techsystem
Soluzioni per l'Informatica

Backup su Server Remoto

Techsystem srl
www.techsystem.it – info@techsystem.it
PEC: amministrazione@pec.techsystem.it

sede legale e amministrativa
via parma, 64 – 10153 Torino
tel. 011.24.89.221 – fax 011.74.32.104

c.f. e p.iva: 08508960013
cciaa di torino n° 08508960013
capitale sociale 10.000 euro i.v.

techsystem
Soluzioni per l'Informatica

Indice del documento

techsystem
Soluzioni per l'Informatica

1. Attacchi alla vostra impresa

1.1 Virus: Il peggio deve ancora venire

La velocità di propagazione e la nocività dei virus fanno parlare ogni giorno di sé. Per definizione gli antivirus trattano solo i virus conosciuti. Contro un nuovo Virus, l'unica risposta è avere una tecnologia che ti consenta di recuperare i dati ripercorrendo il tempo.

1.2 Sinistri: succedono solo agli altri

Inondazioni, incendi, tempeste, sovratensione, crolli, vandalismo, ecc. costano ogni anno milioni di euro alle compagnie di assicurazione. Un risarcimento danni di tipo economico non potrà mai sostituire i vostri dati perduti.

1.3 Pirateria: l'assalto è lanciato

Sapete che l'85% degli atti di pirateria e di danni informatici provengono dall'interno della vostra stessa impresa?

1.4 Errore di manipolazione: tutto questo lavoro è da rifare!

Chi non ha mai distrutto un file per errore? Un comando errato basta per cancellare irrimediabilmente il contenuto di un intero disco. La ricostruzione di poche centinaia di Mb di dati può necessitare molti giorni di lavoro e può costare migliaia di euro.

1.5 Crash informatico: i dati sono la vittima immediata

Spesso accade che un file sia irrecuperabile a causa dell'arresto brutale di un sistema, di un'applicazione errata o di altre ragioni inspiegabili. Spesso il problema viene scoperto troppo tardi e la versione precedente del file non può più essere utilizzata.

1.6 Supporti informatici: fragili e deperibili

Gli hard disk possono essere vulnerabili e i dati sono salvati tradizionalmente su cassette o su supporti magnetici che hanno vita breve e sono fragili.

techsystem
Soluzioni per l'Informatica

2. Un' offerta globale per una protezione totale dei vostri dati

2.1 Per la protezione del vostro sistema informatico

- La salvaguardia quotidiana e automatica delle vostre informazioni
- Il trasferimento via rete dei dati salvati e criptati sul centro esterno in estrema sicurezza
- Il recupero dei dati archiviati in maniera autonoma (nel caso di singoli file) o, su richiesta (opzionale) dell'intero archivio.

2.2 Obbiettivo sicurezza totale

Techsystem vi può fornire tutte le risposte:

- Resoconto dei salvataggi tramite email
- Invio di archivi su CD/DVD

2.3 Protezione della privacy

Tutti i dati trasmessi dal cliente, verso i server di backup remoti, sono protetti da una duplice chiave:

- Una password per l'apertura dei file contenenti i dati
- Una chiave di criptazione a 128/256 bit per criptare e rendere inaccessibili i dati prima che questi vengano trasferiti sul server remoto attraverso internet.

Inoltre i server di backup remoti sono protetti da meccanismi di firewalling che tendono a bloccare tutti i tentativi di accesso non autorizzato ai sistemi.

Questi meccanismi di protezione fanno si che, anche nel caso in cui i dati venissero "rubati", o durante il trasferimento o direttamente sui server remoti, sarebbero comunque inutilizzabili. Neanche il personale di Techsystem è in grado di accedere ai dati del Cliente. La corretta gestione delle password, da parte del Cliente, diventa quindi essenziale per un eventuale corretto ripristino dei dati stessi. L'unica attività che il personale autorizzato di Techsystem è in grado di fare, è di riconsegnare eventualmente gli archivi completi ancora protetti (e quindi inaccessibili), a questo punto solo il Cliente, grazie alle password corrette, potrà decriptare e aprire gli archivi. In assenza delle password gli archivi sono completamente inutilizzabili.

3. Sicurezza

3.1 Sicurezza fisica

Techsystem possiede rack dedicati ai vari server. La soluzioni attualmente adottate per il servizio di backup remoto prevede l'uso di uno o più server con varie tecnologie di protezione (dischi in configurazione RAID, backup su nastro, UPS, protezione fisica).

