Pianificazione per ripristino d'emergenza

Un documento sulla miglior prassi per i partner di Retrospect

Aspetti di preparazione all'emergenza

Prendere in considerazione il ripristino d'emergenza e ciò che comporta per un computer (ad esempio, essere in grado di eseguire un ripristino bare metal dopo un'avaria del disco rigido) abbraccia un ambito decisamente ristretto rispetto al dovere pensare a preparazione e risposta per un intera impresa, vale a dire, garantire che un'impresa possa essere di nuovo operativa subito dopo un incendio, allagamento, furto o altra circostanza. Questioni come "Dove si riuniranno e lavoreranno i dipendenti," e, "Come forniremo i computer senza dovere aspettare che una compagnia d'assicurazioni spedisca un assegno," sono preoccupazioni legittime nello sviluppare un piano per uscire vincenti da una situazione disastrosa.

Inserire la pianificazione della preparazione e risposta all'emergenza tra i propri servizi

La preparazione e risposta all'emergenza rappresenta certamente un tema così ampio e complesso che intere aziende sono state incentrate sulla fornitura di tali servizi. Sebbene delineare i compiti necessari per emulare aziende del genere vada al di là dell'intento di questo documento, una cosa è chiara: i fornitori di servizi informatici si trovano nella posizione migliore per persuadere i loro clienti a pensare a cosa deve essere fatto per garantire la sopravvivenza della propria impresa, e per fornire servizi connessi al garantire le funzionalità e attività informatiche in corso.

Come minimo, anche se solo per proteggere sé stessi e la propria impresa da perdita di dati accidentale quando si lavora su computer dei clienti, si dovrebbe avere un piano dettagliato di backup e ripristino pronto per ciascuno dei propri clienti. Si faccia di tale piano un obbligo, e in esso si dettagli:

- Pianificazione e implementazione iniziali
- Gestione giornaliera (esecuzione di backup e ripristini, controllo delle notifiche via e-mail)
- Manutenzione periodica e collaudo (archiviazione, verifica di ripristini parziali e completi)
- Revisione quando necessario (capacità del sistema, prestazioni, tecnologia, metodologia, etc.)

I compiti elencati sopra forniscono significativi ricavi da servizi nel tempo, e qualcosa come tra il 70 e il 90 per cento di una procedura di backup e ripristino può essere duplicata da un ambiente cliente all'altro, rendendola una procedura quasi del tutto reiterabile. Decidi quello che funziona, e poi prepara i tuoi clienti (e te stesso!) per il successo.

Miglior prassi per il piano di backup e ripristino d'emergenza

Crea e formalizza un piano

Consigliamo di formalizzare un piano di backup e ripristino per ciascuno dei propri clienti. Dovrebbe comprendere elementi cone il vostro accordo a livello di servizi con tempi di risposta che potete rispettare, quali sono le vostre responsabilità e quali le loro, misure per la buona riuscita, e quali servizi senza interruzione saranno forniti.

Archiviazione del backup e ripristino fuori sede

I backup in locale sono la prima linea di difesa contro la perdita dei dati, ma è cruciale avere almeno una copia dei dati di un'organizzazione archiviata al sicuro fuori sede, preferibilmente in un luogo lontano diversi chilometri. Ecco alcune cose da considerare riguardo ai backup fuori sede:

- Quali dati saranno archiviati fuori sede? Alcuni dati possono —come i file di cache—essere esclusi?
- I dati dovrebbero essere crittati?
- Dove saranno archiviati i dati fuori sede?
- Come saranno spostati lì? (Opzioni: backup su cloud, trasporto fisico dei supporti di backup)
- Chi sarà responsabile per il trasporto dei supporti materiali fuori sede?
- Quando avremo accesso ai supporti materiali se ne abbiamo bisogno?
- Con quale intervallo sarà aggiornato l'archivio fuori sede?
- Per quanto tempo saranno conservati i vecchi dati nell'archivio?

Costruisci la tua 'cassetta degli attrezzi' per il ripristino di sistema

Ogni fornitore di servizi di informatica dovrebbe mantenere una collezione di strumenti utili. Per lo meno, si abbiano pronti i seguenti, in ogni momento:

- Masterizza un disco di ripristino d'emergenza Retrospect per sistemi Windows.
  - Meglio se rilasciato con l'add-on ripristino su hardware dissimili di Retrospect
  - Fare attenzione a specifici requisiti hardware (come RAID e reti HBA)
- Crea un disco degli strumenti avviabile per sistemi OS X.
  - Includi l'applicazione, motore, e client Retrospect
  - Aggiungi le tue utility preferite (Disk Warrior, Tech Tool Pro, etc.)
- Se qualche backup fuori sede è archiviato su nastro, assicurati che sarai in grado di procurarti prontamente un'unità capace di leggere quei nastri, nel caso in cui l'unità di backup a nastro principale dovesse diventare inutilizzabile per qualunque motivo.
- Assicurati di avere accesso ad ogni password e chiave necessarie! Se la nota Post-it™ con la tua password del set di backup era sotto la tastiera ed è appena andata in fumo con il resto dell'ufficio, sarai nei guai senza quella password salvata al sicuro altrove!

Collauda, collauda, collauda

Anche piani di ripristino d'emergenza attentamente considerati hanno bisogno di essere testati. Poche cose sono più penose dello scoprire che le cose non stanno funzionando come atteso durante l'esecuzione di un ripristino cruciale. La progettazione di Retrospect include un metodo eccezionale di verifica dei dati che usa realmente le stesse routine usate durante l'esecuzione del ripristino. Questo è fantastico per garantire che i dati di backup sono leggibili e corrispondono esattamente ai dati originali, ma testare con successo un vero e proprio ripristino rimane il modo migliore per mantenere la fiducia nel sistema.

Metti in atto un piano per testare i ripristini almeno trimestralmente per ciascuno dei tuoi clienti. Quando esegui questo collaudo, ci sono diversi test che non dovrebbero essere tralasciati:

- Cerca e ripristina un file
- Ripristina una cartella allo stato di un momento temporale precedente
- Ripristina un intero volume e verifica che si avvii, che le applicazioni vengano eseguite come atteso, etc.
- Controlla che applicazioni critiche per l'impresa (contabilità, e-mail, etc.) funzionano dopo un ripristino
- Ripristino da backup fuori sede

Oltre a verificare l'affidabilità del sistema di backup, il test dei ripristini ti porta regolarmente faccia a faccia con i tuoi clienti e mantiene *la loro fiducia nei tuoi confronti*. È una procedura vantaggiosa per tutti.

Retrospect

Comincia immediatamente; perfeziona nel tempo

Qualunque cosa decidi di fare, non aspettare a fare avere ai tuoi clienti dei backup fuori sede fino a quando hai creato il piano perfetto. Archivia qualcosa fuori sede ADESSO. Proprio per la loro natura, i disastri sia naturali che creati dall'uomo sono difficili da predire o prevenire. È meglio ottenere di avere almeno una copia dei backup dei tuoi clienti archiviata al sicuro fuori sede immediatamente. Poi potrai considerare con calma e implementare nel tempo un sistema che fornirà un livello di servizio che soddisfa al meglio le situazioni e i bisogni dei tuoi clienti.

* Retrospect, Inc. non giustifica la conservazione delle password in nessun modo che non sia un modo sicuro ed affidabile.