Come evitare la perdita dei dati
e proteggerli in modo efficiente

Immagazzinamento Dati e Sistemi di Backup

Con l'aumentare dei rischi associati a virus, attacchi informatici e rotture hardware, implementare una procedura di backup sistematico è una parte necessaria per ogni strategia aziendale di gestione del rischio e per la sicura e corretta conservazione dei file personali.

In informatica con il termine backup, copia di sicurezza o copia di riserva si indica la replicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria di massa dei computer, siano essi stazione di lavoro o server, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. Si tratta dunque di una misura di ridondanza fisica dei dati, tipica delle procedure di disaster recovery.

L'attività di backup è un aspetto fondamentale della gestione di un computer: in caso di guasti, manomissioni, furti, ecc., ci si assicura che esista una copia dei dati, assicurando quindi una ridondanza logico/fisica dei dati.

Pertanto se si dispone di un apposito software dedicato o incluso nel proprio sistema operativo, l'esecuzione del backup è quasi sempre impostata in maniera automatica e svolta normalmente con una periodicità stabilita (per esempio una volta al giorno o alla settimana), e con altre particolarità avanzate se rese disponibili dal software utilizzato.

La maggior parte dei sistemi operativi attuali per personal computer integra un qualche programma di backup da configurare, ma solo i server appositamente equipaggiati contengono normalmente un servizio nativo automatico.

Nelle aziende il tipo di backup e la relativa periodicità sono solitamente regolati da un'apposita procedura aziendale soggetta a verifica periodica e ad altre procedure che comportano un intervento manuale. Il responsabile della sicurezza è tenuto ad annotare i controlli periodici e gli interventi sui sistemi. I supporti su cui viene effettuato il backup normalmente devono essere di tipo e marca approvati nella procedura ed è necessario che siano periodicamente verificati e sostituiti. Devono inoltre essere conservati in accordo con le politiche di sicurezza aziendale, per esempio, ma non solo, per questioni legate alla privacy.

È naturalmente buona norma eseguire periodiche operazioni di backup anche nei personal computer di uso privato, che di solito vengono eseguite dall'utilizzatore del computer stesso che copierà i dati importanti su supporti ottici o magnetici (CD-R, CD riscrivibili, DVD-R, DVD riscrivibili, Digital Audio Tape, cartucce a nastro). Gli hard disk portatili con collegamento esterno USB e le chiavette usb (stick-usb) hanno preso il posto dei floppy disk che sono ormai in disuso per la scarsa affidabilità e la limitata capacità.

È possibile anche eseguire il backup in modo continuo usando servizi come il backup online o i backup appliance che sono degli strumenti che permettono questo

tipo di operatività attraverso gli agent, che sono dei software che si occupano di individuare, attraverso criteri, i file nuovi da archiviare e immediatamente ne eseguono la copia di sicurezza.

Anche il palmare e lo Smartphone sono diventati importanti strumenti per i lavoratori perché contengono dati fondamentali come la rubrica telefonica e il calendario degli appuntamenti, è pertanto diventata buona norma estendere il backup anche a questi strumenti.

Diversi nuovi servizi su internet permettono infine di eseguire il backup degli account e dei dati degli utenti di social network.

Politica di backup

La politica di backup definisce l'insieme di regole a procedure per assicurare che venga eseguito un backup adeguato alle necessità dell'organizzazione aziendale. Una politica di backup definisce il tipo (es. full o incrementale) di backup, la frequenza (generalmente giornaliera), e include le regole per verificare la rispondenza del processo di restore.

Cause della perdita dei dati

Perdere i dati prima o poi capita a tutti, e come partire in vacanza con l'aereo e scoprire all'arrivo che hanno smarrito la tua valigia, c'è sempre una prima volta.

La perdita dei dati è una delle principali cause del fermo di un'azienda, di un'ufficio o semplicemente di un privato. Il danno, se non si sono fatti gli opportuni backup, è notevole. Andiamo dal danno economico (migliaia di euro per pagare ditte specializzate nel recovery), alla sicurezza (smarrimento di password, codici e conti), a quello affettivo (perdita di foto, video e testi della propria famiglia), ed anche di tempo (per ripristinare il tutto) e, chi più ne ha più ne metta.

Le possibili cause che portano alla perdita dei dati possono essere molteplici, con effetti diversi e più o meno gravi al loro verificarsi. Fondamentale quindi e mettere appunto delle opportune strategie di Backup e Recupero, nonchè di protezione e crittografia dei propri dati sensibili. Prima però di parlare dei rimedi, proviamo ad elencare quali sono le più comuni cause di perdita dei dati.

Eccezioni non gestite nei programmi

Durante la normale esecuzione di un programma possono verificarsi delle condizioni non previste dal programmatore, le quali causano delle eccezzioni, ossia condizioni che terminano il programma in modo imprevisto. Se il programma stava eseguendo delle operazioni sul proprio storage (solitamente un database), il verificarsi di un'eccezione può portare ad una chiusura imprevista dell'applicazione e conseguentemente le operazioni sul database non vengono concluse correttamente, lasciando transazioni in sospeso con conseguente incoerenza dei dati. Questa situazione è molto diffusa, e l'unico sistema per prevenirla è una corretta gestione delle eccezioni. Un programma sia esso un'applicazione desktop che web dovrebbe essere sempre in grado di reagire ad una situazione anomala chiudendo correttamente le transazioni in corso, prevedendo magari delle funzioni di commit e di rollback per

il ripristino del database allo stato coerente precedente al verificarsi dell'eccezione. Sebbene non si riesca a prevenire sempre problemi di questo tipo, è possibile adottare misure appropriate per proteggere i dati in caso di chiusura anomala di un'applicazione, come l'opzione di salvataggio automatico.

Errori umani

Purtroppo l'errore umano è sempre da tenere in considerazione, sia esso causato da un'amministratore di sistema, o da un semplice utente, esso è sempre in agguato e può verificarsi molto più spesso di quanto si creda. Gli scenari possono essere molteplici, una cancellazione accidentale, uno script programmato con superficialità, un export di dati che và a sovrascrivere lo storage principale, o più semplicemente ad una normalissima distrazione. Testare quindi sempre gli script, le store procedure e tutte quelle operazioni che coinvolgono i dati, prima di metterle in pratica sullo storage primario, fare regolarmente il backup, ed operare sempre con grande attenzione. Infine eseguire sempre dei backup regolari.

Problemi hardware

Un crash hardware, sia esso legato ad una rottura dell'hard disk, o ad una interruzione improvvisa della corrente; qualsiasi sia il motivo il crash hardware di una macchina può portare ad una situazione in cui sia difficile recuperare i dati. In questo caso mettere appunto un sistema robusto di alimentazione, prevedendo l'allaccio dell'intero parco macchine sotto uno o più gruppi di continuità. In zone particolarmnte soggette agli sbalzi di tensione predisporre uno stabilizzatore di corrente di opportuna dimensione all'igresso della linea elettrica. Infine anche in questo caso un'opportuno backup potrebbe rimediare con facilità al suddetto problema.

