KNOSSO
Knowledge for a Safe and Secure Organization

Disaster Recovery

Essenziale per la protezione informatica delle Organizzazioni pubbliche e private

Una importante perdita di dati è un evento estremamente dannoso e a volte può rendere problematica la stessa sopravvivenza dell'azienda. Senza un appropriato sistema che metta al riparo da eventi imprevisti, le conseguenze possono essere molto spiacevoli.

È ormai cronaca quotidiana, siamo tutti collegati e quindi tutti probabili target dei cyber attacchi.

Nel mirino soprattutto il settore manifatturiero del Made in Italy, tecnico-scientifico e i servizi professionali, con organizzazioni meno strutturate e più impreparate ad affrontare rischi cyber. A causa di scarsa consapevolezza o assenza di risorse.

In questi tempi di attacchi malware dolorosamente evidenti, nelle Aziende i Dipartimenti interni ICT sempre più spesso si trovano a dover affrontare i problemi legati alla necessità di proteggere le applicazioni critiche e l'infrastruttura tecnologica dalle diverse cause di downtime. Gli eventi disastrosi sono inevitabili e spesso imprevedibili per cui un'adeguata soluzione di Disaster Recovery rappresenta una forma di assicurazione per la protezione delle risorse IT, per i dati che custodisce e per i processi aziendali che supporta, proprio come una polizza assicurativa efficace: il Disaster Recovery ideale deve garantire la massima protezione al minor costo e ridurre al minimo i problemi.

Un'importante perdita di dati è un evento estremamente dannoso ed a volte può rendere problematica la stessa sopravvivenza dell'azienda. Senza un appropriato sistema che metta **al riparo da eventi imprevisti**, le conseguenze possono essere estremamente spiacevoli. La soluzione deve essere proporzionata ai rischi che l'azienda corre con il proprio modello di business e nel proprio contesto di mercato, **senza appesantirsi eccessivamente di costi**.

Il presente articolo illustra l'approccio generale alla definizione di un adeguato sistema di Disaster Recovery per la clientela business enterprise, sulla base di tre possibili scenari:

- ✓ cliente che ha già la sua infrastruttura e vuole un DR su un'infrastruttura fisica;
- ✓ cliente che ha già la sua infrastruttura fisica e vuole un DR sul Cloud;
- ✓ cliente che non possiede alcuna infrastruttura e vuole un DR 100% Cloud based.

Disporre dei migliori sistemi e processi di Disaster Recovery è indispensabile per chi fornisce il servizio e rappresenta una garanzia per il cliente. Nella realizzazione di un buon piano DR occorre:

- ✓ definire i processi e le procedure di emergenza per la dichiarazione del "Disastro" e l'attivazione del sito di DR;
- ✓ Accertarsi che tutti i servizi ed i dati critici siano ridondati sul sito di DR.

In via generale non è possibile definire una soluzione standard di DR applicabile a tutte le realtà di business. Ogni cliente va visto come un caso a sé stante e nella definizione di un DR va tenuto conto delle sue specifiche esigenze. Bisogna considerare ogni attività come "soluzione a progetto", da studiare insieme al cliente.

FASE DI PRE-ANALISI

Vengono identificati i possibili rischi e le probabilità relative. La scelta del sistema di DR da implementare parte dall'obiettivo che si desidera raggiungere e cioè del livello di servizio da assicurare.

Questo viene determinato attraverso due obiettivi di ripristino:

- ✓ RTO (Recovery Time Objective): il tempo che intercorre tra un'interruzione e il ripristino delle operazioni.
- ✓ RPO (Recovery Point Objective): il momento in cui i dati ripristinati sono stati salvati e riflette la massima quantità di dati che verranno persi durante il processo di ripristino.

DEFINIZIONE DELLA SOLUZIONE DI DR

Cliente che ha già la sua infrastruttura fisica e vuole un DR su infrastruttura fisica

Viene attivata un'infrastruttura fisica presso il data center prescelto, in grado di replicare ed erogare tutti o parte dei servizi del cliente. Si tratta di definire e configurare il giusto dimensionamento sulla base dell'infrastruttura esistente e secondo le modalità di ripristino dei servizi. Entrano in gioco elementi importanti quali le specificità dei servizi del cliente.

