



Il costo di una giornata di lavoro persa

Una delle sicurezze dei computer è il fatto che, prima o poi, si guasteranno. Quando si è occupati a gestire un'organizzazione, il controllo della strategia di backup e ripristino può l'ultima delle priorità in azienda. Secondo un recente studio condotto da Acronis e dalla società di ricerche Vanson Bourne, il 63% delle PMI impiegherebbe un giorno o più per affrontare un ripristino seguito di un guasto del sistema*. Riuscite a immaginare come potrebbe funzionare la vostra azienda senza sistemi e dati, per un giorno intero?

Malgrado oggi giorno le aziende siano operative ventiquattro ore su ventiquattro, la maggior parte delle aziende di piccole e medie dimensioni mette ancora a repentaglio i propri sistemi, e di conseguenza la produttività e la redditività aziendale, non proteggendoli adeguatamente. Non importa quali siano le cause del mancato funzionamento dei sistemi - un attacco virus, un bug del software o un guasto hardware -, le conseguenze sono quasi sempre le stesse: ore o perfino giorni di inattività e potenziale perdita di quantità incalcolabili di lavoro. Se, tuttavia, si dispone di un backup recente e di un piano di ripristino ben organizzato, l'impatto economico e produttivo può ridursi notevolmente.

Doppia protezione

I feedback dei nostri clienti indicano che in generale le organizzazioni eseguono il backup dei propri server. Spesso li proteggono secondo modalità automatiche, ovvero con strategie regolari di backup pianificate. I server sono vitali per qualsiasi infrastruttura IT e pertanto è fondamentale che siano protetti e sottoposti a regolari backup.

Tuttavia, malgrado i backup costanti dei server, la nostra ricerca ha evidenziato un sorprendente 25% di organizzazioni che ancora esegue il backup manuale dei propri PC e laptop, mentre il 19% di queste non lo esegue affatto. Ai dipendenti si chiede in alcuni casi di creare backup in rete, ma questa attività non è sempre messa in pratica. Molti salvano le cartelle di lavoro in modo casuale sul desktop oppure aggiornano i documenti quando non sono in ufficio.

Di fatto, secondo le stime degli analisti, il 60% dei dati di un'azienda viene archiviato su workstation e non su server. Ciò implica che la maggior parte dei dati potrebbero essere davvero a rischio. Inoltre, occorre considerare la spesa necessaria qualora si dovesse inviare un tecnico a risolvere i problemi di un laptop non utilizzato in sede. Non solo il dipendente avrebbe un accesso limitato ai dati, ma sarebbe impossibilitato a lavorare perché senza PC e applicazioni. In breve, è bene assicurarsi che sia le workstation sia i server aziendali siano protetti e sottoposti a regolari backup, in modo automatico e con una gestione preferibilmente centralizzata.

Ricordate che il backup non equivale al ripristino!

L'organizzazione Freedom of Information Act ha chiesto a tre importanti dipartimenti governativi del Regno Unito quanti casi di guasto al sistema erano stati rilevati in un anno. In totale, sono stati riferiti 608 eventi di questo tipo. Undici a settimana! Il numero è davvero alto, ma non rappresenta un problema se viene applicata una strategia di backup e ripristino efficiente e rigorosa. Accade tuttavia troppo spesso che le aziende ritengano backup e ripristino attività equivalenti. In realtà non è così.

Una recente indagine di IDC ha rilevato che l'87%** dei responsabili dello storage mostrano fiducia o molta fiducia nel fatto che i processi di ripristino d'emergenza da loro messi in atto consentono di ripristinare i dati delle applicazioni critiche aziendali. Eppure, solo metà di questo 87% verifica le strategie di ripristino d'emergenza più di una volta l'anno. Anche se si è tranquilli perché i backup vengono eseguiti in modo regolare, è sempre opportuno testare i ripristini, altrimenti si rischia di non risolvere nulla. È perciò fondamentale eseguire un test dei backup almeno ogni tre mesi.

Esaminare la completezza della strategia in ogni suo aspetto

Molte PMI si affidano a una strategia di backup che potremmo definire "a fine giornata". La nostra ricerca ha svelato che il 72% delle aziende esegue infatti i backup alla chiusura della giornata lavorativa. Tuttavia questo può causare seri problemi. Se si verifica un imprevisto cinque minuti prima della data di esecuzione del backup pianificato, andrà perduta un'intera giornata di lavoro. Qual è per l'azienda il costo di questa mancata produttività?

Oltre a ciò, alcuni sistemi di backup possono ripristinare i dati solo a livello di file, e non a livello di applicazioni o impostazioni di sistema. Una nuova distribuzione si rivelerebbe impegnativa in termini di tempo e di ore di lavoro, perché occorre trovare i dischi del software originali e reimpostare le preferenze manualmente. E se tutti i PC dell'organizzazione venissero colpiti da un virus? Quanto tempo sarebbe necessario per ripristinare ogni macchina da zero?

Il ripristino d'emergenza come priorità aziendale

Le conseguenze finanziarie e di produttività implicate da un'eventuale perdita di dati, insieme alle interruzioni e all'inattività causate dai potenziali guasti, potrebbero mettere in ginocchio qualsiasi attività. I responsabili delle aziende hanno come primo obiettivo la continuità aziendale, la fornitura di sistemi IT funzionanti ai dipendenti e la possibilità per i clienti di comunicare ed effettuare transazioni con l'organizzazione. Perciò, backup e ripristino non devono essere attività difficoltose da implementare, e vanno messe in cima all'elenco delle priorità aziendali.

**L'indagine è stata condotta da Acronis e dalla società di ricerca Vanson Bourne nell'ottobre del 2009. Il campione era costituito da 600 PMI (250-1.000 dipendenti). Hanno risposto al questionario i responsabili IT all'interno delle singole organizzazioni.*

***2009 Annual European Storage Survey di IDC: Understanding User Needs in a Changing Economic Climate (Gennaio 2009 - Doc. IDC codice RS53R)*