Perdita annuale aziendale - W18D4

Durata temporale dell’attività:
4 ore

Attività eseguita dal gruppo
MEF

Indice Generale

Introduzione e metodologia……...……2
Calcoli e risultati……..…….……4
Interpretazione dei dati…….…….……...5
Conclusione e raccomandazioni…….……...6
Facoltativo……7
Confidenzialità, Integrità e Disponibilità dei Dati: Concetti, Minacce e Contromisure……...8
Conclusione e raccomandazioni……..10

Introduzione

L’obiettivo di questa analisi è stimare quantitativamente la perdita annuale (Annual Loss Expectancy, ALE) che una compagnia subirebbe in caso di eventi disastrosi quali terremoti, incendi o inondazioni. L'analisi si concentra su tre asset principali della compagnia: l'edificio primario, l'edificio secondario e il datacenter. I risultati sono stati calcolati utilizzando i dati relativi al valore degli asset, all'Exposure Factor (EF) e al tasso annuale di occorrenza (Annual Rate of Occurrence, ARO) degli eventi.

Metodologia

Per calcolare l’ALE, sono stati utilizzati i seguenti parametri e formule:

1. **Single Loss Expectancy (SLE):** rappresenta la perdita finanziaria stimata per un singolo evento disastroso e si calcola come:
2. **Annual Rate of Occurrence (ARO):** rappresenta la probabilità annuale che un evento si verifichi ed è calcolato come l’inverso del periodo stimato in anni.
3. **Annual Loss Expectancy (ALE):** rappresenta la perdita annuale attesa per un evento specifico ed è calcolata come:

I calcoli sono stati condotti utilizzando i seguenti dati:

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%

Calcoli

1. Edificio Primario

- **Terremoto**:
  SLE=350.000×0.80=280.000
  ALE=280.000×0.033=9.240
- **Incendio**:
  SLE=350.000×0.60=210.000
  ALE=210.000×0.05=10.500
- **Inondazione**:
  SLE=350.000×0.55=192.500
  ALE=192.500×0.02=3.850

2. Edificio Secondario

- **Terremoto**:
  SLE=150.000×0.80=120.000
  ALE=120.000×0.033=3.960
- **Incendio**:
  SLE=150.000×0.50=75.000
  ALE=75.000×0.05=3.750
- **Inondazione**:
  SLE=150.000×0.40=60.000
  ALE=60.000×0.02=1.200

3. Datacenter

- **Terremoto**:
  SLE=100.000×0.95=95.000
  ALE=95.000×0.033=3.135

- **Incendio**:

  SLE=100.000×0.60=60.000

  ALE=60.000×0.05=3.000
- **Inondazione**:

  SLE=100.000×0.35=35.000

  ALE=35.000×0.02=700

Risultati dell'Analisi

I risultati sono stati sintetizzati nella tabella seguente, che evidenzia le perdite annuali attese (ALE) per ogni combinazione di evento e asset.

Asset	Evento	SLE (Euro)	ARO	ALE (Euro)
Edificio primario	Terremoto	280.000	0,03	9.240
	Incendio	210.000	0,05	10.500
	Inondazione	192.500	0,02	3.850
Edificio secondario	Terremoto	120.000	0,03	3.960
	Incendio	75.000	0,05	3.750
	Inondazione	60.000	0,02	1.200
Datacenter	Terremoto	95.000	0,03	3.135
	Incendio	60.000	0,05	3.000
	Inondazione	35.000	0,02	700

Interpretazione dei Risultati

1. **Edificio primario:**
    - L'incendio rappresenta il rischio più significativo, con una perdita annuale stimata di 10.500€. Questo è dovuto all'elevato valore dell'asset e al fattore di esposizione relativamente alto.
    - Il rischio di inondazione è meno significativo rispetto agli altri eventi, con una ALE di 3.850€.
2. **Edificio secondario:**
    - Anche qui l'incendio è il rischio più elevato, ma con una perdita annuale di 3.750€, inferiore rispetto all'edificio primario a causa del minor valore dell'asset.
    - Le inondazioni rappresentano il rischio meno significativo, con una ALE di 1.200€.
3. **Datacenter:**
    - Il terremoto rappresenta il rischio più significativo per il datacenter, con una ALE di 3.135€, dovuta al fattore di esposizione molto alto (95%).
    - L'inondazione è il rischio meno rilevante, con una ALE di 700€.

Conclusioni e Raccomandazioni

1. **Priorità di mitigazione:**
    - Le azioni di mitigazione dovrebbero concentrarsi inizialmente sull'incendio per l'edificio primario, dato il rischio elevato e la perdita potenziale significativa.
    - Per il datacenter, sarebbe opportuno rafforzare le misure antisismiche a causa dell'elevata esposizione al rischio di terremoti.
2. **Prevenzione:**
    - Implementare sistemi di rilevamento precoce di incendi e migliorare le infrastrutture di sicurezza antincendio per entrambi gli edifici.
    - Per ridurre il rischio di inondazioni, si possono adottare misure preventive come la costruzione di barriere o il miglioramento dei sistemi di drenaggio.
3. **Assicurazione:**
    - Considerare polizze assicurative specifiche per gli eventi con il rischio più elevato, come terremoti e incendi, per minimizzare l'impatto finanziario in caso di disastro.