Vantaggi: risorse fisiche dedicate completamente al cliente, maggiore capacità computazionale.

Cliente che ha già la sua infrastruttura fisica e vuole un DR sul Cloud

La scelta del sito di Disatater Recovery può ricadere sull'attivazione di un'infrastruttura Cloud privata, quindi dedicata esclusivamente al cliente o pubblica, dove le risorse sono garantite ma condivise. In entrambe le soluzioni l'architettura IT in questione sarà localizzata all'interno di uno dei data center prescelti dal cliente, con possibilità di scegliere un data center italiano o una struttura situata all'estero.

Vantaggi: la virtualizzazione consente di ottimizzare l'architettura in termini di hardware necessario sul sito di DR e semplifica le operazioni di ripristino, sia in caso di effettivo disastro, sia di test delle procedure di DR.

Cliente che non possiede alcuna infrastruttura e vuole un DR 100% cloud based

È possibile definire una infrastruttura virtuale per entrambi gli ambienti (primario-produzione e secondario-Disaster Recovery) utilizzando un network di datacenter.

A seconda delle specificità del progetto, potrà essere conveniente realizzare un Cloud privato o pubblico.

Quali sono i vantaggi, innanzitutto massima flessibilità sul Cloud pubblico che si traduce nella possibilità di modificare il dimensionamento dell'infrastruttura sulla base di esigenze anche momentanee. Si ha lo stesso livello di flessibilità sia per l'ambiente di produzione sia per quello di DR. Nel caso si scelga una piattaforma pubblica si otterranno grandi benefici in termini di contenimento dei costi e scalabilità. Nel caso si tratti di un'infrastruttura privata il maggiore vantaggio sarà relativo alle performance garantite dall'ambiente dedicato. Sia a livello applicativo che di storage è possibile automatizzare e semplificare il fail over delle macchine virtuali, accelerando il processo di Disaster Recovery.

Cos'è la Business Continuity?

La Business Continuity per le organizzazioni è oggi più che mai determinante garantire la continuità dei servizi, sia per quanto riguarda i processi interni, che per quanto concerne l'erogazione nei confronti dei clienti finali. A tal proposito, la disciplina della Business Continuity è diventata via via più complessa nel corso degli anni.

Se negli anni Settanta era sufficiente che una linea di produzione funzionasse a dovere, con la trasformazione digitale occorre considerare tantissimi fattori non direttamente riconducibili alle operations, a cominciare dalle normative vigenti in merito alla conservazione e al trattamento dei dati, le cui violazioni possono rendere vano qualsiasi sforzo a livello puramente funzionale.

La Business Continuity è pertanto diventata una disciplina molto approfondita, che si concretizza nei sistemi di gestione (il BCMS – Business Continuity management system), indispensabili per garantire la continuità

operativa soprattutto nel caso in cui si verificassero incidenti a livello IT o altre situazioni impreviste, come i disastri naturali, le pandemie, le crisi globali delle supply chain e i sabotaggi su ampia scala.

Cos'è un Business Continuity Plan (BCP)

Il Business Continuity plan (BCP) è un documento che definisce come un'organizzazione deve agire per garantire la continuità operativa nel contesto di un incidente o di una interruzione non pianificata di uno o più servizi potenzialmente critici per la resilienza aziendale. Come vedremo, rispetto al classico piano di Disaster Recovery, il Business Continuity plan si pone ad un livello più elevato, comprendendo anche istruzioni utili per affrontare le emergenze per i processi, le risorse umane, gli stakeholder della supply chain e qualsiasi altro elemento potrebbe essere colpito in maniera critica.

A livello operativo, un Business Continuity plan contiene delle checklist molto pratiche in merito alle macchine, al backup dei dati e all'ubicazione degli storage utilizzati, indicando le procedure da eseguire nel caso in cui dovesse verificarsi una situazione di emergenza.