Attachi dai Virus e dai Cracker

In un mondo sempre più connesso la possibilità di cadere vittima di un attacco di un cracker (hacker male intenzionato) o un virus è sempre più alta. Facile a questo punto immaginarne le conseguenze, formattazione del disco fisso, furto telematico d'informazioni e di dati sensibili. Backup ed opportuni strumenti di protezione quali patch sulla sicurezza del S.O., antivirus, firewall, crittografia ed altro ancora possono rilevarsi fondamentali per sventare questa possibile minaccia.

Catastrofi, incendi e furti

Bisogna tenere in considerazione anche una possibile situazione catastrofica, come un incendio od un allagamento, con conseguente danneggiamento delle macchine contenente i nostri dati. Per non parlare poi di ladri ghiotti di notebook ed apparecchiature tecnologiche. Quest'ultima situazione assieme ad un'attacco cracker a mio avviso è una delle peggiori, poichè non comporta solamente la perdita dei nostri dati, ma mette i nostri dati a disposizione del ladro, che può usfruirne nel modo peggiore delle nostre password, codici di conto corrente e quant'altro. Anche

qui oltre al consueto backup, e utile crittografare i dati più importanti e munire l'accesso alla nostra macchina, ai nostri file e directory di opportune password.

I Sistemi di Backup

Il backup è una copia addizionale dei dati di interesse di un sistema che può essere utilizzata per il ripristino e recupero degli stessi. In generale la copia di backup viene utilizzata quando la copia principale dei dati viene danneggiata o persa; si possono avere due modi di creare il backup:

- *semplice copia dei dati*: dove viene creata una o più copie del dato di interesse;
- *mirroring dei dati*: dove la copia è sempre aggiornata con ciò che è scritto nella copia primaria.

Perché fare backup dei dati? Lo scopo principale del fare backup dei dati è quello di riportare il sistema ad uno stato originale funzionante, se i dati del sistema attuale sono stati persi o danneggiati; conservare delle copie secondarie di dati nel caso in cui le originali vengano perse. Prevedere una buona politica di backup può ridurre o addirittura eliminare i danni causati dalla perdita dei dati.

Come prevenire la perdita dei dati? Gli step generali per prevenire la perdita dei dati sono:

- eseguire backup spesso ma con saggezza (soprattutto sui dati sensibili)
- dare priorità ai dati che eventualmente possono supportare il disaster recovery (classificazione in base ai tempi di ripristino dei dati): backup ridondante (richiesto immediatamente), backup altamente disponibile (massimo minuti o ore), backup appoggiato (quattro ore o giorni)
- prevedere un archiviazione dei dati importanti a lungo termine
- memorizzare i dati che effettivamente hanno un costo in termini di politiche aziendali.

Come deve essere una procedura di ripristino? Bisogna considerare una vera e propria strategia di ripristino che dipende fondamentalmente dal tipo di backup scelto. Questa strategia di backup deve essere ben documentata e testata affinchè sia garantito il corretto recupero dei dati dati. Bisogna avere una disponibilità di hardware e alloggi alternativi nel caso in cui quelli originali vengano distrutti.

Strategie di backup

l backup porta con se numerose problematiche alle quali un sistemista si deve sottoporre prima di scegliere la strategia da adottare:

- quanti dati devono essere protetti e su che dispositivo vogliamo importarli?
- quale strategia utilizzare per effettuare il backup dei dati?

- quando fare il backup?
- dove salvare le copie di backup?
- quali sono le procedure di ripristino? e quali sono i dati di cui abbiamo necessariamente bisogno in breve termine?
- qual'è la piattaforma migliore con la quale poter salvare i dati del backup?

Per la scelta di quali dati proteggere, bisogna effettuare uno studio del sistema e chiedere o quanto meno capire, quali sono i servizi che bisogna tenere sempre disponibili; da quì si ottiene un'informazione relativa a quali sono i dati sensibili che vanno protetti.

backup completo

Esistono diversi livelli di granularità di backup, che a seconda delle esigenze richieste possono essere considerate. Il full backup o backup completo è una strategia che prevede l'intero salvataggio dei dati, una volta a settimana. Questa tecnica ha come vantaggio la semplicità di implementazione, in quanto bisogna prevedere soltanto un unico salvataggio dei dati in un giorno prestabilito; inoltre risulta estremamente semplice la procedura di ripristino, in quanto a partire dalla data del punto di rottura del sistema, basta ripercorrere a ritroso la settimana e prendere l'ultima copia salvata del sistema.

Vi sono naturalmente degli ovvi svantaggi: in primis questa tecnica può essere applicata a sistemi in cui i dati sono modificati con bassa frequenza, e ciò lo si deduce dal fatto che effettuando poche copie di backup e perlopiù a fine settimana, tutti i dati modificati durante la stessa saranno persi. Dunque c'è un forte limite applicativo.

backup differenziale

Un'altra tecnica utilizzata è quella del Backup Cumulativo o Dierenziale. I backup differenziali o cumulativi, modificano solo i file, memorizzando ogni volta che c'è un backup, le nuove informazioni del sistema più quelle precedentemente salvate. I backup differenziali sono anche detti cumulativi in quanto con un backup differenziale, una volta che un file viene modificato esso continua ad essere incluso in tutti i backup differenziali successivi (fino ovviamente al successivo backup completo). Ciò significa che ogni backup differenziale contiene tutti i file modificati fino all'ultimo backup completo, rendendo possibile l'esecuzione di un ripristino completo con solo l'ultimo backup completo e l'ultimo backup differenziale.

Come la strategia di backup utilizzata con i backup progressivi, normalmente i backup differenziali seguono lo stesso approccio: Un singolo backup periodico completo seguito da backup differenziali più frequenti. L'effetto nell'uso in questo senso dei backup differenziali, è rappresentato dal fatto che i suddetti backup tendono ad aumentare attraverso il tempo (assumendo il fatto che diversi file possono essere stati modificati col tempo dall'ultimo backup).

