White Paper

Disaster Recovery: chi fa il piano va sano e va lontano

A dirlo oggi sembra incredibile, ma c'è stato un tempo in cui l'informatica era solo un semplice, per quanto utile, accessorio nella vita lavorativa di un'azienda. Nel corso della lunga fase di transizione dal vecchio mondo analogico al nuovo futuro digitale è sempre stato possibile tornare a "fare le cose a mano": e ogni tanto lo si faceva, magari perché era più comodo, per abitudine o per scarso interesse a imparare qualcosa di nuovo, o magari perché i computer facevano le bizze e allora si tornava alla cara, buona carta & matita che non tradisce mai.

Certo, i PC aiutavano a fare tante cose, le rendevano più veloci ed evitavano di ripetere continuamente le medesime operazioni; potevano essere un vantaggio competitivo per chi li utilizzava – maggiore l'efficienza, migliore la posizione sul mercato – ma tutto sommato non erano proprio del tutto indispensabili. Diciamo la verità: alla fine in molte aziende erano poco più che macchine per scrivere potenziate sulle quali era anche possibile divertirsi ai videogiochi in pausa pranzo.

Gli anni sono passati, tante cose sono cambiate e il nostro mondo è andato sempre **più trasformandosi in direzione del digitale.** Se sei convinto che l'informatica sia ancora un semplice accessorio del tuo lavoro, prova a immaginare per un momento cosa sarebbe della tua attività se mancassero i computer.

Come potresti organizzare la gestione della produzione e delle vendite, ad esempio? La comunicazione e i pagamenti con clienti e fornitori? La contabilità, i rapporti con le banche, gli adempimenti fiscali? Magari la tua azienda si trova all'interno di un cosiddetto smart building, quindi senza un'infrastruttura IT ben funzionante è probabile che tu non riesca nemmeno ad aprire la porta d'ingresso col tuo badge.

Vedi bene come un ambiente informatico adeguato e privo di inconvenienti non si traduce più solamente in un pur necessario vantaggio competitivo: in realtà da esso dipende l'essenza stessa della tua attività. L'equazione fondamentale è: **IT funzionante = *azienda funzionante***. Chi non la rispetta oggi non perde un vantaggio competitivo, chiude e basta.

E attenzione, non è sufficiente aver progettato e messo in opera un ambiente IT come si deve: bisogna infatti assicurarsi che esso funzioni costantemente senza problemi. Guasti, attacchi da parte di cybercriminali e disastri ambientali come incendi e allagamenti sono sempre in agguato, pronti a trasformare la migliore delle infrastrutture in una inutile massa inerte di metallo e plastica. Una situazione dalla quale il 40% delle aziende non si riprende più, **chiudendo i battenti per sempre**[1].

Se invece vuoi essere sicuro di far parte dell'altro 60%, quello che supera indenne i momenti critici che prima o poi inevitabilmente accadono, il segreto è quello di evitare atteggiamenti attendisti o fatalisti e affrontare preventivamente i possibili problemi preparando quello che, in gergo, si chiama piano di *disaster recovery*.

Il vero disastro è far finta di niente

Se il termine tecnico può far pensare a qualcosa che può riguardare solamente grandi organizzazioni strutturate su vasta scala che dispongono di intere squadre di tecnici IT esperti, in realtà il **piano di disaster recovery** (o piano di DR) non è altro che una buona pratica studiata e definita in base alla specifica situazione di ciascuna azienda grande o piccola che sia.

Quel che cambia è solamente la complessità del piano: ovviamente più ampia e ramificata l'organizzazione, più saranno gli aspetti da tenere in conto e gestire; più sensibile la natura dell'attività, più sofisticati dovranno essere gli strumenti da utilizzare per rispondere alle criticità.

Detto in altre parole, il piano di disaster recovery di un piccolo studio di architettura composto da un professionista e un paio di collaboratori avrà caratteristiche differenti da quello di un impianto chimico farmaceutico. Resta immutato lo scopo del piano, ovvero quello di assicurare continuità di funzionamento in caso di problemi e la salvaguardia dei crescenti patrimoni di dati e informazioni che costituiscono ormai la linfa vitale di qualsiasi attività.

