Business continuity & Disaster recovery

Traccia:
Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell'esempio pratico di oggi, 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»

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%

Riferimenti teorici

Nonostante le misure di sicurezza messe in atto, alcuni eventi esterni possono impattare negativamente sulla sicurezza delle compagnie, come può essere un evento catastrofico naturale oppure un attacco. Le compagnie resilienti predispongono di conseguenza piani e procedure per ridurre gli effetti dell'evento ed assicurare la continuità operativa, queste pratiche prendono il nome di «**business continuity plan**» e «**disaster recovery**».

Business continuity plan (BCP)

Il «business continuity plan», piano per la continuità del business, ha lo scopo principale di dettagliare le policy e le procedure per minimizzare gli impatti negativi sull'operatività di una compagnia a valle di un evento catastrofico / attacco, e ad assicurare la continuità delle operazioni svolte dalla compagnia anche in situazioni di emergenza.

Il business continuity plan (BCP) si compone di quattro step principali:

- Pianificazione e scopo
- **Business impact assessment (BIA)**, ovvero valutazione degli impatti sul business

- **Business planning**, ovvero piano di continuità operativa
- Approvazione ed implementazione

Pianificazione e scopo
-Un'analisi strutturata dell'organizzazione e del business è il primo passo nella stesura di un piano di continuità. In questa fase lo scopo è quello di dettagliare e «mappare» i dipartimenti interni di una compagnia e gli individui con i servizi critici erogati dalla compagnia stessa. Infatti, in ottica di evento catastrofico, un piano di continuità ben strutturato dovrà come prima priorità ridurre gli impatti su quelli che sono i «servizi core», ovvero i servizi principali erogati dalla compagnia. Anche in questo contesto c'è il concetto di «priorità»: gli asset critici, relativi al business hanno sempre la priorità.
-La creazione di un team / gruppo di lavoro responsabile del BCP che deve essere approvato dai dirigenti della compagnia stessa.
-Una valutazione delle risorse ed asset disponibili che saranno incluse nelle attività di business continuity (Sviluppo del BCP; Test, manutenzione e training per gli impiegati; Implementazione del BCP -> la maggior parte dell'effort per le attività relative al BCP sono imputabili al capitale umano, con una porzione minore dedicata a risorse quali software ed hardware per garantire continuità dei servizi).
-Un'analisi delle leggi e regolamentazioni che la compagnia deve rispettare. Ad esempio, potrebbero essere in vigore delle leggi che stabiliscono quali servizi devono essere sempre erogati anche in situazioni critiche da una data compagnia.

Business impact assessment (BIA)
È l'analisi degli impatti sul business. Il BIA ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Inoltre, il BIA ha lo scopo di misurare la probabilità che tali minacce possano verificarsi e l'impatto che esse potrebbero avere sul business. Il BIA e conseguentemente la sua «misurazione» può seguire l'approccio qualitativo o quantitativo.
-Identificazione delle priorità del business: Da un punto di vista qualitativo, si potrebbero, di fatto, identificare le priorità in base alla loro criticità relativamente al business – dove agli asset a supporto del business viene assegnata una priorità superiore. Da un punto di vista quantitativo, si potrebbe invece creare una lista contenente tutti gli asset della compagnia ed assegnare ad ognuno di essi un valore monetario, chiamato «asset value» (AV) e successivamente assegnare una priorità in base al valore.
All'interno di questa fase si definiscono altri due valori quantitativi:
Maximum tolerable downtime (MTD): definito come il limite massimo di tempo durante il quale un business può non essere operativo senza causare danni irreparabili al business stesso.
Recovery time objective (RTO): definito come l'ammontare di tempo necessario a recuperare un sistema o una funzionalità di esso in caso di disastro.
Lo scopo del BCP è di assicurare che RTO <= MTD, ovvero che il tempo per recuperare un sistema o una funzionalità critica in caso di disastro sia minore del tempo limite «sopportabile» dal business, e superato il quale si avrebbero conseguenze permanenti sul business stesso.