Il vantaggio di questa tecnica è che il ripristino è molto veloce in quanto basta solo l'ultima copia completa e l'ultimo copia cumulativa. Gli svantaggi evidenti sono invece che occorre più tempo per eseguire i backup dei dati man mano che ci si avvicina alla fine della settimana, inoltre la dimensione degli stessi è molto grande.Tuttavia i backup differenziali sono in una posizione compresa tra i backup progressivi e quelli completi, in termine di utilizzo dei media di backup e della

relativa velocità, fornendo spesso il ripristino di file singoli più veloci ed un ripristino completo con poche informazioni (dovuti ad un minor numero di backup da ricercare/ripristinare).

backup incrementale

Un altra tecnica è quella del backup incrementale o progressivo. Diversamente dai backup completi, quelli progressivi controllano prima se l'orario di modifica del file sia più recente rispetto all'ultimo orario di backup. Se questo non è il caso, il file non è stato modificato dall'ultimo backup e quindi può essere saltato. Se la data della modifica è più recente rispetto alla data dell'ultimo backup, il file è stato modificato e quindi si può eseguire il suo backup. I backup progressivi sono usati insieme con i backup completi (per esempio, un backup settimanale completo, insieme con backup progressivi giornalieri). Il vantaggio primario riguardante l'uso dei backup progressivi è rappresentato dal fatto che questi ultimi sono più veloci dei backup completi e richiedono meno spazio, in quanto le copie di backup sono realizzate solo sui file che sono stati modificati rispetto alle copie precedenti. Mentre lo svantaggio primario è quello che il ripristino di ogni dato file potrebbe significare eseguire uno o più backup progressivi fino a che non viene trovato il file in questione. Quando si esegue il ripristino di un file system completo, è necessario ripristinare l'ultimo backup completo ed ogni successivo backup progressivo.

Backup come immagine disco

Un'immagine disco è un file contenente tutte le informazioni complete di un disco, di un supporto di memorizzazione o di un dispositivo, ad esempio un disco rigido, un'unità nastro, un floppy disk, un disco ottico o una USB flash drive. L'immagine del disco è di solito creata sotto forma di copia completa, settore per settore, del supporto di origine e quindi è in grado di replicare perfettamente la struttura e il contenuto del dispositivo di archiviazione.

Alcune utility di imaging del disco omettono lo spazio relativo ai file inutilizzati nel supporto di origine, o comprimono i file del disco replicato per ridurre i requisiti di storage, anche se, in questo caso, sono generalmente indicati come file di archivio, in quanto non sono letteralmente immagini disco.

I formati di file immagine del disco possono essere standard aperti, come il formato di immagine ISO per le immagini di un disco ottico, o di proprietà di particolari applicazioni software.

Alcuni programmi di backup effettuano solo il salvataggio dei documenti maggiormente utilizzati, le informazioni di avvio e i file bloccati dal sistema operativo, come quelli in uso al momento del backup, non possono essere salvati su alcuni sistemi operativi. Un'immagine disco contiene tutti i file, replicando fedelmente tutti i dati. Per questo motivo, è utilizzatoaanche per il backup di CD e DVD.

E' solitamente possibile eseguire il backup dei documenti utilizzando il backup standard basato su file, e questo è solitamente preferito poiché il backup basato su file di solito consente di risparmiare più tempo e spazio attraverso l'utilizzo di backup incrementali, e generalmente hanno una maggiore flessibilità. Tuttavia per i file relativi al software le soluzioni di backup basati su file non possono riuscire a riprodurre tutte le caratteristiche necessarie al loro corretto funzionamento, in particolare con i sistemi Windows. Ad esempio, in Windows alcune chiavi di registro

usano nomi di file brevi, che non sono a volte riprodotti da backup basato su file. Alcuni software commerciali utilizzano una protezione contro la copia che causerà problemi se un file viene spostato in un settore del disco diverso. Inoltre i backup basati su file non sono sempre in grado di riprodurre i metadati come gli attributi di sicurezza. La creazione di un'immagine disco identica è un modo per garantire che il backup di sistema sia esattamente come l'originale.

Hot Backup

Un backup a caldo, detto anche backup dinamico, è un backup eseguito su dati accessibili agli utenti, che possono quindi essere attualmente in uno stato di aggiornamento. Il backup a caldo è in grado di fornire una soluzione conveniente in sistemi multi-utente, in quanto non richiede tempi di inattività, come succede in un backup a freddo convenzionale.

I backup a caldo comportano determinati rischi. Se i dati vengono modificati mentre il backup è in corso, la copia risultante potrebbe non corrispondere alla configurazione definitiva dei dati. Se il recupero dei dati diventa necessario (ad esempio, a seguito di un crash del sistema), l'inconsistenza dovrà essere risolta.

Il database Oracle, ad esempio, preserva l'integrità dei dati creando un cosiddetto registro di ripristino prima di eseguire un backup a caldo e ponendo l'unità in modalità hot-backup mentre i dati vengono copiati. Le prestazioni possono tuttavia degradare mentre il backup è in corso.

Software di backup

Ci sono molte filosofie diverse quando si parla di backup e relative applicazioni, e quelle che abbiamo selezionato ricadono in due grandi categorie: strumenti che clonano i dischi e creano il backup di un certo drive o partizione, sostanzialmente copiando tutto (a volte creano anche un disco avviabile), e altri che invece prevedono un backup selettivo di cartelle, file e database. Alcune delle principali funzionalità che un programma di backup deve fornire, sono:

- Copia immagine di un disco rigido;
- Copia selettiva di directory e singoli file;
- Criteri di selezione per la ricerca dei contenuti salvati e per la scelta di quelli che devono essere oggetto di backup (per data, tipo di file, autore della modifica);
- Compressione dei contenuti per ridurre la memoria richiesta per la copia;
- Sicurezza: protezione dei dati copiati attraverso password e crittografia.

Qualsiasi sia il programma scelto, bisogna assicurarsi di eseguire il backup regolarmente (alcune applicazioni aiutano con la programmazione automatica), e di copiare i dati su diversi supporti, anche online o tramite la rete locale se possibile. Se si ha un solo backup su un hard disk esterno, infatti, si corre comunque il rischio di perderlo in caso il supporto si danneggi.

Drive Image XML

Cominciamo dai programmi che clonano l'intero disco o una sua partizione, che è proprio ciò che fa Drive Image XML. Ci piace in particolare il fatto che può clonare l'intero disco senza riavviare il sistema e, grazie all'uso di Microsoft Volume Shadow Services (VSS), può creare una hot image anche se il disco è in uso. È anche possibile programmare backup incrementali, e creare un live CD per ripristinare un'immagine. Ne esiste anche una versione a pagamento, che offre un anno di assistenza e aggiornamenti.

Clonezilla

Clonezilla è uno strumento open source per la clonazione dei dati e la creazione di Live CD - dischi avviabili ricchi di strumenti. È pieno di opzioni avanzate, ed è compatibile con diversi file system e supporti per il backup; ha anche l'opzione per usare drive di rete e creare immagini del disco. C'è anche la Server Edition, da usare per creare il backup di 40 computer contemporaneamente, il che è molto utile in piccole e medie aziende. L'interfaccia testuale può essere un po' complessa da usare per chi è abituato a quelle grafiche, ma una volta che ci si prende la mano Clonezilla è molto potente.

Macrium Reflect

Macrium Reflect Free è una versione gratuita e destinata all'uso domestico dell'omonimo software professionale. Permette di copiare specifiche cartelle o file, e anche di duplicare un sistema attivo, montarne l'immagine, per poi esplorare e copiare file specifici. È possibile poi programmare le attività, e creare un disco di ripristino basato su Linux.