Per capire meglio le sue caratteristiche, vediamo rapidamente come è strutturato di solito un normale piano di DR:

- Un buon piano di DR stabilisce innanzitutto una serie di obiettivi fissando i limiti di tempo di inattività e la quantità di dati che si possono perdere senza compromettere la ripartenza dell'azienda e la sua capacità di sopravvivenza;
- Il piano di DR assegna **compiti** precisi a figure specifiche, affinché ciascun dipendente sappia esattamente come comportarsi nel momento in cui occorre entrare in azione evitando malintesi e perdite di tempo;
- Senza una mappa si rischia di muoversi alla cieca, ed è per questo che i piani di DR contengono un **inventario** dei sistemi IT che ne riassume la collocazione fisica, le funzioni a cui sono assegnati, i dati e le applicazioni che contengono, e il relativo livello di criticità;
- Una risorsa essenziale per qualsiasi azienda è il **backup**. Il piano di DR elenca tutti i backup che vengono effettuati indicandone la frequenza e la tipologia dei dati che vi sono contenuti, oltre alle procedure necessarie per il loro ripristino;
- Gli eventi disastrosi possono prolungarsi nel tempo, quindi è importante che il piano di DR tratteggi anche tutte le procedure utili a **mitigare** o circoscrivere i danni;
- L'ultima voce di un piano di DR riguarda il cigno nero che nessuno vorrebbe mai incontrare, poiché è quella che specifica tutto ciò che occorre fare per tornare al pieno **recupero** dell'attività in seguito a una perdita totale catastrofica di tutti i sistemi e di tutti i dati.

Come puoi vedere, un piano di disaster recovery non è altro che un manuale per tutte le situazioni di emergenza che possono colpire l'ambiente IT di un'azienda in modo da minimizzarne gli effetti negativi.

Non sottovalutarne l'importanza crogiolandoti nella comoda illusione "perché tanto a me non succede". Le casistiche di disastro sono davvero tantissime e non guardano in faccia a nessuno:

- **cause provocate dall'uomo**: sono gli effetti di comportamenti dolosi o involontari, per esempio PMI che perdono tutti i dati per via degli attacchi ransomware cui sono sottoposte quotidianamente [2], furti di apparecchiature elettroniche [3], oppure data center (interni piuttosto che dei provider esterni a cui ci si appoggia) distrutti da incendi [4] purtroppo sempre possibili;
- **cause naturali**: terremoti e inondazioni possono essere casi limite, ma la crescente frequenza di fenomeni meteoclimatici estremi sta diventando una preoccupazione molto concreta. Bombe d'acqua [5], trombe d'aria, ondate di calore [6] possono avere effetti dirompenti sia direttamente nell'area in cui si verificano, sia indirettamente e a distanza, ad esempio provocando blackout elettrici di durata più o meno lunga.

Come creare un buon piano e dormire tranquilli

Vale la pena ripetere che un piano di DR è qualcosa **alla portata di qualsiasi azienda**, uno strumento che può tornare utile a chiunque indipendentemente da dimensioni organizzative, volumi di dati o criticità dei sistemi.

Un buon piano non nasce semplicemente mettendosi a ragionare a tavolino ma è frutto di una serie di attività preparatorie necessarie a ottenere tutte quelle informazioni oggettive su cui saranno successivamente costruite le varie procedure da seguire in caso di emergenza.

Si tratta di una fase molto importante dalla quale spesso scaturiscono vere e proprie sorprese, come magari scoprire che il sistema a maggior traffico non era quello che si pensava che fosse o che nelle pieghe dell'infrastruttura IT si trovano risorse inutilizzate, utenze obsolete o dispositivi isolati dal resto dell'ambiente. In questo senso, la redazione del piano di DR rappresenta anche una **preziosa occasione** per mettere un po' di ordine, specialmente in quei contesti che sono cresciuti un po' troppo velocemente rispetto alle effettive capacità di gestione dei suoi amministratori.