Conclusione

Questa analisi evidenzia l'importanza di una gestione proattiva del rischio. Identificando le principali minacce e le loro conseguenze economiche, è possibile allocare risorse in modo efficiente per ridurre l'impatto dei disastri sugli asset aziendali.

Facoltativo:

Relazione Estesa sull'Analisi Quantitativa dell'Impatto di Eventi Disastrosi su Asset Aziendali

Introduzione

Questa sezione estende l'analisi precedente per includere ulteriori scenari di inondazione e terremoto sull'asset "edificio primario". Inoltre, viene approfondito il concetto di confidenzialità, integrità e disponibilità dei dati, identificando minacce specifiche e **proponendo** contromisure adeguate.

Estensione dell'Analisi: Altri Scenari

Asset	Evento	SLE (Euro)	ARO	ALE (Euro)
Edificio primario	Inondazione	192.500	0,02	3.850
	Terremoto	280.000	0.03	9.240

Risultati:

1. L'inondazione sull'edificio primario genera un'ALE di 3.850€, principalmente a causa di un EF moderato (55%) e di un basso ARO (0,02).
2. Il terremoto sull'edificio primario rappresenta un rischio più elevato, con un'ALE di 9.240€, dovuto a un EF più alto (80%).

Confidenzialità, Integrità e Disponibilità dei Dati: Concetti, Minacce e Contromisure

La protezione dei dati aziendali è essenziale per garantire la continuità operativa e minimizzare i rischi legati a eventi disastrosi o attacchi informatici. In questa sezione, analizziamo i concetti fondamentali di Confidenzialità, Integrità e Disponibilità dei dati, le minacce a cui sono soggetti e le contromisure necessarie per mitigarle.

1. Confidenzialità

La confidenzialità consiste nel proteggere i dati dall'accesso non autorizzato, garantendo che solo le persone autorizzate possano accedervi. Le principali minacce alla confidenzialità includono attacchi informatici che sfruttano vulnerabilità nei sistemi, furti fisici di dispositivi contenenti dati sensibili e backup non adeguatamente protetti.

Per contrastare tali minacce, è essenziale adottare controlli di accesso stringenti, come l'autenticazione a due fattori (2FA) e la crittografia dei dati, sia in transito che a riposo. Inoltre, una gestione accurata dei privilegi degli utenti può limitare l'accesso ai dati sensibili, riducendo così il rischio di esposizione non autorizzata.

2. Integrità

L'integrità dei dati garantisce che le informazioni rimangano accurate, complete e non modificate in modo non autorizzato. Tra le minacce principali all'integrità vi sono la corruzione dei dati causata da malware o ransomware, gli errori umani durante la manipolazione delle informazioni e i danni fisici ai supporti di memorizzazione.

Le contromisure per preservare l'integrità dei dati includono l'utilizzo di soluzioni di backup con versioning, che consentono di ripristinare versioni precedenti dei file, e l'implementazione di algoritmi di hash per verificare eventuali modifiche non autorizzate. Monitorare le modifiche ai file tramite sistemi di audit avanzati rappresenta un ulteriore strumento per identificare e correggere eventuali alterazioni.

3. Disponibilità

La disponibilità si riferisce alla capacità di garantire l'accesso ai dati ogni volta che è necessario. Le principali minacce alla disponibilità comprendono interruzioni di servizio dovute a guasti hardware, eventi naturali come terremoti o inondazioni e attacchi DDoS che sovraccaricano le reti aziendali.

Per assicurare la disponibilità, è fondamentale utilizzare infrastrutture ridondanti, come data center situati in diverse aree geografiche, e implementare soluzioni di failover automatico.

Inoltre, pianificare e testare regolarmente un piano di Disaster Recovery permette di garantire una risposta efficace in caso di emergenze.

Conclusione e Raccomandazioni

Le analisi dei rischi effettuate evidenziano che la priorità di mitigazione deve essere assegnata ai rischi sismici che interessano l'edificio primario, poiché questi rappresentano il maggiore impatto finanziario potenziale. Parallelamente, è cruciale proteggere i dati nel datacenter mediante backup sicuri e infrastrutture ridondanti, garantendo così la continuità operativa in caso di guasti o disastri.

L'adozione di piani di continuità operativa efficaci è altrettanto importante. Questi piani devono includere esercitazioni periodiche per testare la capacità dell'azienda di rispondere a scenari critici e minimizzare l'impatto di eventi avversi. Infine, un approccio multilivello alla protezione dei dati, che combini tecnologie avanzate con procedure organizzative ben definite, è essenziale per garantire la resilienza aziendale.

Questa analisi sottolinea l'importanza di una preparazione proattiva per mitigare le perdite finanziarie e garantire la sicurezza e l'efficienza operativa anche in presenza di eventi straordinari.