Paragon Backup & Recovery

Paragon Backup & Recovery 2012 Free è un altro strumento gratuito piuttosto robusto e valido. Include funzioni per creare immagini e fare backup, la programmazione dell'attività e i backup differenziali o incrementali. È compatibile con molti metodi diversi, permette di escludere automaticamente alcuni tipi di dati e di creare dischi Live, con diversi strumenti per gestire le partizioni.

EaseUS Todo Backup

EaseUS Todo Backup Free si mette in qualche modo a cavallo tra le due categorie che abbiamo citato in apertura. Offre una buona gamma di strumenti, che vanno dal backup e ripristino di tutto il sistema alla clonazione del disco, passando dalla selezione di singoli file e cartelle. Gli strumenti di programmazione permettono di automatizzare tutto, e non manca un wizard che aiuta a gestire tutto facilmente senza rinunciare alla flessibilità.ù

Passiamo ora ai sistemi che permettono di copiare e archiviare i dati in modo più selettivo, o di creare dei mirror delle informazioni.

Backup Maker

Partiamo con BackUp Maker di Ascomp Software GmbH, che merita una menzione per l'usabilità e l'ottima interfaccia, oltre che per il buon numero di funzioni disponibili. Questo programma ha un valido sistema per programmare le attività, e può fare il backup completo o di singole cartelle, con funzioni di copia incrementale. Non manca la possibilità di proteggere le copie con crittografia, o quella di eseguirle su un supporto di rete o esterno. È possibile ripristinare la totalità dei dati o solo una parte, tanto nelle vecchia locazione o in una nuova. Considerate tutte queste qualità Backup Manager è senz'altro un ottimo strumento gratuito, che si può ulteriormente impreziosire con degli add-on che permettono di copiare solo i file aperti, come per esempio i database e i file di sistema; o ancora è possibile eseguire Backup Manager come servizio in Windows NT/2000/XP/2003. Chi sceglierà la Professional Edition, infine, avrà anche il supporto da parte dell'azienda.

Synchredible

Anche Synchredible è prodotto da Ascomp Software GmbH, la stessa di Backup

manager. È uno strumento pensato per la sincronia di dati su LAN o supporto esterni, mono o bidirezionale. Questa impostazione non lo rende meno interessante come strumento di backup: basta collegare un drive esterno o di rete per creare una copia fedele dei propri dati con Synchredibile.

Cobian Backup Cobian Backup 11 Gravity è un programma per il backup automatico con una potente funzione di programmazione. Può copiare tutti i dati, anche in forma compressa o crittografata, su un disco esterno, di rete o indirizzo FTP. Si possono programmare backup completi, incrementali o differenziali, in abbinamento a strumenti di compressione e crittografia. Cobian Backup si può anche impostare per l'esecuzione in background.

FBackup FBackup è un programma gratuito e facile da usare per programmare i backup e alcune azioni preliminari. Si può scegliere solo tra il backup completo e compresso e il mirroring grezzo, ma è facile da usare e si possono usare plugin per proteggere impostazioni e dati di specifiche applicazioni.

Genie Timeline Genie Timeline Free 2012 è un programma semplice e ben fatto, che ha abbracciato l'impostazione estetica di Windows 8. Al di là del suo aspetto, è anche un solido programma per creare versioni storiche dei propri dati. Alla prima esecuzione un Wizard permette di selezionare la destinazione dei dati, e di decidere quanto spazio dedicare ai backup. Poi si può scegliere tra diversi filtri, per determinare i tipi di file da copiare. Dopodiché ci si può anche dimenticare di Genie Timeline, che continuerà a mantenere intatta la copia dei dati e controllare ogni otto ore eventuali cambiamenti. Se cercate un sistema poco invasivo e siete disposti a tollerare qualche limitazione, questo programma è ciò che fa per voi.

Toucan Giungiamo infine a Toucan, un programma leggero e portatile che può eseguire backup completi, incrementali e differenziali, sincronia dei dati, compressione (7-zip e zip), crittografia e ripristino. Diversi filtri permettono di scegliere quali file proteggere e quali escludere, e alcune opzioni di scripting permettono agli utenti più avanzati di personalizzare tutte le operazioni. Ci sono altri programmi che fanno le cose che fa Toucan, ma la portabilità di quest'applicazione la rende unica: basta installarla su un pendrive per usarla dove e quando si vuole.

Tecnologie e Topologie di Backup

Il mercato offre diverse soluzioni per una scelta di un valido supporto di memorizzazione esterno.

I vantaggi dei supporti di memorizzazione esterna, sono da ricercarsi nella loro praticità e la facilità con cui vengono utilizzati, inoltre lo sviluppo tecnologico contribuisce ad avere sempre più supporti di memorizzazione veloci e con grosse capacità, oltre all'abbattimento dei costi.

Tra le altre caratteristiche interessanti da segnalare per questi dispositivi, vi è la possibilità di utilizzarli come dischi di avvio nel caso in cui la scheda madre supporti il boot da USB.

Un altro fattore di rilievo, è da ricercarsi nelle dimensioni ridotte di tali supporti, che risultano facilmente trasportabili e consultabili presso un qualsiasi computer, per

esempio, dotato di porte USB. In alcuni casi, comunque, è necessario installare dei driver che permettono al supporto di dialogare con il PC tramite il proprio reader.

Se da una parte questi vantaggi portano l'utente alla scelta di uno o l'altro dei prodotti offerti dal mercato, non è da sottovalutare l'aspetto sicurezza che riveste un ruolo fondamentale sia nella scelta del prodotto, che nell'uso. Si pensi, solo per un momento, alle conseguenze che si avrebbero se un malintenzionato in possesso di un token USB, guadagnasse l'accesso fisico ad una macchina, tenuto conto che questo tipo di dispositivo riesce ad immagazzinare fino a 2 Gbyte. Il legittimo proprietario non si accorgerebbe del furto delle informazioni, se non consultando il log del sistema operativo.

Un eventuale svantaggio derivante dalle piccole dimensioni dei dispositivi, potrebbe essere la perdita degli stessi, permettendo così ad una terza persona di impossessarsi impropriamente dei dati contenuti. Per ovviare a questi inconvenienti possiamo, installare un programma di autenticazione del token, che in pratica autentichi, con username e password, la persona che inserisce il token nel computer. Altra soluzione è quella di usare determinati tipi di supporti di memorizzazi one, dotati di un proprio chip il cui compito è quello di scaricare i file e cifrarli nello stesso tempo: tutto il procedimento risulta totalmente trasparente all'operatore.

I nastri di backup

Il nastro è un media ideale per le sue notevoli capacità di immagazzinamento, per il basso costo, e la possibilità di archiviare i nastri in luoghi protetti. Organizzare un numero di nastri in una efficiente strategia di backup permette inoltre di ripristinare i dati da diversi punti temporali, e di archiviarli.