Nel contesto attuale, la resilienza aziendale è un valore garantito da molteplici fattori, peraltro in continua evoluzione. Rispetto a qualche anno fa, quando questo aspetto era più marginale, attualmente qualsiasi BCP efficiente considera anche gli scenari di incidente tipici della sicurezza informatica, uno dei fattori più critici per la continuità operativa dei sistemi, dato il costante incremento dell'attività cybercriminale, sia a livello quantitativo sia per quanto riguarda la capacità di colpire una varietà di industrie sempre più ampia.

Differenze tra BCP e Disaster Recovery plan

Il piano di continuità di business (BCP) e il piano di Disaster Recovery (DRP) costituiscono due dei componenti fondamentali del Business Continuity management system. In particolare, il DRP include le strategie operative per gestire le interruzioni che possono verificarsi a livello IT su server, reti, PC e dispositivi mobile. Il piano mira a fornire tutti gli elementi necessari per ripristinare la produttività a livello hardware e software in modo da soddisfare tutte le esigenze di business previste, assicurando in ogni caso la continuità anche durante le situazioni di emergenza.

Per capire come pianificare correttamente la gestione della continuità di business possiamo tracciare la seguente sintesi, relativa ai tre componenti fondamentali di un BCMS.

BIA (business impact analysis)

La valutazione degli impatti sul business consiste nella mappatura dei processi aziendali per definirne le rispettive criticità. Uno degli elementi più rilevanti della BIA è costituito dalla tempistica di ripristino da rispettare (RTO), oltre che dall'indispensabile mappa delle risorse necessarie a garantire che ciascun processo funzioni almeno al livello minimo richiesto.

BCP (Business Continuity plan)

Il piano di continuità di business, per offrire una definizione differente rispetto a quella fornita in apertura, è costituito dall'insieme di procedure formalizzate che guidano le organizzazioni nel rispondere all'incidente, recuperare e ripristinare i processi critici ad un livello di funzionalità accettabile, anche se non ottimale, e soprattutto di farlo entro il tempo di ripristino stabilito (RTO).

DRP (Disaster Recovery plan)

Il piano di Disaster Recovery, come il termine stesso suggerisce, si occupa di stabilire le misure necessarie per il recupero dei sistemi informatici in caso di incidente, documentando nel dettaglio le procedure da eseguire per garantire il corretto ripristino di tutte le funzionalità previste. Nelle casistiche di disastro sono contemplate sia quelle causate da una calamità naturale o da un incendio, che quelle causate da minacce di natura informatica, come l'attività cybercriminale.

Caratteristiche del Business Continuity plan

Il BCP deve integrare in maniera efficace tutti i componenti fondamentali della Business Continuity. Secondo quanto previsto da IBM sarebbe opportuno considerare:

- ✓ Organizzazione: oggetti relativi alla struttura, alle competenze, alle comunicazioni e alle responsabilità dei dipendenti;
- ✓ Strategia: oggetti relativi alle strategie implementate nei processi di business per completare le attività quotidiane assicurando la continuità operativa;
- ✓ Dati e applicazioni: oggetti legati al software necessario per abilitare le operazioni di business, oltre alle procedure di high-availability utilizzate per implementare il software stesso;
- ✓ Processi: oggetti legati al processo di business critico necessario per il funzionamento aziendale, a partire dai processi IT impiegati per assicurare il corretto funzionamento dei sistemi;
- ✓ Tecnologia: oggetti legati ai sistemi, alla rete e alla tecnologia necessari ad assicurare le operations e i backup continui dei dati e delle applicazioni;
- ✓ Strutture: oggetti che sono legati alla creazione di un sito di Disaster Recovery, qualora il sito primario dovesse risultare compromesso.

Perché è importante dotarsi di un Business Continuity plan

Per comprendere il reale valore di un Business Continuity plan efficace nel garantire la continuità di business dell'organizzazione è sufficiente pensare agli impatti negativi in termini di costi derivanti da downtime imprevisti e altre condizioni che impediscono di erogare correttamente i servizi previsti.