Vediamo ora più in dettaglio come si articola la preparazione di un piano di DR.

Assessment

La valutazione preliminare dell'ambiente IT, dei suoi sistemi e dei suoi dati. Un lavoro di investigazione che prende il via dall'eventuale documentazione esistente **verificandola e integrandola** attraverso una ricerca sul campo. Da qui si capisce quali sono le risorse – sia fisiche, come macchine e dispositivi, che immateriali, come le informazioni – che sono prioritarie per l'attività dell'azienda e da quali altri sistemi esse dipendono.

L'obiettivo infatti non è solamente stilare un elenco di ciò che è importante, ma anche definire le relazioni e i collegamenti esistenti al fine di avere chiaramente consapevolezza del percorso lungo cui si snodano i flussi dell'intero ambiente IT. In questo modo si potrà proteggere adeguatamente non solo la risorsa prioritaria (esempio: un database che memorizza informazioni in tempo reale), ma anche i sistemi complementari da cui dipende il suo funzionamento (esempio: i sensori che alimentano quel database e i segmenti di rete che uniscono il tutto).

Nella fase di assessment non è insolito imbattersi in situazioni aggrovigliate o inutilmente complesse. In questo caso è opportuno intervenire per semplificare e razionalizzare il necessario: ne guadagnerà la normale efficienza operativa dell'azienda così come la rapidità delle eventuali operazioni di DR che dovessero mai servire. Già questo sarebbe sufficiente a giustificare tutto il lavoro di assessment!

Criticità

Mappate le risorse esistenti, è il momento di assegnare un punteggio di criticità che aiuti a differenziare l'importanza che ciascuna di esse riveste ai fini del business.

Questa fase richiede una approfondita conoscenza delle strutture produttive e amministrative dell'azienda; se l'assessment serve a ricostruire la catena di ripristino e riavvio dei sistemi più appropriata dal punto di vista tecnico, adesso è ora di fare lo stesso concentrandosi sul lato organizzativo del lavoro.

Per esempio, un'attività prettamente commerciale con una limitata capacità produttiva potrebbe trovare più vantaggioso assegnare la priorità alla gestione del magazzino e delle spedizioni. Un'azienda specializzata invece nella produzione just-in-time su commissione vorrà assegnare la precedenza ai sistemi produttivi rispetto a quelli che gestiscono il magazzino in uscita. Lo stesso ragionamento vale per altri aspetti come gestione finanziaria, supporto post-vendita e così via.

Incrociando il risultato della fase di assessment con la scaletta ragionata delle priorità di business si inizia a delineare un quadro preciso dei **punti su cui occorre intervenire** a prescindere e quelli su cui è possibile agire in un momento successivo o a seconda delle necessità del momento. In questo modo non si perderà tempo inutilmente concentrandosi su risorse di secondaria importanza.

Analisi del rischio

Ma quali sono le minacce che l'azienda si trova ad affrontare nella realtà? Saperlo aiuta innanzitutto a minimizzare il rischio intervenendo dove necessario con un rafforzamento delle difese.

In genere si parte con qualcosa che non risparmia nessuna attività: gli attacchi cybercriminali a scopo di spionaggio, estorsione o vendetta. La valutazione permette di identificare i sistemi critici e quantificare i rischi di attacco interno ed esterno verificando quindi il grado di protezione in vigore. Da qui può seguire ovviamente un intervento di rafforzamento delle misure in atto, se necessario, per poi procedere con la definizione delle azioni da effettuare nel momento in cui venga rilevato un attacco in corso o, nel caso peggiore, una volta che un attacco sia stato completato con successo danneggiando i sistemi dell'azienda.