I principali vantaggi del salvataggio su nastri dei dati sono:

- bassi costi
- elevate capacità di memorizzazione dei dati
- possibilità di conservare le copie di backup fuori sede

Una delle composizioni fisiche dei nastri è la cosiddetta Physical Tape Library (libreria fisica a nastro). Essa fornisce alloggio e alimentazione per un certo numero di unità nastro e cartucce, ed è dotata di un braccio robotico o meccanismo selettore. Il software di backup ha l'intelligenza per gestire il braccio robotico e l'intero processo di backup. Questa tecnologia però sta per essere soppiantata in quanto sta diventando insufficiente per il backup dei dati a causa di elevate percentuali di insuccesso e bassa efficienza.

Le tecnologie di Physical Tape Library stanno scomparendo, non il backup su nastro, in quanto questi presentano sempre e comunque i vantaggi sopra esposti, rispetto alle altre tecniche che presenteremo successivamente.

I nastri hanno varie tecniche per effettuare il backup: le *cinque di rotazione dei nastri*, la *rotazione nonno-padre-figlio* e la *strategia torri di Hanoi*.

La Cinque di rotazione dei nastri è il più semplice schema di rotazione del nastro. Consiste nell'avere un nastro per ogni giorno della settimana lavorativa; i nastri sono

etichettati: Lunedì, Martedì, Mercoledì, Giovedì, Venerdì. I dati possono essere ripristinati da uno qualsiasi dei nastri nella libreria - o in questo caso, un giorno passato della settimana.

La rotazione nonno-padre-figlio è il metodo più utilizzato. Esso comporta il backup dei dati nel mo do seguente: tutti i giorni sui nastri figlio, settimanale nei nastri padre, mensile sui nastri nonno.

Questo sistema è molto più potente rispetto alle cinque rotazioni del nastro, ma richiede più nastri. Fornisce inoltre la possibilità di ripristinare i dati dalla scorsa settimana, più ogni Lunedì nel corso dell'ultimo mese, più ogni mese, per i tanti nastri mensili.

La strategia Torre di Hanoi è una strategia complessa in cui si utilizzano cinque nastri: A, B, C, D, E. A viene utilizzato a giorni alterni, B è utilizzato ogni 4 giorni, C viene usato ogni 8 giorni, D ed E vengono utilizzati ogni 16 giorni.

I dischi

Un giusto complemento al backup su nastro è il backup su disco, esso può esser fatto sui dischi già presenti sulla macchina o collegati direttamente ad essa (DAS), su sistemi di dischi disponibili in rete (NAS) e strutture di rete progettate per l'immagazzinamento di dati (SAN). Il backup su disco permette di solito di avere una maggiore velocità di esecuzione, consentendo di ridurre la finestra temporale che deve essere resa disponibile al backup di file aperti o altamente utilizzati.

Gli svantaggi sono che è una tecnica dipendente da altre tecnologie, come replica locale e remota. Alcuni prodotti di backup richiedono: moduli aggiuntivi e licenze per supportare il backup su disco, operazioni di configurazione aggiuntive, tra cui la creazione di gruppi RAID.

Infatti una delle tecniche più utilizzate per realizzare backup su disco è la tecnica RAID (Redundant Array of Independent Disks).

Un RAID è un insieme ridondante di dischi indipendenti (originariamente: Redundant Array of Inexpensive Disks, insieme ridondante di dischi economici), è un sistema informatico che usa un gruppo di dischi rigidi per condividere o replicare le informazioni. Nella sua implementazione originaria il fattore chiave era l'abilità di combinare parecchi dischi a basso costo ed obsoleti per rendere il sistema complessivamente migliore di un disco di ultima generazione per capacità, affidabilità e velocità. I benefici del RAID sono dunque l'aumento dell'integrità dei dati, la tolleranza ai guasti e le prestazioni, rispetto all'uso di un disco singolo.

Nel suo livello più semplice, il sistema RAID permette di combinare un insieme di dischi in una sola unità logica. In questo modo il sistema operativo gestisce i differenti dischi come un unico volume. Il RAID è tipicamente usato nei server, e di solito è implementato con dischi di identica capacità. Con il calo del costo dei dischi rigidi e con il diffondersi della tecnologia RAID nei chipset delle schede madri, il RAID è spesso offerto come opzione sia sui computer di fascia alta sia su quelli usati da utenti domestici, specialmente se dedicati a compiti che richiedono un grande immagazzinamento di dati, come ad esempio il montaggio audio e video o la raccolta dati di un grande database.

Anche se RAID può proteggere da eventuali malfunzionamenti del disco, non protegge da errori dell'operatore e dell' amministratore (errori umani), o da errori dovuti a bug di programmazione (forse dovuti anche ad errori nello stesso software RAID). La rete abbonda di storie tragiche di amministratori di sistema che hanno installato RAID e hanno perso tutti i loro dati. RAID non sostituisce un backup frequente e regolarmente programmato.

Topologie per il salvataggio dei dati

NAS e SAN sono le iniziali dei due sistemi di storage condiviso maggiormente utilizzati nelle configurazioni di rete.

NAS

Un Network Attached Storage (NAS) è un dispositivo collegato ad una rete di computer la cui funzione è quella di condividere tra gli utenti della rete una memoria di massa, in pratica costituita da uno o più dischi rigidi.

Generalmente i NAS sono dei computer attrezzati con il necessario per poter comunicare via rete. Si tratta di dispositivi dotati solitamente di un sistema operativo basato su Linux (generalmente trasparente all'utente) e di diversi hard disk destinati all'immagazzinamento dei dati. Tale architettura ha il vantaggio di rendere disponibili i file contemporaneamente su diverse piattaforme, come ad esempio Linux, Windows e Unix (o Mac OS X), dove il sistema operativo implementa i server di rete con gli standard più diffusi tra i quali ad esempio FTP, Network File System (NFS), Samba per le reti Windows e AFP per le reti Mac OS X.

Questi dispositivi non vanno scambiati con gli Storage Area Network (SAN); questi ultimi sono soluzioni di immagazzinamento dati (storage) ben differenti: tali sistemi comprendono una rete e fanno riferimento a tecnologie e protocolli spesso proprietari. Talvolta un sistema NAS può essere utilizzato come nodo di una SAN, data la scalabilità di tale architettura.

I vantaggi offerti dai NAS sono molteplici. Innanzitutto un NAS permette di centralizzare l'immagazzinamento dei dati in un solo dispositivo accessibile a tutti i nodi della rete, altamente specializzato per le prestazioni; quindi un NAS permette di implementare schemi RAID (Redundant Array of Independent Disks), i quali garantiscono una migliore gestione della sicurezza dei dati. Normalmente un NAS consente l'eventuale rimozione ed aggiunta di dischi a caldo (hot swap), senza la necessità di disattivare l'unità.

Nell'ambito dell'adozione di tale architettura un eventuale svantaggio potrebbe essere costituito dall'enorme quantità di dati che viene a transitare sulla rete, come potrebbe essere costituito dai limiti di prestazione e di stabilità di un NFS e degli altri filesystem utilizzabili in rete.