Quando si affronta tale argomento, ci si ritrova spesso al cospetto di uno studio realizzato da IDC, in merito ai costi relativi ai downtime imprevisti, calibrati per una company inserita nei Fortune 1000. Secondo IDC infatti:

Il costo medio di un downtime imprevisto varia da 1,5 milione a 2,5 milioni di dollari all'anno, il costo medio orario di un'infrastruttura ammonta a circa 100mila dollari all'ora, il costo medio orario legato all'interruzione di un'applicazione critica varia da 500mila dollari a un milione di dollari.

Per quanto riguarda le PMI i costi stimati da IDC si collocano su una scala inferiore rispetto al livello Fortune 1000, ma comportano danni che possono arrivare anche a diverse migliaia di euro al minuto, secondo parametri molto eterogenei, che dipendono sia dalla tipologia che dalla dimensione del business.

I fattori che incidono nella quantificazione dei costi legati alle interruzioni di servizio del business sono vari e comprendono ad esempio:

- ✓ Mancati ricavi;
- ✓ Risorse inutilizzate;
- ✓ Stress sul reparto IT;
- ✓ Insoddisfazione e calo di produttività dei dipendenti;

- ✓ Insoddisfazione dei clienti e rischio di incremento del churn rate (tasso di abbandono);
- ✓ Danno reputazionale per il brand;
- ✓ Sanzioni e conseguenze legali per violazioni di normative e accordi vigenti.

Come si può declinare il proprio BCP. Quando si tratta di definire un Business Continuity plan è opportuno considerare almeno tre obiettivi fondamentali; *la high availability, la continuità delle operations e il recupero dei dati in emergenza.*

- ✓ High availability: occorre prevedere le risorse, i sistemi e le procedure necessarie per garantire l'accesso alle applicazioni anche in presenza di guasti e malfunzionamenti a livello locale, a prescindere che interessino i processi, le location o l'infrastruttura IT (hardware e software);
- ✓ Continuità delle operations: occorre prevedere che i sistemi critici per la salvaguardia della funzionalità delle operazioni rimangano attivi anche nel caso di un'interruzione, come nel caso dei backup e dei programmi di manutenzione;
- ✓ Recupero dati in emergenza: occorre considerare delle procedure utili a recuperare i dati presso un differente data center, qualora quello primariamente previsto fosse reso inutilizzabile da incidenti o calamità.

Fatta questa doverosa premessa, occorre prevedere le vere e proprie fasi di realizzazione del Business Continuity plan, a cominciare dalla definizione degli obiettivi, focalizzando e cercando di misurare puntualmente i risultati, per verificare costantemente la rispondenza di quanto previsto dal BCP rispetto alle esigenze di business.

Una volta identificati gli obiettivi, occorre individuare gli stakeholder del piano. Le organizzazioni dovrebbero sempre nominare un Business Continuity manager, o un ufficio destinato a tale funzione, con almeno un referente per ogni linea di business.

Il Business Continuity manager deve in primo luogo identificare le necessità e le aree fondamentali per il business, che, in caso di fermo prolungato, rischiano di causare i danni più rilevanti all'azienda. Tale attività non può prescindere dalla valutazione dei rischi finanziari e operativi che possono verificarsi nei casi di emergenza e dei relativi impatti sul business, con l'obiettivo di individuare con accuratezze le conseguenze di ogni avversità.

Una volta definito il quadro analitico e le conseguenti valutazioni si hanno tutti gli elementi necessari per procedere con la redazione del Business Continuity plan, in cui vengono indicate le strategie per la gestione del rischio e la loro gestione durante il periodo dell'emergenza, con l'obiettivo di garantire il totale ripristino della continuità di business.

Dopo tutto questo si passa alla creazione del piano operativo, il Business Continuity Plan vero e proprio, in cui vengono indicate strategie di prevenzione del rischio e la sua gestione, il superamento dell'emergenza fino al ripristino della continuità del business.

