giornale delle Assicurazioni

Mensile

Data 05-2012
Pagina 66/67
Foglio 1 / 2

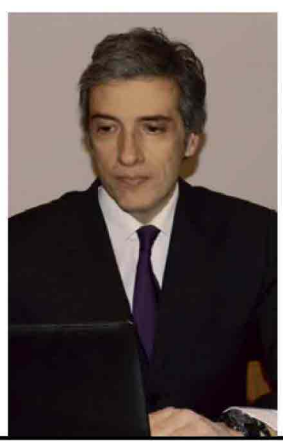
BUSINESS CONTINUITY Nuove strategie

Disaster recovery in outsourcing

Reale Mutua e Rsa svilupparno i piani di ripristino insieme a partner tecnologici. Con l'obiettivo di accelerare il processo di recupero dei dati.

Michela Montagna

Non tutte le compagnie assicurative sono partite con un piano unitario di business continuity. Molte aziende assicurative, infatti, si sono limitate all'organizzazione del disaster recovery (attivo da molto tempo), rimandando un'organizzazione più organica della business continuity alle scadenze stabilite dalla *compliance*. Così, per gran parte delle imprese del settore, continuità operativa significa (almeno fino a oggi) sito gemello, backup in un ambiente remoto e, in alcuni casi, outsourcing. Le compagnie offrono spesso in locazione spazi fisici all'interno dei centri funzionali, per ospitare i sistemi informativi gemelli, che devono essere costantemente allineati, per essere attivati immediatamente in caso di guasto. In questo modo, le aziende assicurative possono contenere le spese di gestione di applicazioni critiche, che richiederebbero infrastrutture autonome molto costose.
Tuttavia, si tratta di ambienti informatici che non vengono replicati istantaneamente e tra la caduta e il ricorso al sistema di emergenza è previsto un tempo di inattività che varia a seconda della criticità dei processi. L'obiettivo? Salvaguardare le informazioni, ottimizzando la convergenza tra attività di stoccaggio, governo dei dati e gestione delle emergenze. E di ripristino immediato dei sistemi e dei collegamenti in caso di fermo.
Il *Giornale delle Assicurazioni* ne ha parlato con i responsabili dei progetti di disaster recovery di Reale Mutua assicurazioni e Royal Sun Alliance.



Reale Mutua «I nostri sistemi informatici non sono ancora in regime di business continuity, ma, attraverso il piano di disaster recovery che abbiamo predisposto, possiamo garantire l'erogazione del servizio, anche in caso di danno grave al sito primario. Abbiamo puntato a un *recovery time objective* che prevede il pieno recupero dell'operatività dei sistemi in 24 ore», afferma **Alfredo Robusto**, responsabile sicurezza e continuità del business di Reale Mutua, «un progetto che si basa sulla replica dei dati in modalità asincrona, effettuata con tecnologia *Hp continous access*, e prevede un tempo massimo di dieci millisecondi tra la produzione delle informazioni e la loro messa in sicurezza».
Da inizio 2012, la società si è affidata all'outsourcing per la gestione delle strategie di ripristino, attraverso un contratto che prevede l'*housing* dell'infrastruttura primaria presso Cedacri (nella sede di Collecchio, *ndr*) e l'erogazione dei servizi di disaster recovery da un sito secondario, di proprietà del fornitore. «Le modifiche infrastrutturali sono gestite attraverso un processo di *change management* tecnologico, per consentire il continuo aggiornamento delle strutture hardware e software. Il sito gemello si trova a Castellazzo Bormida, presso il data centre Cedacri, dove i dati vengono replicati e stoccati in ambiente ad atmosfera controllata. Le modifiche ai sistemi che non vengono replicati automaticamente avvengono comunque in concomitanza con gli aggiornamenti degli applicativi di produzione, in presenza di una specifica autorizzazione comunicata dall'azienda».
La strategia prevede che vengano effettuati *crash test* periodici, al fine di verificare il costante allineamento delle strutture e i tempi di attivazione dei sistemi di emergenza. Vi sono tuttavia livelli diversi, a seconda della criticità dei processi coinvolti: «Tutto il sistema di disaster recovery, come da contratto con il fornitore, viene testato quattro volte all'anno», ricorda Robusto. «Ma le applicazioni non sono state inserite nel progetto con le stesse modalità e tempistiche di attivazione. L'analisi di impatto sul business, che viene effettuata ogni anno, ci consente di individuare i contenuti e i processi chiave, per identificare modalità di salvataggio diverse, sia per quanto riguarda il tempo che intercorre tra la produzione del dato e la sua messa in sicurezza, sia dal punto di vista del

Modalità asincrona
«Reale Mutua ha puntato a un recovery time objective che prevede il pieno recupero entro 24 ore», afferma il responsabile sicurezza e continuità del business Alfredo Robusto. «Il progetto si basa sulla replica dei dati in modalità asincrona, e prevede un tempo massimo di dieci millisecondi tra la produzione delle informazioni e la loro messa in sicurezza».

giornale delle Assicurazioni

Mensile

Data 05-2012
Pagina 66/67
Foglio 2 / 2

Visione organica
Molte compagnie si sono limitate all'organizzazione del disaster recovery, rimandando una visione più organica della business continuity alle scadenze stabilite dalla compliance.

tempo necessario per il pieno recupero dell'operatività. Per gli ambienti a più alta criticità, per esempio, sono previsti server configurati in *cluster* a più nodi, che, in caso di *fault*, possono provvedere alla continuità del servizio».