SAN

Le SAN (Storage Area Network) invece sono i dispositivi più recenti nella catena evolutiva. Rispetto ai NAS, utilizzano protocolli più sofisticati e talvolta impiegano connessioni fisiche dirette ai server (tipicamente in fibra) oppure usano la rete primaria mediante il proto collo iSCSI che comunque viene convogliato su porte di switch dedicate e perciò rimane separato dal resto del traffico e non incide sull'efficienza complessiva della LAN: spesso si tratta di connessioni Gigabit Ethernet che uniscono direttamente una o più porte del server e una o più porte del sistema di storage

Un vantaggio infatti di una SAN consiste nel permettere un collegamento ridondante per garantire la continua accessibilità ai dati. La tipologia di trasferimento di grandi blocchi di dati li rende più efficienti nelle situazioni in cui sono presenti applicazioni che trasferiscono notevoli quantità di dati, tipicamente database e servizi di posta elettronica. Le SAN inoltre sono dotate di sistemi evoluti di protezione dei dati e hardware ridondanti per la massima protezione e disponibilità dei dati senza interruzioni del servizio

Scelta dei siti di salvataggio

Una delle principali problematiche del backup, per quanto possa sembrare banale e scontata, è proprio quella di decidere dove mettere le copie di backup realizzato. In generale abbiamo che a seconda della tecnica scelta abbiamo un vincolo. Infatti la differenza principale tra i dischi (anche i RAID) ed i nastri, sta proprio nel fatto che i secondi sono portabili, ovvero possiamo metterli dove vogliamo, mentre i primi sono legati alla loro locazione fisica. Inoltre un'altra imp ortante differenza tra queste due tecnologie sta nei costi: infatti i nastri sono meno costosi dei dischi.

Un esperienza preliminare ci dice in generale che nel caso di nastro, abbiamo bisogno almeno di 2/3 copie dei dati. La locazione di queste possono essere varie e varie domande sorgono in tal senso. In genere si preferisce avere una copia in loco, dove è presente il sistema, ma opportunamente immagazzinata in armadi ignifughi.

Le altre copie invece si preferisce tenerle in luoghi differenti da quelle in cui è presente il sistema. Il problema adesso è a che distanza situare queste copie? breve? lunga? a questi interrogativi vi sono molteplici risposte: se situiamo le copie a breve distanza, in caso di catastrofe naturale (come inondazione, eruzione vulcanica etc..) non siamo coperti e potremmo perderle. D'altro canto se situiamo le copie a notevole distanza sarà più complesso in termini di tempo il recupero delle stesse e il ripristino dei dati di nostro interesse.

Il Ripristino dei Dati

Il backup dei dati di un computer fisso, un laptop o un server è piuttosto semplice: basta copiare i dati desiderati dal proprio sistema in un'altra destinazione - un nastro di backup, un server centrale, un secondo disco, una SAN (Storage Area Network) fuori sede, un CD, un drive fl ash o qualcosa di simile. Tuttavia, questa semplice operazione di copia "da qui a lì" è fonte di preoccupazione per quasi tutte le aziende, in quanto prima o poi i backup non vengono eseguiti o si interrompono a metà o, ancor peggio, i dati archiviati non sono più recuperabili.

L'unico vero metro di misura di un sistema di backup è la sua capacità di recupero dei dati, cioè la parte "da lì a qui". 500 nastri di backup disposti ordinatamente in una scaff alatura e suddivisi per colori possono essere belli da vedere, ma sono utili solo se sono leggibili e consentono un recupero semplice e rapido dei dati. Una vera soluzione di backup e ripristino deve essere affi dabile, semplice da usare e veloce.

Disaster Recovery

Per disaster recovery (brevemente DR, in italiano: Recupero dal Disastro) si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.

L'impatto di tali emergenze è tale che si stima che la maggior parte delle grandi imprese spendano fra il 2% ed il 4% del proprio budget IT nella pianificazione della gestione dei disaster recovery, allo scopo di evitare perdite maggiori nel caso che l'attività non possa continuare a seguito della perdita di dati ed infrastrutture IT. Delle imprese che hanno subito disastri con pesanti perdite di dati, circa il 43% non ha più ripreso l'attività, il 51% ha chiuso entro due anni e solo il 6% è riuscita a sopravvivere nel lungo termine. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi possono provocare il fallimento dell'impresa o dell'organizzazione, ragion per cui investire in opportune strategie di recupero diventa una scelta quasi obbligata.

disaster recovery plan

Il Disaster Recovery Plan (DRP) (in italiano, Piano di disaster recovery) è il documento che esplicita tali misure. Esso fa parte del più ampio Business Continuity Plan (BCP).

Affinché una organizzazione possa rispondere in maniera efficiente ad una situazione di emergenza, devono essere analizzati i possibili livelli di disastro e la criticità dei sistemi/applicazioni.

Per una corretta applicazione del piano, i sistemi devono essere classificati come critici, vitali, delicati e non critici.

critici

Nei sistemi critici le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

vitali

Nei sistemi vitali le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, conseguentemente il costo di una interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

delicati

Nei sistemi delicati queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

non-critici

Nei sistemi non critici le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente. Applicazioni, software e file classificati come critici hanno una tolleranza molto bassa alle inter-

ruzioni. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.

Un piano d'emergenza deve prevedere il ripristino di tutte le funzioni aziendali e non solo il servizio ICT centrale. Per la definizione del DRP devono essere valutate le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione degli equipaggiamenti e ruoli e responsabilità dei team. La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

tecniche

Allo stato attuale, la tecnologia offre la possibilità di realizzare varie soluzioni di continuità e Disaster Recovery, fino alla garanzia di fatto di un'erogazione continua dei servizi IT, necessaria per i sistemi (es. finanziari o di monitoraggio) definiti mission critical.

In pratica i sistemi e i dati considerati importanti vengono ridondati in un sito secondario o sito di Disaster Recovery per far sì che, in caso di disastro (terremoto, inondazione, attacco terroristico, ecc.) tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario nel più breve tempo e con la minima perdita di dati possibile.

Chiaramente quanto più stringenti saranno i livelli di continuità tanto più alti saranno i costi di implementazione della soluzione.

replica sincrona

La replica sincrona garantisce la specularità dei dati presenti sui due siti poiché considera ultimata una transazione solo se i dati sono stati scritti sia sulla postazione locale che su quella remota. In caso di evento disastroso sulla sede principale, le operazioni sul sito di Disaster Recovery possono essere riavviate molto rapidamente (basso RTO e RPO praticamente nullo).

La replica sincrona è limitata dalla incapacità dell'applicazione di gestire l'impatto del ritardo di propagazione (vincolo fisico quindi, e non tecnologico) sulle prestazioni. In funzione della sensibilità dell'applicazione e della tecnologia di comunicazione tra i due siti, l'efficacia della copia sincrona inizia a diminuire a una distanza variabile tra i 35 km e i 100 km.

replica asincrona

Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre spesso alla tecnica di copia asincrona. In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli. In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze).