Fisicamente i locali, in cui sono posizionati i server, sono ad accesso limitato e controllato. I server sono monitorati e controllati quotidianamente e vengono costantemente mantenuti aggiornati per eliminare tempestivamente tutte le "falle" sulla sicurezza riscontrate e risolte dai produttori dei vari software installati. I server sono anche protetti da firewall dedicati che vengono controllati ed analizzati quotidianamente.
Un impianto di allarme dedicato avvisa telefonicamente e tempestivamente i tentativi di accesso non autorizzati ai locali che sono anche sorvegliati nei giorni di chiusura e durante la notte da un servizio di pattugliamento esterno.

3.1 Sicurezza logica

Il backup su server remoti offre:

- un maggior grado di sicurezza rispetto ai normali sistemi di backup dei dati (su DVD, cartuccia magnetica, HD esterni). In caso di eventi dannosi quali furto, incendio, allagamento, crollo, ecc...
- Maggior sicurezza sulla inviolabilità dei dati stessi. Questi infatti non sono facilmente accessibili su supporti normalmente lasciati appoggiati sopra i server o in un posto comunque vicino e facilmente accessibile, ma sono remoti (quindi irraggiungibili fisicamente) e solo l'utilizzo delle apposte password ne consente l'accesso.
- L'inviolabilità dei dati, oltre che essere garantita a livello fisico (vedi punto precedente) è anche garantita dal fatto che tutti i dati, prima di essere trasferiti in remoto, sono criptati con algoritmi di criptazione molto forti e inviolabili con le attuali tecnologie.

3.2 Garanzie di continuità

I nostri server sono attivi e monitorati 24h su 24h, 365 giorni l'anno. Il ripristino di dati persi può avvenire con semplicità e direttamente da parte del Cliente a qualsiasi ora del giorno e della notte. Nel caso in cui fosse necessario il supporto tecnico, il nostro staff è in grado di seguire ed aiutare il Cliente per ogni necessità

4. Confronto con le soluzioni tradizionali

Per poter correttamente valutare i pregi del backup su un server remoto è possibile fare delle veloci considerazioni sui possibili lati negativi del backup di tipo tradizionale (es. su nastro magnetico, su HD esterno):

- Il nastro magnetico è soggetto ha molti problemi fisici (smagnetizzazione causata da scorretta conservazione, dal caldo/, dalla vicinanza di altre apparecchiature elettromagnetiche).
- Solitamente ci si accorge che il backup tradizionale non funziona solo dopo molti mesi e solitamente quando sarebbe necessario recuperare dei dati (che quindi sono andati persi).
- Le procedure di controllo della corretta esecuzione dei backup tradizionali sono solitamente impegnative (dovrebbero essere fatti quotidianamente) e un normale utente aziendale spesso non ha le conoscenze tecniche per poter correttamente valutare situazioni di pericolo, il che porta spesso a sottovalutarle e a rendersi conto del problema quando ormai è troppo tardi
- Gli hard esterni spesso smettono di funzionare senza che nessuno se ne accorga e se si rompono si perde tutto.
- Un nastro e/o un hard disk esterno è e soggetto a facili furti. Tutti i dati aziendali possono essere quindi trafugati con la massima velocità e semplicità. Spesso passano mesi prima che qualcuno se ne accorga. In molti casi il Cliente non se ne accorge proprio (ad es. per i nastri).
- I costi legati ai ricambi (cassette, dischi, DVD, ecc) ed i costi legati al tempo impiegato da una persona per cercare di fare e controllare (male) tali procedure sono spesso "nascosti" ma sono valutabili anche in qualche migliaio di euro/anno (in relazione alla dimensione del Cliente)
- Un attacco tramite un virus può facilmente compromettere completamente un hard disk esterno cancellando o infettando tutti i dati presenti rendendoli inutilizzabili.

… e queste sono solo alcuni dei molti problemi. A conti fatti, una soluzione di backup su server remoto, oltre a risultare decisamente più affidabile e sicura risulta anche essere di pari costo (e spesso addirittura più economica) di una soluzione tradizionale…

In ogni caso è comunque sempre consigliabile avere una soluzione tradizionale a cui affiancare la soluzione di backup remoto. La protezione dei dati viene prima di tutto!