Un ragionamento simile va fatto anche per tutti gli altri rischi che si possono realisticamente correre: guasti informatici diretti o in conseguenza di altro avvenimento; catastrofi naturali, dall'allagamento causato da un forte temporale estivo fino al terremoto (qui può venire in aiuto la mappa di rischio sismico del territorio italiano approntata dall'INGV[7]); attività criminali o disordini sociali, in particolare per attività con sede in aree disagiate o di abbandono urbano; atti terroristici o di guerra, che possono colpire aziende sensibili operanti nella filiera della difesa o comunque esposte all'opinione pubblica.

Un consiglio: in questa fase è sempre utile chiedere l'opinione degli utenti finali presenti in azienda. Trovandosi quotidianamente a diretto contatto con i sistemi e le risorse che si intende proteggere, essi sono a conoscenza di rischi concreti che potrebbero sfuggire a una pur accurata analisi effettuata però lontana dal campo.

Obiettivi di ripristino

Un piano serve a poco se non fissa nero su bianco i risultati che si vogliono raggiungere. In questo caso si tratta di definire **la situazione alla quale bisogna idealmente tornare operativi** in seguito a un evento disastroso e le tempistiche disponibili per poterlo fare.

No, "prima possibile" non è una risposta: occorre fissare obiettivi realistici in base alle specificità della propria attività e del proprio ambiente. Dal momento che l'implementazione pratica di un piano di DR comporta inevitabilmente tempo, lavoro e costi, è sempre buona cosa che queste risorse siano allineate alla realtà dell'azienda e delle sue esigenze effettive per evitare sprechi e complicazioni inutili.

In genere gli obiettivi di ripristino si concentrano su due parametri fondamentali:

- **RTO o Recovery Time Objective**: è il tempo che possiamo permetterci di lasciar passare tra l'evento disastroso e il ritorno all'operatività. Viene calcolato in base a quanto l'azienda può restare ferma e dipende ovviamente dal tipo di attività che svolge, dalla natura dei suoi clienti, dagli accordi contrattuali esistenti e dai requisiti tecnici della produzione. Può essere utile determinare più RTO a partire da un valore ottimale che minimizza le conseguenze negative dell'evento per poi fissare l'entità delle perdite che subentrano per RTO più lunghi;
- **RPO o Recovery Point Objective**: semplificando possiamo definirlo come il tempo che intercorre tra un backup e l'altro. Poiché i ripristini fanno affidamento sui backup più recenti disponibili, il valore di RPO si traduce nella quantità di dati che possiamo permetterci di perdere, quantità proporzionale all'intervallo tra due backup. Se non l'hai mai fatto prima, calcolare il tuo RPO è essenziale per avere un riscontro oggettivo sull'adeguatezza dei tuoi piani di backup.

Una volta che avrai definito correttamente i tuoi obiettivi di ripristino avrai chiare le priorità sulle quali concentrare gli sforzi, sia per la preparazione del piano di ripristino sia per l'esecuzione dello stesso in malaugurato caso di necessità.

Scelta degli strumenti

A questo punto hai ottenuto un quadro completo della tua azienda: situazione attuale, rischi, obiettivi, priorità, tutto quello che ti occorre per passare all'azione e metterti effettivamente al riparo.

Per poterlo fare dovrai tuttavia dotarti di **una o più soluzioni adatte**. Il mercato mette a disposizione migliaia di applicazioni, sistemi, dispositivi hardware e apparecchiature virtuali per ogni necessità di backup e disaster recovery. Ogni prodotto si differenzia dagli altri per una serie di caratteristiche, tra le quali:

- tecnologia impiegata
- ricchezza e varietà delle funzionalità dedicate
- semplicità di installazione, configurazione e utilizzo
- affidabilità e sicurezza
- compatibilità con l'ambiente esistente
- aderenza a standard tecnici e normativi
- volumi di dati e dimensione dell'ambiente da proteggere
- possibilità di integrazione con altre soluzioni
- costo di acquisto e manutenzione
- disponibilità di assistenza e aggiornamenti

Dunque la fase di selezione richiede una certa attenzione andando a incrociare la propria personale mappa dei requisiti con quello che le varie soluzioni offrono. Consultare i siti e il materiale informativo dei produttori non è sufficiente ma permette di restringere i candidati per poi approfondire – magari attraverso qualche dimostrazione o il ricorso all'esperienza di esperti – l'effettivo allineamento tra caratteristiche del prodotto, promesse del produttore ed esigenze della tua azienda.

