EPICODE

ESERCIZIO W18D4

Perdita annuale di un'azienda

Mungiovì Fabio

TASK

In questo esercizio, ipotizzeremo 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»

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%

Facoltativo:

Estendere l'esercizio precedente andando a valutare:

- Inondazione sull'asset «edificio primario»;
- Terremoto sull'asset «edificio primario».

Successivamente, scegli uno scenario tra quelli proposti e definisci:

- Cosa si intende per Confidenzialità, Integrità e Disponibilità dei dati;
- Potenziali minacce alla Confidenzialità, Integrità e Disponibilità dei dati;
- Contromisure per proteggere i dati da queste minacce.

ESECUZIONE

Per risolvere l'esercizio e calcolare la perdita annuale che l'azienda subirebbe in caso di disastro, dobbiamo prima capire alcuni concetti chiave e le formule da applicare.
Si valuta l'impatto di un disastro su un bene aziendale.

L'esercizio ci chiede di calcolare la perdita annuale in diversi scenari:

- Inondazione sull'asset "edificio secondario"
- Terremoto sull'asset "datacenter"
- Incendio sull'asset "edificio primario"
- Incendio sull'asset "edificio secondario"

Ci vengono fornite tre tabelle con i dati necessari:

- **Valore degli asset:**
    - Edificio primario: 350.000€
    - Edificio secondario: 150.000€
    - Datacenter: 100.000€
- **ARO (Annualized Rate of Occurrence):**
    - Terremoto: 1 volta ogni 30 anni
    - Incendio: 1 volta ogni 20 anni
    - Inondazione: 1 volta ogni 50 anni
- **Exposure Factor (EF):** La percentuale di valore che un asset perderebbe a causa di un determinato evento.

Per calcolare la perdita annuale, possiamo utilizzare le seguenti formule:

1. **Single Loss Expectancy (SLE):** Questa formula ci dice la perdita monetaria che si verificherebbe ogni volta che un rischio si materializza. Si calcola moltiplicando il valore dell'asset (AV) per l'Exposure Factor (EF).

$$SLE = AV \times EF$$

2. **Annualized Rate of Occurrence (ARO):** Questo dato ci indica quante volte un evento si prevede che accada in un anno. Se, ad esempio, un terremoto avviene una volta ogni 30 anni, l'ARO sarà 1/30.
3. **Annual Loss Expectancy (ALE):** Questa è la perdita annuale attesa. Si calcola moltiplicando l'SLE per l'ARO.

$$ALE = SLE \times ARO$$

Ora possiamo procedere con i calcoli per ogni scenario richiesto:

1. Inondazione sull'asset "edificio secondario"

- Valore dell'asset (AV) "edificio secondario": 150.000€
- Exposure Factor (EF) per inondazione sull'edificio secondario: 40% (0.40)
- ARO per inondazione: 1 volta ogni 50 anni (1/50=0.02)

Calcolo:

- SLE = 150.000€×0.40=60.000€
- ALE = 60.000€×0.02=1.200€

La perdita annuale per un'inondazione sull'edificio secondario sarebbe di 1.200€.

2. Terremoto sull'asset "datacenter"

- Valore dell'asset (AV) "datacenter": 100.000€
- Exposure Factor (EF) per terremoto sul datacenter: 95% (0.95)
- ARO per terremoto: 1 volta ogni 30 anni (1/30≈0.0333)

Calcolo:

- SLE = 100.000€×0.95=95.000€
- ALE = 95.000€×0.0333≈3.163,5€

La perdita annuale per un terremoto sul datacenter sarebbe di circa 3.163,5€.

3. Incendio sull'asset "edificio primario"

- Valore dell'asset (AV) "edificio primario": 350.000€
- Exposure Factor (EF) per incendio sull'edificio primario: 60% (0.60)
- ARO per incendio: 1 volta ogni 20 anni (1/20=0.05)

Calcolo:

- SLE = 350.000€×0.60=210.000€
- ALE = 210.000€×0.05=10.500€

La perdita annuale per un incendio sull'edificio primario sarebbe di 10.500€.

