Informatica

Salvaguardare i dati per salvare l'azienda

di Nicola Bortolotti

Non esistono - almeno in Italia - polizze assicurative che coprano espressamente la perdita di dati su supporto informatico. Esiste una legge, mal scritta e - di conseguenza - spesso disattesa, che prescrive le "misure minime per la protezione dei dati personali" non ottemperando alle quali si può incorrere in sanzioni civili e penali in assenza di un'adeguata salvaguardia dei dati.
In moltissimi uffici è facile vedere una cassaforte, più o meno dissimulata, più o meno voluminosa, più o meno tecnicamente avanzata. Ma non si vedrà mai un Personal Computer dentro una cassaforte, anche se il suo contenuto è non meno prezioso.
La vera ricchezza di molte aziende - anche nel settore funerario e cimiteriale - è costituita, infatti, proprio dai dati memorizzati nei computer o - meglio - nei "dischi fissi" (che in realtà si possono montare su supporto per essere facilmente rimossi...) più propriamente detti "dischi rigidi", fedele traduzione dell'inglese "hard disk". Dischi che, in quanto uniche parti in movimento del computer (a parte le ventole, non a caso tra le principali imputate in caso di guasti), hanno una vita dichiaratamente limitata, sono fisicamente fragili, sensibili ad urti e vibrazioni.
Affidereste la vostra vita a qualcosa che, cadendo inavvertitamente dalle mani, si guasterebbe quasi sicuramente? Probabilmente no. E, allora, perché affidare la gestione del core business a tecnologia siffatta? La risposta è semplice: non esistono a tutt'oggi valide ed economiche alternative "consumer" alla tecnologia di memorizzazione su disco magnetico rigido. Vi sono tuttavia numerosi accorgimenti tecnici ed operativi, la maggior parte dei quali a costo quasi zero, in grado di salvare i dati - e con essi l'azienda - di fronte a - pressoché - qualsiasi evenienza, ivi compreso l'attacco di un virus che potrebbe distruggere, modificare o diffondere i dati contenuti nell'hard disk più affidabile dell'universo.

Qualche definizione

Esistono due termini fondamentali da considerare quando si parla di sistemi informatici: "high reliability", ossia alta affidabilità, e "disaster recovery", ossia ripristino dopo un disastro. Con alta affidabilità si intende un sistema capace di funzionare h24 mentre con disaster recovery si indica la possibilità di recuperare i dati vitali dopo un evento traumatico.
Queste espressioni hanno un significato ben distinto quando si parli di "grandi" sistemi informatici (ad esempio: la capacità di funzionare in presenza di un'interruzione nell'erogazione dell'energia elettrica attiene all'high reliability mentre il ripristino dopo un terremoto o un'alluvione riguarda il disaster recovery) mentre le differenze tendono a stemperarsi quando ci si occupa di piccoli sistemi, ossia quelle configurazioni che possono andare dal singolo Personal Computer stand alone alla piccola rete locale con alcune decine di PC collegati. Nel seguito, dunque, non si farà specifica distinzione tra i due casi parlando genericamente di misure per la salvaguardia dei dati memorizzati su supporti informatici.

Per bene iniziare

Si è accennato, in apertura, alla causa forse primaria di perdita di dati in un piccolo contesto aziendale, ossia il guasto di un hard disk. Esistono società in grado di tentare il recupero di dati da dischi non funzionanti, ad esempio la famosa Ontrack (l'homepage del sito in figura 1, all'indirizzo http://www.ontrack.com) che si occupò - fra l'altro - del recupero di molti dei dischi alluvionati in Piemonte qualche anno fa.
È bene tuttavia sottolineare che il recupero è un'operazione sempre assai costosa e dall'esito incerto.
Mai come in questo caso - dunque - è opportuno prevenire gli eventi. Una misura che è sempre consigliabile mettere in opera a priori su almeno uno dei PC utilizzati in una piccola rete (tipicamente quello al quale vengono affidati i compiti di "server"), è il cosiddetto "mirroring" dei dati, tecnicamente definito anche RAID1.