Un ulteriore vantaggio della copia asincrona è la possibilità di essere implementata via software non dovendo necessariamente ricorrere a sofisticate e costose tecnologie di storage.

tecnica mista

Per garantire la disponibilità dei servizi anche in caso di disastro esteso e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere ad una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario e una copia asincrona su un sito a grande distanza.

Backup Online

Oggi i supporti di archiviazione tradizionale (DVD, Hard Disk esterni, penne USB, cartucce magnetiche, ecc.) sono ormai obsoleti, perché poco sicuri, troppo costosi e scomodi da gestire. Attualmente, si sta diffondendo un nuovo servizio, uno strumento che promette di rivoluzionare il modo di proteggere ed organizzare i propri file: il Backup Online.

Il Backup Online è un servizio informatico di cloud computing gestito attraverso un software che si installa (solitamente) sul proprio computer e che effettua l'archiviazione dei file attraverso connessione ad Internet sicura su un server remoto. Questo nuovo strumento a disposizione degli utenti della Rete prevede l'archiviazione di qualsiasi tipo di dato in modo completamente automatico.

La procedura classica è la seguente (ma può variare secondo il fornitore del servizio): una volta scaricato il software (il client) si avvia la procedura guidata di installazione. Quando questa è completata, si può scegliere se si vuole eseguire il backup dell'intero computer, oppure solo di alcune cartelle. Da questo momento, il software monitora i file in modo del tutto automatico, andando a salvare e a proteggere ogni volta tutti i documenti che vengono modificati o creati. Ci sono software che eseguono continuamente l'operazione di verifica e salvataggio (real-time) altri che sono invece programmati per operare ogni 24 o 12 ore.

I vantaggi del Backup Online rispetto all'archiviazione tradizionale sono molteplici, ecco alcuni esempi:

- I file sono trasferiti ed archiviati in modo sicuro, alcuni software utilizzano una cifratura a 128 bit, uguale o superiore a quella delle banche.
- Sono fisicamente in luoghi diversi da quelli in cui si trovano gli originali. In questo modo sono protetti anche in caso di furto o incendio.
- Si dispone di un grande spazio di archiviazione generalmente espandibile con un costo aggiuntivo nel momento in cui se ne ha bisogno.
- È possibile accedere ai propri dati, con credenziali riservate, in qualsiasi momento da qualsiasi postazione connessa ad Internet, alcuni fornitori del servizio consentono l'accesso anche da cellulare.

Requisiti tecnici del servizio

Il Backup Online presenta diverse caratteristiche che lo rendono più vataggioso rispetto ai classici sistemi di backup.

accesso ovunque

Prima di tutto è possibile accedere ai file protetti da sistemi di Backup Online in qualsiasi momento, direttamente dal client installato sul computer. Oppure da qualsiasi PC connesso ad internet e da telefono cellulare attraverso il sito web del gestore del servizio. Multicomputer (più computer un solo account): solo alcuni servizi consentono ad un solo utente di proteggere con il proprio account più computer. La maggior parte di essi segue il concetto: un account un computer. Grazie a questo sistema è possibile fare il Backup ad esempio del proprio computer di casa

e di quello del lavoro ed accedere ai dati con un'unica interfaccia indipendentemente da dove i file siano stati salvati.

archiviazione permanente

Inoltre è importante prestare particolare attenzione nei confronti della durata di archiviazione. Alcuni servizi, infatti, assicurano protezione per un tempo che può essere definito virtualmente infinito (ovvero per tutta la durata dell'abbonamento), altri servizi, invece, archiviano e proteggono i dati soltanto per alcuni giorni (solitamente 30 giorni). Questo significa che se per qualsiasi motivo hai smarrito i tuoi dati, hai a disposizione solo 30 giorni di tempo per recuperarli online, dopodiché li avrai definitivamente persi.

backup in tempo reale

Se l'utente crea un nuovo documento o modifica un file già esistente, il client salva immediatamente ed in automatico la modifica sul server remoto. Non tutti i servizi dispongono di questa funzione, alcuni eseguono il salvataggio solo ogni 12 o 24 ore.

completamente automatico

Una volta scelto cosa salvare, il client si avvia insieme al computer, lavora silenziosamente e continuamente in background per la protezione dei dati senza l'intervento dell'utente e solo se le risorse del computer (banda, ram, CPU) non sono utilizzate da altri processi più importanti. È possibile decidere di archiviare nuovi file in qualsiasi momento fino al completamento dello spazio disponibile.

condivisione

Il Backup Online è a tutti gli effetti un'estensione degli ormai noti sistemi di 'file sharing', ovvero i servizi che permettono di pubblicare online i propri files per renderli disponibili ad amici e colleghi o per disporre di un hard disk virtuale su Internet. Nel Backup Online c'è però una differenza importante. I dati sono già su Internet, questi vengono uplodati mentre si fanno altre cose e possono essere condivisi immediatamente con un solo click. Con alcuni servizi di Backup Online non importa, infatti, quale dimensione abbia il file da condividere, il client invia in automatico una e-mail al destinatario prescelto contenente l'indirizzo URL presso cui poter trovare il file. A questo punto, chi riceve l'e-mail clicca sul link ricevuto e preleva il file senza problemi. Per altri sistemi, invece, c'è un limite nella dimensione del file da uplodare ed il processo è più macchinoso.

prestazioni ottimali

I migliori servizi di Backup Online non rallentano il computer sul quale sono installati. Generalmente monitorano quante risorse del sistema si stanno utilizzando adeguandosi alle esigenze dell'utente. In questo modo le performance del computer non vengono compromesse.

motore di ricerca

Alcuni software di Backup Online hanno un motore di ricerca interno che consente una ricerca e gestione rapida dei propri file. Alcuni sono dotati di un sistema di ricerca semantica che consente una più approfondita ricerca ed analisi anche all'interno dei documenti e quindi un risultato più preciso.

scalabile On-Demand

In quasi tutti i servizi è possibile aumentare lo spazio a disposizione pagando una somma in base al numero di Gigabyte aggiuntivi richiesti. Molte software-house vendono lo spazio a pacchetti fissi di n. Gigabyte, altre invece, sono più flessibili e prendono in considerazione le richieste del cliente che esulano dai pacchetti standard.

versioning

Infine è il sistema che tiene traccia di tutte le modifiche effettuate su un determinato file per un tempo virtualmente infinito. Ogni volta che il file viene salvato, il sistema archivia la sola parte incrementale dello stesso e crea una nuova versione. Così, se si vuole ripristinare un vecchio documento che è stato sovrascritto involontariamente, è possibile tornare indietro ed accedere a tutte le versioni del file. Il

sistema non cancella i file salvati a meno che non sia l'utente stesso a deciderlo. Solo la minoranza dei fornitori dispone di questa caratteristica importante.