Il piano va continuamente revisionato ed aggiornato, in modo da mantenere coerenti e pertinenti le misure individuate a fronte delle variazioni di business che intervengono in un determinato periodo. Genericamente l'aggiornamento del BCP è previsto su base annuale.

Per realizzare un BCP efficace è possibile avvalersi di vari framework, anche se non esiste un BCP valido per tutte le situazioni ed occorre diffidare delle soluzioni troppo pronte all'uso. Ogni azienda dispone infatti di caratteristiche ed esigenze anche molto specifiche che richiedono competenze o consulenze qualificate e dotate di una comprovabile esperienza sul campo.

In sintesi, il ciclo di vita di un Business Continuity plan contiene almeno le seguenti fasi:

- ✓ Raccolta e analisi delle informazioni, oltre alla definizione della BIA (analisi impatti business) e del RA (valutazione dei rischi);
- ✓ Pianificazione e sviluppo del piano;
- ✓ Implementazione del piano;
- ✓ Test del piano;
- ✓ Revisione e aggiornamento del piano.

Anche il Disaster Recovery diventa *as a service* con il modello DRaaS, che offre il vantaggio di una migliore sicurezza, automazione, resilienza alle minacce informatiche e l'incorporazione di tecnologie all'avanguardia, inclusa l'intelligenza artificiale. Questo servizio fornisce soluzioni di ripristino rapide e affidabili in un ambiente digitale che sta diventando più complicato e interconnesso, migliorando la protezione contro le minacce It e proteggendo la continuità di business. La crescente minaccia di attacchi ransomware accelera ulteriormente l'adozione, con le organizzazioni che cercano opzioni di ripristino rapide e affidabili. Lo scrive Markets and Markets nel suo nuovo report sul futuro del mercato del DRaaS o Disaster Recovery as a service.

L'ascesa del paradigma *as a service* per il Disaster Recovery si lega alla proliferazione dei dati. In questo contesto, il DRaaS sfrutta tecnologie come la deduplicazione e la compressione per ottimizzare lo storage e ridurre i costi. Ciò consente alle organizzazioni di gestire e proteggere in modo efficiente ed economicamente sostenibile grandi quantità di dati.

Dal punto di vista tecnologico, le soluzioni DRaaS incorporano intelligenza artificiale e automazione per migliorare l'orchestrazione del ripristino di emergenza. L'analisi predittiva e gli algoritmi di apprendimento automatico (machine learning) possono identificare potenziali vulnerabilità e attivare automaticamente le procedure di failover, risparmiando tempo prezioso durante le crisi. Inoltre, poiché le organizzazioni si affidano sempre più all'edge computing per l'elaborazione dei dati in tempo reale, il DRaaS estende la sua portata alle sedi periferiche. Ciò garantisce la Business Continuity anche nelle operazioni periferiche critiche e la replica dei dati nei datacenter centralizzati o nel cloud.

Infine ma non certo per ultimo il Disaster Recovery insieme alla Business Continuity, rivestono un'importanza primaria ai fini del GDPR (General Data Protection Regulation), infatti il Regolamento Europeo n°679/2016 è tra i temi più dibattuti in tema di Sicurezza informatica aziendale e ha come fine, disciplinare uno standard più semplice del trattamento e la circolazione dei dati relativi le persone fisiche e giuridiche, ovvero sia i cittadini e le organizzazione in tutti i Paesi membri dell'Unione Europea e offrire ai cittadini europei un senso di fiducia nelle nuove tecnologie e – soprattutto – sensibilizzare la aziende affinché riservino alla privacy la massima importanza in tema di Sicurezza informatica aziendale.

Hardware is easy to protect, lock it in a room, chain it to a desk or buy a spare. Information poses more of a problem: it can exist in more than one place, be transported halfway across the planet in seconds and be stolen without your knowledge" (Bruce Schneier)

Fonti: IBM Research; Markets and Markets ; Corcom, Centro Studi Confindustria; Francesco LA Trofa "Business Continuity plan: cos'è e perché averne uno: Articolo B. Costanzo su Airpress; Hermes Centro Studi Europeo.