PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5267 di Mercoledì 2 Novembre 2022

Un piano di disaster recovery per un sistema informatico

Durante un recente convegno, un esperto ha presentato un disaster recovery Plan in quattro passi, che merita di essere attentamente studiato da tutti coloro, cui aziende, pubbliche e private, affidano la responsabilità di gestione del sistema informativo.

Non v'è dubbio che la messa punto di un piano di disaster recovery, per un sistema informatico, non è un'operazione che può essere sviluppata in pochi minuti, seduti da soli a un tavolino. Si tratta di un'attività oltremodo impegnativa, che coinvolge numerose figure aziendali e che deve essere tempestivamente elaborata e costantemente messa a punto.

Questo problema si pone in modo particolare per le piccole e medie aziende, che spesso ritengono che un sistema informativo, di ridotte dimensioni, sia più facilmente gestibile, in caso di emergenza. L'esperienza mostra che questo convincimento non è affatto vero ed il responsabile della sicurezza informatica deve attivarsi, in modo appropriato, per sensibilizzare la direzione aziendale su questo tema.

Vediamo ora i quattro passi in cui si articola l'impostazione e lo sviluppo di un piano di disaster recovery.

La valutazione dell'impatto

Quando si sviluppano analisi di rischio, i parametri fondamentali da prendere considerazione sono la valutazione di impatto e la frequenza dell'impatto stesso. Nel nostro caso evidentemente si prende in considerazione solo il primo parametro.

Occorre che il soggetto, incaricato di sviluppare il piano, prenda contatto con tutte le rilevanti funzioni aziendali, per prendere conoscenza delle conseguenze che possono avere, sulla operatività aziendale, avarie o di indisponibilità, di durata più o meno lunga, di una parte o di più parti del sistema informativo aziendale.

Per aiutare i soggetti coinvolti a dare risposte appropriate, si possono simulare scenari legati a principi di incendio del sistema informativo, mancanza di alimentazione, disastri naturali come ad esempio un allagamento, che, anche se non coinvolge direttamente il sistema informativo, può coinvolgere le linee di comunicazione. A seconda della natura dell'interruzione, si può avere un rallentamento od un fermo dell'attività aziendale, si possono ricevere lagnanze dai clienti e incorrere in significative perdite di mercato.

Nel quadro della valutazione di impatto occorre individuare un parametro fondamentale, chiamato RTO - recovery time objective, vale a dire il tempo massimo accettabile per il ripristino della funzionalità informatica, se non completa, almeno ad un livello soddisfacente.

La valutazione del rischio

Sulla base della valutazione di impatto, si può andare adesso a valutare quale sia la probabilità che rischio si verifichi.

Gli esperti raccomandano di non fare eccessivo affidamento sulla valutazione di probabilità, perché in molte aziende anche una remota probabilità, che abbia però a materializzarsi, può portare a conseguenze assolutamente drammatiche.

Ecco il motivo per cui la valutazione di rischio di situazioni gravi o catastrofiche deve concentrarsi più sulla valutazione dell'impatto, che sulla valutazione della probabilità dell'evento stesso.

Lo sviluppo della strategia di ripristino

Una volta che sono state individuate le attività critiche dell'impatto, con conseguente indisponibilità, più o meno lunga, si può attivare una strategia di messa sotto controllo.

Ad esempio, se un'applicazione critica si appoggia a un fornitore esterno, occorrerà verificare il livello di preparazione di questo fornitore.

Se invece la gestione di un applicativo critico è tutta interna, occorrerà verificare la disponibilità di sistemi di backup, non solo a livello di disponibilità di dati, ma anche a livello di disponibilità di applicazioni di trattamento dei dati stessi.

È un'esperienza purtroppo frequente che le aziende facciano attenzione ad avere a disposizione un regolare backup dei dati, ma non un regolare backup delle applicazioni, che tali dati debbono utilizzare.

Laddove il costo di queste predisposizioni sia difficilmente sostenibile dall'azienda, una strategia sempre valida è quella di appoggiarsi a servizi di disaster recovery esterni, con una politica che gli anglosassoni chiamano "DRaaS" ? disaster recovery as a service.

La documentazione del piano di recovery

Dopo avere effettuato tutti i passi precedentemente illustrati, è indispensabile documentare la strategia delle procedure di recovery. Anche in questo caso, l'approccio da parte di una piccola e media azienda deve essere più snello, rispetto a quello di un'azienda di maggiori dimensioni. Dei piani di disaster recovery estremamente dettagliati sono oltremodo lunghi da sviluppare difficile mantenere aggiornato.

Ecco perché gli elementi essenziali che dovrebbero essere documentati sono i seguenti

- Lo RTO,
- le procedure di recovery,
- l'ubicazione dei dati e degli applicativi di backup,
- i punti di contatto per il personale che riveste ruoli critici.

Infine, non bisogna dimenticarsi di effettuare con una ragionevole frequenza delle prove pratiche, che mettano in evidenza l'efficienza, l'efficacia ed il livello di aggiornamento del piano.

Buon lavoro a tutti i lettori!

Adalberto Biasiotti

www.puntosicuro.it