: 0,05

$$\text{SLE} = 150.000 \times 0,50 = 75.000\text{€}$$

$$\text{ALE} = 75.000 \times 0,05 = \mathbf{3.750\text{€ annui}}$$

Analisi dei risultati

Dai calcoli emerge che il rischio economicamente più impattante per l'azienda è:

👉 Incendio sull'edificio primario (10.500€ annui)

Questo significa che l'azienda dovrebbe concentrare maggiormente:

- investimenti in sicurezza antincendio
- sistemi di prevenzione
- assicurazioni
- piani di disaster recovery

Il calcolo dell'ALE consente infatti di capire dove conviene investire per ridurre il rischio.

Parte facoltativa – Estensione

Inondazione edificio primario

Valore: 350.000€

Exposure factor: 55%

ARO: 0,02

$$SLE = 350.000 \times 0,55 = 192.500\text{€}$$

$$ALE = 192.500 \times 0,02 = \mathbf{3.850\text{€ annui}}$$

Terremoto edificio primario

Exposure factor: 80%

ARO: 0,033

$$SLE = 350.000 \times 0,80 = 280.000\text{€}$$

$$ALE = 280.000 \times 0,033 \approx \mathbf{9.240\text{€ annui}}$$

CIA TRIAD (Confidenzialità, Integrità, Disponibilità)

Scenario scelto: incendio nel datacenter

Confidenzialità

Garantisce che i dati siano accessibili solo a utenti autorizzati.

Possibili minacce:

- accesso non autorizzato ai server danneggiati
- furto di dischi o backup
- perdita di controllo sui dati

Contromisure:

- cifratura dischi
 - controllo accessi fisici
 - autenticazione forte
-

Integrità

Assicura che i dati non vengano alterati.

Minacce:

- danneggiamento hardware
- corruzione dati
- modifiche non autorizzate

Contromisure:

- backup verificati
 - hashing e controlli integrità
 - sistemi RAID
-

Disponibilità

Garantisce accesso ai dati quando necessario.

Minacce:

- distruzione server
- downtime prolungato

- perdita servizi

Contromisure:

- disaster recovery plan
 - backup off-site
 - replica cloud
 - UPS e sistemi antincendio
-

Conclusione

Questo esercizio mi ha permesso di comprendere come calcolare in modo concreto il rischio economico legato a eventi disastrosi e come applicare i principi della sicurezza informatica nella gestione aziendale.

L'utilizzo di metriche come SLE, ARO e ALE consente di valutare il rischio in maniera quantitativa e prendere decisioni strategiche per la protezione degli asset e dei dati aziendali.