4. Incendio sull'asset "edificio secondario"

- Valore dell'asset (AV) "edificio secondario": 150.000€
- Exposure Factor (EF) per incendio sull'edificio secondario: 50% (0.50)
- ARO per incendio: 1 volta ogni 20 anni (1/20=0.05)

Calcolo:

- SLE = 150.000€×0.50=75.000€
- ALE = 75.000€×0.05=3.750€

La perdita annuale per un incendio sull'edificio secondario sarebbe di 3.750€.

FACOLTATIVO

Dobbiamo estendere l'esercizio valutando anche:

- Inondazione sull'asset "edificio primario"
- Terremoto sull'asset "edificio primario"

Inondazione sull'asset "edificio primario"

- Valore dell'asset (AV) "edificio primario": 350.000€
- Exposure Factor (EF) per inondazione sull'edificio primario: 55% (0.55)
- ARO per inondazione: 1 volta ogni 50 anni (1/50=0.02)

Calcolo:

- SLE = 350.000€×0.55=192.500€
- ALE = 192.500€×0.02=3.850€

La perdita annuale per un'inondazione sull'edificio primario sarebbe di 3.850€.

Terremoto sull'asset "edificio primario"

- Valore dell'asset (AV) "edificio primario": 350.000€
- Exposure Factor (EF) per terremoto sull'edificio primario: 80% (0.80)
- ARO per terremoto: 1 volta ogni 30 anni (1/30≈0.0333)

Calcolo:

- SLE = 350.000€×0.80=280.000€
- ALE = 280.000€×0.0333≈9.324€

La perdita annuale per un terremoto sull'edificio primario sarebbe di circa 9.324€.

Scenario: Incendio sull'asset "edificio primario"

Ora scegliamo uno scenario tra quelli proposti e definiamo Confidenzialità, Integrità e Disponibilità dei dati, le potenziali minacce e le contromisure.

Prendiamo come esempio l'Incendio sull'asset "edificio primario".

Questo scenario riguarda un edificio fisico, quindi la Confidenzialità, Integrità e Disponibilità si riferiscono ai dati e ai sistemi presenti all'interno di quell'edificio.

Confidenzialità, Integrità e Disponibilità (CID) dei dati

Questi tre concetti sono i pilastri della sicurezza delle informazioni, spesso indicati come "Triade CID":

- **Confidenzialità:** Immaginiamo di avere un diario segreto. La confidenzialità è come assicurarsi che solo noi (o chi è autorizzato) possiamo leggerlo. Significa che le informazioni sensibili non devono essere accessibili a persone o sistemi non autorizzati. Se i dati vengono rivelati a chi non dovrebbe vederli, la confidenzialità è compromessa.
- **Integrità:** Pensiamo al nostro diario. L'integrità è come assicurarsi che nessuno abbia cambiato le pagine, aggiunto nuove scritte o strappato via qualcosa senza il nostro permesso. Significa

che i dati devono essere accurati, completi e non modificati in modo non autorizzato durante il loro ciclo di vita. Se i dati vengono alterati o corrotti, l'integrità è compromessa.

- **Disponibilità:** Tornando al diario, la disponibilità è come essere sicuri di poterlo trovare e leggere ogni volta che ne abbiamo bisogno. Significa che gli utenti autorizzati devono avere accesso alle informazioni e ai sistemi quando richiesto. Se non possiamo accedere ai dati o ai sistemi quando necessario, la disponibilità è compromessa.