In questo tipo di struttura, i server rappresentano una singola risorsa *computazionale*: il cluster può avere prestazioni più elevate, poiché, anziché gravare su di un unico sistema, suddivide il lavoro su più macchine. E per le componenti a impatto minore, come le connessioni di rete con le strutture distributive, i siti periferici e le altre compagnie del gruppo? «Tutte le connessioni sono ridondate, sia attraverso un collegamento con il nostro sito principale, sia utilizzando connessioni dedicate con il sito di disaster recovery», dice Robusto. «Tutte le architetture sono realizzate con tecnologia Mpls su reti Telecom e Fastweb. In caso di crollo del sistema, vengono effettuate le variazioni ai routing, tramite sistemi di autenticazione che utilizzano il protocollo Ospf/Bgp. Si tratta di un sistema di instradamento dei collegamenti che agisce nel cuore della rete internet, collegando tra loro diversi sistemi autonomi. Queste operazioni, effettuate sulla struttura hardware della rete (che si trova nel sito gemello) possono essere eseguite sia dai dipendenti dell'azienda, sia dall'outsourcer, che è in possesso, all'occorrenza, di specifiche credenziali di accesso».

Linee dedicate
«Abbiamo fatto in modo di dotare tutte le nostre agenzie di linee dedicate, che possono tuttavia essere sostituite, in caso di crash, da una normale connessione internet», dice Riccardo Roncon, information security e disaster recovery manager di Rsa.

Rsa In collaborazione con Ibm, Rsa ha sviluppato una strategia di system recovery, per consentire la ripresa dei servizi core nell'arco di 24 ore dalla caduta del sistema. La strategia prevede tre fasi: la dichiarazione dell'emergenza, l'attività di ripristino presso il sito gemello e la ripresa, che si conclude con il rientro dei servizi ripristinati nel centro elaborazione dati primario. L'obiettivo è quello di coordinare una serie di procedure che porti al ripristino dell'intero sistema nel minor tempo possibile e con una minima perdita di dati. Un'operazione che presuppone differenti criticità, legate all'importanza dei processi interessati e coinvolge tutti i collegamenti. Anche quelli telefonici. «Attualmente», spiega **Riccardo Roncon**, information security e disaster recovery manager di Rsa, «siamo in grado di ripristinare i sistemi di business in 24 ore, in 36 i sistemi critici e in circa 70 l'intero sistema informatico. Abbiamo inoltre realizzato un progetto, in collaborazione con il nostro provider telefonico, per ripristinare anche l'intero apparato dedicato alla telefonia: in caso di *fault* che colpisca una delle nostre sedi, è possibile trasferire le utenze sull'altra o sulla *work area* presso Ibm, mantenendo gli stessi numeri. In questo modo, i nostri dipendenti sono sempre raggiungibili anche in caso di crollo del sistema, per garantire la continuità del servizio. L'intero sistema di ripristino sfrutta la procedura "a freddo", che prevede l'attivazione di un sistema alternativo: una sede cablata che si attiva solo *on demand*, con costi più contenuti rispetto alla modalità sincrona, ma tempi di ripristino più lunghi».

Come viene aggiornato il sito gemello? «Tutti i sistemi vengono sottoposti a backup notturni duplici. Una copia viene custodita all'interno della sede dell'azienda, per il *restore* dei dati dell'utente, mentre la seconda è prelevata da un fornitore specializzato e trasportata in un caveau di massima sicurezza che si trova vicino al sito di disaster recovery di Settimo Milanese. In caso di caduta del sistema i nastri vengono portati nel centro Ibm per le operazioni di ripristino».

In che modo trasferite le connessioni degli utenti dal sito tradizionale a quello di emergenza? «Nel sito di disaster recovery presso il centro Ibm abbiamo installato applicativi e componenti di rete pronte, in caso di evento catastrofico, a essere configurate sulla base degli apparati di produzione che si trovano presso la sede principale di Genova», risponde Roncon. «Le linee dati vengono ripristinate in tutte le loro funzionalità in quattro ore dalla caduta del sistema. Per quanto riguarda invece i collegamenti con la rete agenziale, abbiamo fatto in modo di dotare tutte le nostre agenzie di linee dedicate, che possono tuttavia essere sostituite, in caso di crash, da una normale connessione internet».

Per le funzioni a elevata criticità, la compagnia londinese ha previsto anche un sistema di replica delle informazioni, che avviene in tempo reale all'interno della sede principale di Genova, attraverso sistemi di storage con server configurati in cluster: «Recentemente abbiamo implementato una strategia di business continuity che prevede la replica sincrona dei dati, attraverso due sistemi di storage che si alimentano in tempo reale, per consentire la disponibilità del dato in caso di fault di uno dei due», dice Roncon. «L'obiettivo è quello di azzerare i tempi di disservizio».

L'intero sistema viene testato una volta l'anno presso il centro Ibm per provarne l'affidabilità e i tempi di ripristino dei dati e della rete. «Il test prevede il coinvolgimento di tutti gli utenti delle nostre sedi e, una volta eseguito l'esercizio di *recovery*, si apre immediatamente una fase di *remediation activity*, con lo scopo di analizzare e affinare le procedure per migliorare il piano di gestione delle emergenze». ■