In questa fase, oltretutto, non è raro imbattersi in qualche novità di mercato basata sull'ultimissima tecnologia disponibile che promette di fornire la risposta definitiva a qualunque necessità di DR. Non accettare mai queste

affermazioni a scatola chiusa ma verificale sul campo. Il settore è effettivamente molto innovativo, ma la tecnologia non va mai adottata come scelta fine a sé stessa bensì sulla base della propria peculiare situazione.

Definizione del budget

Ne abbiamo accennato tra gli elementi che conducono alla scelta dei tool necessari a mettere in pratica il piano di DR, ma in realtà è un parametro che si presenta come il convitato di pietra in tutte le fasi viste sinora e in tutti i ragionamenti che circondano una strategia di continuità operativa aziendale: **il costo**.

Non è possibile infatti evitare di bilanciare qualunque progetto o soluzione con la realtà dei budget disponibili, tenendo conto che non si tratta solamente di quantificare l'investimento iniziale rispetto alle performance desiderate, bensì di proiettare la previsione degli impegni di denaro, di tempo e di risorse lungo tutto l'arco di esistenza e funzionamento del piano. Quello che gli esperti definiscono come TCO o Total Cost of Ownership – costo totale di possesso – rappresenta infatti un buon indicatore per capire la sostenibilità finanziaria di una soluzione.

Un prodotto potrebbe anche esserci proposto a un prezzo davvero conveniente, ma richiederci poi in realtà un notevole lavoro di implementazione e manutenzione. Viceversa, un prodotto che appare più caro all'acquisto potrebbe essere dotato di funzionalità di automazione tali da minimizzare successivi interventi da parte del personale tecnico o di consulenti esterni.

La stessa cosa può valere per l'hardware, dove alcune configurazioni a prezzi stracciati possono nascondere costi proibitivi in caso di ulteriore ampliamento della capacità oppure essere legati a contratti di assistenza e manutenzione particolarmente onerosi.

Da considerare anche la crescente diffusione di modelli commerciali "as-a-Service" o "pay-as-you-go" che altro non sono che abbonamenti a consumo: il loro pregio è quello di evitare immobilizzi di capitale e relativi ammortamenti per l'acquisto iniziale di una soluzione spostando il costo patrimoniale a una voce di spesa ordinaria immediatamente detraibile e allineata all'uso effettivo di una soluzione: più si consuma e più si spende, ma in genere le crescite dei consumi sono la conseguenza di un incremento del business e quindi il maggior costo è legato a maggiori entrate.

Test, verifiche e revisioni

Puoi aver architettato il piano di DR più bello del mondo ed esserti portato in casa le soluzioni più sofisticate, potenti e innovative del pianeta – ma tutto questo è destinato a rimanere un puro esercizio teorico fintanto che non lo avrai messo alla prova facendolo scontrare **con la realtà sul campo**.

Dunque la parte finale del tuo piano deve prevedere la simulazione di un disastro o, meglio ancora, di varie tipologie di disastro di differente gravità:

- **l'inaccessibilità** di qualche database o applicazione, come se ci fosse stato un cyberattacco con conseguente indisponibilità di informazioni e funzionalità;
- **lo spegnimento** di un dispositivo chiave del tuo ambiente IT, per vedere cosa succede nel caso in cui si dovesse guastare;
- **un distacco improvviso** della corrente nelle varie aree della tua azienda seguito da un distacco generale, per verificare il comportamento a fronte di avvenimenti catastrofici.