Potenziali minacce alla Confidenzialità, Integrità e Disponibilità dei dati in caso di incendio sull'edificio primario

Un incendio in un edificio primario, dove probabilmente risiedono server, workstation e archivi fisici di documenti, può avere conseguenze devastanti sulla triade CID:

- **Minacce alla Confidenzialità:**
    - **Distruzione incontrollata:** Se i server o i documenti che contengono dati sensibili vengono bruciati, non si può più controllare chi accede alle ceneri o ai resti. Frammenti di dati potrebbero sopravvivere e essere recuperati da persone non autorizzate.
    - **Accesso non autorizzato durante il recupero:** Durante le operazioni di soccorso e recupero, potrebbero esserci opportunità per persone non autorizzate di accedere ai resti fisici di server o documenti, compromettendo la riservatezza.
- **Minacce all'Integrità:**
    - **Danneggiamento dei dati:** Il calore intenso, il fumo e l'acqua usata per spegnere l'incendio possono danneggiare o distruggere fisicamente i dischi rigidi, i server e i supporti di memorizzazione, corrompendo irrimediabilmente i dati.
    - **Perdita di dati:** Se non ci sono backup o se anche i backup sono stati compromessi dall'incendio, i dati potrebbero essere persi per sempre, rendendoli incompleti e inutilizzabili.
- **Minacce alla Disponibilità:**
    - **Interruzione dei servizi:** L'incendio distruggerà o renderà inagibili i server e le infrastrutture di rete presenti nell'edificio, portando all'interruzione completa dei servizi IT e all'impossibilità di accedere ai dati e alle applicazioni.
    - **Difficoltà nel recupero:** Anche dopo l'incendio, il processo di ricostruzione e ripristino dell'infrastruttura può richiedere tempo, prolungando l'indisponibilità dei dati e dei servizi.

Contromisure per proteggere i dati da queste minacce

Per mitigare l'impatto di un incendio e proteggere i dati, si possono adottare diverse contromisure:

- **Per la Confidenzialità:**
    - **Crittografia dei dati:** Tutti i dati sensibili, sia sui server che sui dispositivi portatili, dovrebbero essere crittografati. In questo modo, anche se i supporti fisici vengono recuperati dopo l'incendio, i dati rimarrebbero illeggibili senza la chiave di decrittazione.
    - **Distruzione sicura:** In caso di recupero di hardware danneggiato, si dovrebbe attuare una procedura di distruzione sicura per garantire che nessun dato residuo possa essere estratto.
- **Per l'Integrità:**
    - **Backup e Disaster Recovery Plan:** È fondamentale avere backup regolari di tutti i dati critici, archiviati in un luogo geograficamente separato (off-site) e sicuro. Un piano di Disaster Recovery ben definito permetterebbe di ripristinare i dati e le operazioni in caso di un evento distruttivo come un incendio.

    - **Sistemi di rilevamento e soppressione incendi avanzati:** Installare sistemi antincendio (come sprinkler o sistemi a gas inerti) che possano intervenire rapidamente per limitare i danni fisici ai server e ai supporti di memorizzazione.
    - **Redundancy dei sistemi:** Implementare sistemi ridondanti per i dati e le applicazioni critiche (es. server cluster, replicazione dei dati) in modo che se un sistema viene distrutto, un altro possa prendere il suo posto.
- **Per la Disponibilità:**
    - **Business Continuity Plan:** Oltre al Disaster Recovery, un piano di continuità operativa assicura che le funzioni aziendali critiche possano continuare a operare anche in caso di inagibilità dell'edificio primario. Questo può includere l'utilizzo di uffici temporanei o il telelavoro.
    - **Centri di elaborazione dati secondari (DR site):** Avere un data center di recupero o un sito di disaster recovery remoto permette di far ripartire i servizi in tempi rapidi, minimizzando l'interruzione.
    - **Alimentazione e raffreddamento ridondanti:** Anche se non direttamente legati all'incendio, sistemi robusti di alimentazione e raffreddamento aiutano a prevenire guasti che potrebbero esacerbare una situazione già critica.

In sintesi, la preparazione e la pianificazione sono essenziali per proteggere i dati da eventi distruttivi come un incendio, garantendo che anche di fronte a un disastro, la Confidenzialità, l'Integrità e la Disponibilità delle informazioni siano il più possibile preservate.