-Identificazione dei rischi: Stimare il rischio che impatterebbe l'organizzazione in caso di disastro naturale o causato dall'uomo.
-Valutazione della probabilità: Una volta identificati i rischi che possono impattare sull'organizzazione, ad ognuno di essi si associa la probabilità che l'evento si verifichi. Se la probabilità è stimata in numero di volte che l'evento si è verificato nel corso di un anno, si parla di «annualized rate of occurrence» (ARO), ovvero tasso annuale di occorrenza.
I dati storici e le statistiche messe a disposizione degli enti pubblici possono sicuramente supportare la valutazione delle probabilità per quanto riguarda i disastri naturali.
-Valutazione degli impatti: Il risultato della fase è una misura qualitativa (basso, medio, alto) o quantitativa (e quindi espressa in forma monetaria) degli impatti sul business legati ad un determinato evento.
Da un punto di vista quantitativo: si assegna ad ogni asset quello che viene chiamato «exposure factor» (EF), misurato come la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento, e si introduce il concetto di «single loss expectancy» (SLE), che ci dà una misura monetaria della perdita che si subirebbe al verificarsi dell'evento, calcolato come il prodotto tra il valore dell'asset (AV) e la percentuale impattata in caso di evento (EF): SLE = AV x EF
Se volessimo ora il valore della perdita subita in un arco temporale di un anno, chiamato ALE (annualized loss expectancy), dovremmo moltiplicare il valore del SLE per il numero di volte stimato dell'evento in un anno (ARO): ALE = SLE x ARO
Da un punto di vista qualitativo, invece, bisognerebbe considerare tutti gli impatti «non numerici» sul business come ad esempio: Pubblicità negativa (immaginate una banca che non riesce ad assicurare servizio agli intestatari dei conti corrente); Sfiducia dei clienti; Responsabilità etica e sociale dell'organizzazione. Non restituisce un numero in valuta, ma piuttosto una stima degli impatti sul business di un dato evento.

Business continuity planning
Ha lo scopo di sviluppare ed implementare una strategia per la riduzione dell'impatto dei rischi sugli asset protetti. Possiamo identificare le seguenti sottofasi:
Sviluppo della strategia: lo sviluppo della strategia è un'attività complementare all'identificazione delle priorità, discussa nella fase di BIA. Infatti, se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo strategia si decidono i rischi che verranno gestiti all'interno del BCP. In questa fase il management deciderà quali rischi potrebbero essere accettabili, e quali invece no, quali rischi sono da evitare e quali invece inserire all'interno del BCP.
Stesura dei processi: all'interno di questa fase vengono dettagliati i processi e le procedure da seguire per la salvaguardia degli asset critici: personale, edifici ed infrastrutture. È bene ricordare che le persone sono sempre «l'asset» più significativo di una compagnia e pertanto devono essere dettagliati i processi per assicurare l'incolumità durante un'emergenza.

Approvazione ed implementazione
Nella fase di implementazione il team responsabile del BCP deve assicurarsi che tutte le risorse necessarie siano disponibili e che è stato organizzato, o erogato un piano di training per tutti gli impiegati che prendono attivamente parte al BCP. Infine, tutte le fasi precedenti

devono essere ampiamente documentate e rese disponibili per eventuale consultazione da parte degli impiegati.

Disaster recovery (DR)

Abbiamo visto il BCP, che ha lo scopo di supportare le organizzazioni nella riduzione degli impatti sugli asset prioritari a valle di un evento critico (governance, pianificazione e gestione).
Il **Disaster recovery planning (DRP)** può essere visto come il complemento tecnico al BCP che include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi dopo un evento catastrofico.
Insieme, il BCP ed il DRP, servono da guida durante i momenti di crisi o emergenza per recuperare l'operatività del business quanto prima così da impattare gli utenti fruitori del servizio quanto più lievemente possibile.