È l'unico modo per essere certi che il tuo piano funzioni non solo sulla carta, consentendoti di apportare modifiche e correttivi in caso di necessità prima di doverlo scoprire nel momento meno opportuno. Certo, si tratta di un investimento di tempo e di denaro che oltretutto provoca sempre qualche palpitazione (c'è sempre quella vocina che sussurra: "e se non dovesse funzionare?"). Ma l'alternativa sarebbe quella di scoprire se tutto va bene solamente quando non c'è più spazio per gli errori, i ripensamenti, le modifiche e le aggiunte. Quando una banale dimenticanza, facilmente individuabile in occasione di un semplice test, si trasforma invece nell'impossibilità di ripartire del tutto.

Si tratta di far tesoro di un detto militare che recita: nessun piano di battaglia sopravvive all'impatto col nemico. Significa che, per quanto ci si sforzi di prevedere l'imprevedibile, la realtà dei fatti ha sempre in serbo qualcosa a cui non si era pensato. I test sul campo servono proprio a minimizzare questa evenienza e intervenire tempestivamente laddove qualche elemento del piano di DR non si comporti come previsto.

Ogni tanto sui giornali si può leggere di qualche azienda che ha perso tutti i propri dati e la propria capacità tecnologica a seguito di un guasto, di un attacco ransomware o di qualche calamità naturale. Basta approfondire la notizia per scoprire come in quasi tutti i casi il problema non sia dovuto all'assenza di backup – in fondo oggi è ben difficile imbattersi in un'attività talmente fuori dal mondo da non avere alcun genere di backup, per quanto elementare – bensì dal fatto che i backup esistenti si sono rivelati inutili nella pratica[8]. Senza test adeguati, meglio ancora se periodici, non potrai essere certo che lo stesso non possa capitare anche a te.

Piano piano... siamo arrivati al dunque: ora tocca a te

Come hai visto, redigere e implementare un piano di DR è **la migliore assicurazione** che puoi accendere per minimizzare il rischio di dover chiudere i battenti della tua attività a causa della perdita di una risorsa tanto critica come l'IT nelle sue varie sfaccettature.

Hai anche potuto vedere come alcuni passaggi della realizzazione di un buon piano di DR richiedano competenze specifiche e una certa esperienza pratica. Il consiglio è quindi di iniziare a parlarne con gli specialisti a cui già ti affidi per l'erogazione dei tuoi servizi IT: sono interlocutori qualificati che possono darti suggerimenti efficaci mentre approfondiscono gradualmente le caratteristiche del tuo ambiente IT e della tua attività.

Un piano di DR potrebbe rivelarsi uno dei migliori investimenti che tu abbia mai effettuato per la tua azienda. Se anche non dovrai mai metterlo in pratica, come ti auguriamo, ti sarà comunque servito non solo per dormire più tranquillo la notte, ma anche per verificare, valutare e ottimizzare alcuni importanti aspetti del tuo ambiente esistente rendendolo ancora più robusto, agile e affidabile.

Di fronte a vantaggi del genere, non far nulla restando alla finestra non ha davvero alcun senso.

Glossario

Cloud – Un modello di erogazione di servizi informatici attraverso un'architettura distribuita. Le risorse che costituiscono un ambiente cloud vengono condivise tra i diversi utilizzatori e possono essere scalate in modo elastico senza provocare interruzioni operative. Vi sono differenti tipologie di cloud: pubblico, la cui infrastruttura non appartiene all'utente finale a differenza del cloud privato; ibrido, formato da un mix di ambienti cloud e tradizionali; e multicloud, composto da più servizi cloud di tipologie e fornitori differenti.

Malware – Combinazione dei termini inglesi "malicious" (malevolo, pericoloso, illecito) e "software". Indica l'insieme degli strumenti software che i cybercriminali utilizzano per entrare nei computer delle loro vittime, assumerne il controllo in modo parziale o integrale, propagarsi all'interno della rete colpita ed effettuare attività illecite come la sottrazione di dati personali o sensibili, lo spionaggio, l'invio di messaggi di posta indesiderata o il blocco crittografico dei dati a scopo di riscatto. Ognuna di queste attività assume una propria denominazione, come spyware, spamware, ransomware ecc.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.