Tutela della privacy

Tutti i fornitori di servizi di Backup Online sono attenti e rispettano in modo rigoroso le norme vigenti in materia di privacy. Lo staff delle software-house che gestiscono questo tipo di servizio, aderisce ad un codice deontologico per il rispetto della privacy e utilizza le più avanzate tecnologie di sicurezza (spesso superiori a quelle previste dalla normativa) per garantire che i file degli utenti vengano archiviati nel modo più sicuro possibile. Normalmente tutte le comunicazioni con i server avvengono su un canale criptato SSL, lo stesso utilizzato dagli istituti bancari, mentre l'archiviazione dei file sui server avviene crittografando con i massimi standard internazionali.

Alcuni servizi di Backup Online garantiscono l'anonimato dell'utente perché non richiedono alcun dato personale per la registrazione al servizio. In altri casi ogni file è suddiviso in molte parti (i pacchetti) che vengono distribuiti su più server e ricostruiti solo quando il file è richiesto dall'utente. È come se si passasse il documento in un distruggidocumenti e si mettessero le striscioline di carta in luoghi diversi, solo quando il documento è necessario, questo viene riconsegnato intatto ovvero ricostruito dal sistema. In questo modo, anche se un malintenzionato trafugasse uno o più server dell'azienda fornitrice e riuscisse a decifrare il potente codice di protezione, non potrebbe aggregare i dati in suo possesso e quindi non potrebbe leggere alcuna informazione utile.

Servizi di backup online

Negli Stati Uniti il fenomeno del Backup Online è esploso nel 2007. Le aziende più conosciute sono attualmente Mozy e Carbonite. Anche i 'Big' sono, di fatto, entrati nel mercato del Backup Online. Amazon ha creato il proprio servizio S3 che distribuisce attraverso rivenditori terzi e Google ha intenzione di lanciare G-Drive, una sorta di estensione online del proprio hard-disk. Anche Microsoft e Sky stanno tentando di accaparrarsi una fetta di mercato offrendo servizi simili: il primo con Skydrive (http://skydrive.live.com) ed il secondo con Sky Store&Share (http://storeandshare.sky.com).

In realtà nei casi di Google, Sky e Microsoft è più corretto parlare di Storage Online e non di Backup. Infatti, nel loro caso si tratta solo di un'estensione online del proprio hard-disk che è offerta gratuitamente, ma garantisce solo pochi Gb di archiviazione per scopi non professionali. Tra i servizi fin'ora più utilizzati negli USA, oltre a quelli già citati, ci sono gli americani Idrive (www.idrive.com), Beinsync (www.beinsync.com) e iBackup (www.ibackup.com)

Memopal

In Europa, il servizio più conosciuto e che si sta rapidamente diffondendo in tutto il mondo, è Memopal (www.memopal.com) nato alla fine del 2007 dall'idea di imprenditori ed ingegneri Italiani ed ora focalizzato sulla qualità del servizio offerto.

CreshPlan+

CrashPlan+ è uno dei migliori servizi di backup online perché offre un software

eccellente, piani efficaci di backup e un buon insieme di funzionalità. L'interfaccia di CrashPlan è eccellente e le caratteristiche abbondano. Tra queste l'opzione web-based di ripristino, backup continuo, un livello di crittografia a 448-bit senza precedenti (meglio della tua banca). CrashPlan+ 10GB costa $ 2.99/mese e consente fino a 10 GB di spazio di archiviazione.

Backblaze Backblaze è un servizio di backup online molto semplice. Non inpone limiti di dimensione dei file, il che significa che si può eseguire il backup dei file della macchina virtuale e video! L'interfaccia del software è semplice, ma c'è un sacco di messa a punto disponibile se lo si desidera. Il costo di Backblaze è di 5 $ / mese / computer e consente archiviazione illimitata. Il costo può arrivare fino a un mensile di 3,96 dollari se si acquisto un piano di due anni.

Carbonite Qualsiasi servizio di backup dovrebbe essere facile da usare, automatico, affidabile e facile da ripristino. Carbonite è tutto questo. Molte persone vanno in estasi per i piani di backup online di Carbonite - è stata una scelta molto popolare per un tempo molto lungo. La mia esperienza è stata altrettanto positiva. Il servizio di backup online Carbonite costa $ 59.99 / anno e permette un backup dei dati illimitato.

Mozy Il servizio di backup online di Mozy funziona in modo simile ad altri servizi - basta scaricare e configurare il software e il backup viene gestito automaticamente in background. Mozy Home è gratuito e permette fino a 2 GB di spazio di archiviazione sui server di Mozy. Ulteriori piano prevedono 5.99 dollari/mese per 50 GB da un computer e 9,99 dollari/mese per 125 GB di spazio di archiviazione da un massimo di tre computer.

SOS SOS è un grande servizio nel mondo del backup online, e per buoni motivi. Tutti i piani offrono il supporto per un numero illimitato di dispositivi, versioning illimitato, backup dei dati continuo, supporto di unità di rete, e tanto di più. I piani di backup on-line SOS sono disponibili da 100 GB, 150 GB e 250 GB e le dimensioni sono in base al prezzo, rispettivamente, a 9,99 dollari / mese, 15,99 dollari/ mese e 19,99 dollari/ mese. È possibile ottenere forti sconti su tali prezzi se il pagamento avviene anticipatamente per uno o due anni.

Livedrive Livedrive è un servizio di backup online che offre un interessante mix di piani di backup, un modo conveniente per aggiungere i computer, e davvero una bella interfaccia mobile. Il piano Livedrive Backup è illimitato e costa 8,00 dollari/ mese per computer. Aggiungere un computer costa solo 1,50 dollari / mese.

SugarSync SugarSync è un servizio diverso, in senso buono. In realtà è molto più di un servizio di backup online. Mentre SugarSync fa backup tradizionale, altrettanto bene o meglio di gran parte della sua concorrenza, può anche sincronizzare i file tra tutti i dispositivi, consente di accedere ai vostri dati di backup dal vostro smartphone, e molto altro.

IDrive IDrive è simile per molti versi ad altri servizi di backup online. Forse la cosa migliore di IDrive è che si tratta di una opzione gratuita di backup non in linea, qualcosa che non ho visto con qualsiasi altro servizio e che risulta (molto) utile per backup di grandi dimensioni iniziali. Altre caratteristiche che permettono a IDrive di distinguersi tra la concorrenza includono il supporto per la mappatura delle unità ed eccellenti applicazioni mobili. IDrive di base è completamente gratuito e vi offre fino a 5 GB di spazio di archiviazione.

Ciphertite

Cyphertite è un piccolo provider di backup online, ma può essere considerato tra i migliori per una serie di motivi, tra cui il fatto di essere open source e facile da usare, e per offrire forse la migliore sicurezza tra qualsiasi offerta di backup online.