Bisogna considerare:

DISASTRI NATURALI	DISASTRI CAUSATI DALL'UOMO
Terremoti	Atti di terrorismo
Inondazioni	Esplosioni
Temporali	Interruzioni di corrente
Maremoti	Guasti infrastrutturali o di rete

I seguenti documenti devono essere presenti:
- Executive summary, ovvero un documento che andrà al management al cui interno sarà presenta una vista globale sul piano di disaster recovery
- Un documento tecnico per il personale IT responsabile dell'implementazione e della manutenzione dei sistemi
- Un piano d'azione per tutte le persone ingaggiate nel piano di disaster recovery
- Copie complete del piano di disaster recovery per i responsabili primari dell'implementazione e attuazione del piano

Tecniche e dei controlli utilizzati in fase di disaster recovery
-Resilienza dei sistemi: i controlli tecnici che aumentano la resilienza di sistemi impattano positivamente sulla disponibilità di sistemi e servizi, uno dei principi cardine della triade CIA. Si definisce resilienza di un sistema la sua capacità di far fronte a determinati eventi critici. L'obiettivo primario dei controlli in esame è di eliminare i cosiddetti «single point of failure» (SPOF), intesi come quei componenti del sistema che possono causare anomalie o cessazione dell'intero sistema.

-Tolleranza agli errori: «fault tolerance» è la capacità di un sistema di continuare ad essere operativo nonostante un errore. Essa si può aumentare aggiungendo ad esempio componenti ridondanti all'interno dell'architettura, come ad esempio un disco in più per il salvataggio dei dati.
-Protezione dei dischi: la tolleranza agli errori e la resilienza di un sistema possono essere rinforzate come abbiamo visto aggiungendo ridondanza, per esempio eliminando SPOF causati da dischi rigidi unici, tramite l'inserimento di dischi aggiuntivi secondo la configurazione RAID. Un vettore RAID infatti, include 2 o più dischi per garantire continuità di servizio anche quando uno dei dischi non risulta più disponibile.
-Configurazioni RAID: RAID-1: questa configurazione utilizza 2 dischi, entrambi contenenti gli stessi dati. Se uno dei due dischi smette di funzionare, il sistema non è impattato, in quanto il secondo disco ne assicura l'operatività.
RAID-5: questa configurazione utilizza 3 o più dischi, e tramite un tecnicismo chiamato «parità» implementa una soluzione che consente al sistema di funzionare anche se uno qualsiasi dei dischi smette di funzionare. La «parità» infatti rende possibile recuperare i dati sul disco non funzionante così da garantire continuità di servizio.
Il concetto di ridondanza può essere applicato a tutti gli asset critici, dove la ridondanza può dare un valore aggiunto al sistema. Quando parliamo di server, il concetto di ridondanza trova applicazione pratica nel «failover cluster», dove con cluster si intende un gruppo di computer che svolge generalmente lo stesso ruolo e che sono tra di loro sincronizzati, i singoli computer vengono chiamati anche nodi del cluster. Il «failover cluster» include due o più server e permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quando il server attivo smette di funzionare, l'altro nodo del cluster viene «promosso» a nodo attivo tramite un meccanismo automatico detto failover. Questo concetto può essere applicato a vari tipi di server ad esempio: web server che erogano servizi su internet, application server, database.
-Disponibilità elettrica: la tolleranza agli errori può essere applicata anche ai sistemi elettrici mediante l'utilizzo di generatori di corrente autonomi. Ad esempio se il data center che ospita tutti i server della compagnia subisse una perdita di corrente elettrica potrebbe causare molti danni.
-Backup: un piano di disaster recovery deve assolutamente prevedere una strategia preventiva di backup. Ovvero una strategia di come copiare i dati, i sistemi e le configurazioni attualmente in produzione al fine di recuperare l'operatività a fronte di un disastro. Tra le strategie di backup troviamo: Full backup, Incremental backup, Differential backup.
-Migration to cloud: fenomeno tecnologico della migrazione dei server da on-premise (utilizzo di server fisici) al cloud. Ad oggi, ci sono molti cloud service provider (CSP) come Google, Amazon, Microsoft che mettono a disposizione servizi in Cloud per le compagnie. Di conseguenza la stesura di un piano di disaster recovery deve anche considerare l'approccio adottato. Una compagnia potrebbe avere una parte dell'infrastruttura nei propri datacenter e quindi gestirne la sicurezza e il piano di disastro ed una parte completamente demandata al cloud provider, che in tale caso sarebbe anche parte responsabile delle politiche di disaster recovery.

Metodologie di disaster recovery
Possiamo identificare quattro diversi scenari:
-Cold site: questa modalità di ripristino prevede un secondo sito (una seconda sede) attrezzata con gli strumenti e le dotazioni per l'operatività del business da attivare dopo il disastro. Prevede dei costi di gestione sicuramente minori rispetto ad altre soluzioni, ma tra i contro troviamo i tempi di recupero piuttosto alti e il disallineamento dei dati rispetto al sistema primario.
-Hot site: è un sito sempre attivo, e dunque dispone dei dati sempre aggiornati. Lo spostamento da un sito primario ad un sito secondario in caso di disastro non comporta discontinuità di servizio. Tuttavia, tra i contro troviamo gli alti costi di gestione.
-Virtualizzazione: è l'adozione di ambienti virtuali in sostituzione ai server fisici. I motori di virtualizzazione mettono a disposizione delle compagnie tecnologie per replicare completamente l'ambiente informatico virtualizzato quali server, sistemi operativi, dischi per salvataggio di dati, applicazioni, database.
-Disaster recovery as a service (DRaaS): i cloud provider mettono a disposizione delle compagnie un modello di cloud chiamato «disaster recovery as a service», dove il cloud provider mette a disposizione un'infrastruttura in cloud che viene immediatamente attivata in caso di disastro sul sito primario della compagnia. Tra gli svantaggi troviamo i tempi di latenza per lo «switch» dal sito primario al sito secondario. Tuttavia, in termini di ottimizzazione budget è spesso la soluzione migliore considerato che si pagherebbe il servizio solo in caso di effettivo utilizzo.

PROCEDIMENTO

Per calcolare il danno subito dalla compagnia dobbiamo prima calcolare il danno monetario ogni qualvolta si verifica l'evento per poi moltiplicare per il fattore di occorrenza annuale.

SLE = AV x EF, dove:
AV: asset value -> valore monetario assegnati agli asset della compagnia
EF: exposure factor -> la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento
SLE: single loss expectancy -> una misura monetaria della perdita che si subirebbe al verificarsi dell'evento

ALE = SLE x ARO, dove:
ARO: annualized rate of occurrence -> numero di volte che l'evento si è verificato nel corso di un anno, tasso annuale di occorrenza
ALE: annualized loss expectancy -> il valore della perdita subita in un arco temporale di un anno

Inondazione - Asset Edificio secondario
AV= 150.000€
EF = 40%
SLE = 150.000 x 0,40 = 60.000€
ARO= 1 volta ogni 50 anni
ALE = 60.000 x 0,02(1/50) = 1200€/anno
Quindi, ogni volta che un'inondazione si verifica, l'impatto sulla compagnia per l'asset «edificio secondario» è di 60.000€. L'impatto sulla compagnia per l'evento inondazione sull'asset edificio secondario è di 1200€/anno.

Terremoto - Asset Datacenter
AV= 100.000€
EF = 95%
SLE = 100.000 x 0.95 = 95.000€
ARO= 1 volta ogni 30 anni
ALE = 95.000 x 0,03 = 2850€/anno
Quindi, ogni volta che un terremoto si verifica, l'impatto sulla compagnia per l'asset «datacenter» è di 95.000€. L'impatto sulla compagnia per l'evento terremoto sull'asset datacenter è di 2850€/anno.

Incendio - Asset Edificio primario
AV= 350.000€
EF = 60%
SLE = 350.000 x 0.60 = 210.000€
ARO= 1 volta ogni 20 anni
ALE = 210.000 x 0,05(1/20) = 10500€/anno
Quindi, ogni volta che un incendio si verifica, l'impatto sulla compagnia per l'asset «edificio primario» è di 210.000€. L'impatto sulla compagnia per l'evento incendio sull'asset edificio primario è di 10500€/anno.