Il “mirroring” consiste nel gemellare due dischi rigidi, preferibilmente di pari caratteristiche, facendo in modo che contengano esattamente gli stessi dati in ogni momento, ossia che siano l’uno lo specchio (da cui il nome) dell’altro. L’utente non vedrà due hard disk ma solo uno, in quanto ogni scrittura su disco è in realtà un “write” simultaneo su entrambi i dischi. Eventuali incongruenze ed errori vengono prontamente segnalati (all’occorrenza anche in email!) dando la possibilità di sostituire l’unità guasta senza la perdita di nemmeno un byte: è infatti estremamente improbabile che due dischi cessino di funzionare esattamente nello stesso istante.

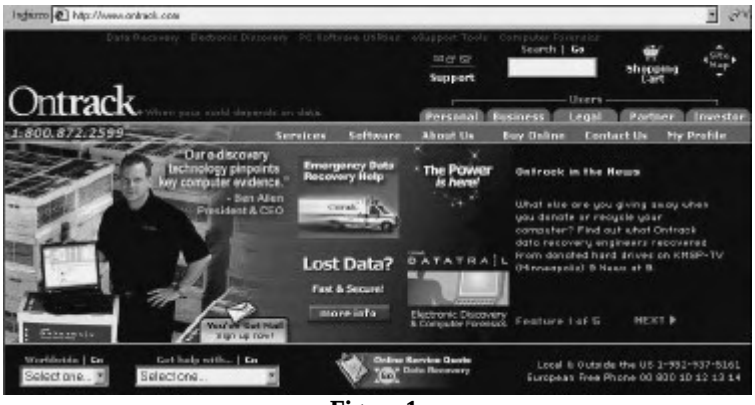

Figura 1

In figura 2 un esempio di due hard disk identici in mirroring (l’array è visto a tutti gli effetti come un unico disco, ma assai più affidabile); in calce è visibile la segnalazione di un errore verificatosi nel passato.

Il RAID1 si può attivare via software (ad esempio in Windows NT Server) ma è sicuramente preferibile affidarsi a un controller hardware che si occupi di tutto. Una valida alternativa alla soluzione SCSI, assai costosa, è costituita dai RAID controller EIDE: sono economici (in figura 3 l’homepage di HighPoint, uno dei principali produttori) e spesso vengono direttamente inclusi nelle mother board di maggior pregio (la loro incidenza di costo si può valutare in una quarantina di euro). Vi è poi da considerare il raddoppio del costo dell’hard disk (occorre acquistarli a coppie) ma - considerando il drastico incremento di affidabilità conseguente ed il prezzo ridotto dei dischi rigidi (un’ottantina di euro per un 20 GB ad alte prestazioni) - un tale investimento appare quasi come un dovere.

Figura 2

Non è necessario dotare ogni macchina di mirroring: è sufficiente prevedere l’array dei due dischi gemelli sul server, ossia sul PC alle cui directory condivise in rete confluiranno tutti i dati della rete locale. Server che andrà anche dotato di gruppo di continuità (UPS) in modo da permettere uno spegnimento non traumatico (sempre sgradito ai dischi) anche in presenza di interruzione della corrente di alimentazione.

L’importanza dei backup

Da quanto esposto potrebbe apparire fortemente ridimensionata l’utilità dei cosiddetti “backup”, ossia delle copie di salvataggio dei dati da effettuarsi periodicamente.

In realtà il mirroring non sostituisce il backup: lo “specchio” dei dischi non consente infatti di supplire alla cancellazione involontaria dei dati, alla perdita o corruzione di files derivante dall’azione di un virus e ad altri eventi similari.

Sarebbe dunque bene prevedere un archivio storico di backup, da aggiornarsi con cadenza almeno settimanale.

Sulla tecnologia da adottare per il backup esistono differenti scelte. Per grandi volumi di dati, ossia per immagini di interi dischi, la tecnologia d’elezione è quella della cassetta di nastro magnetico (tipicamente 4mm, 8mm o formati specifici per dati). Per dimensioni più limitate - che sono quelle che interessano in questa sede - può essere invece sufficiente e consigliabile (se intorno ai 600-700 MB) un CDRom o un CD riscrivibile.

I vantaggi del CD sono - principalmente - il costo ormai irrisorio, l’insensibilità ai campi magnetici e ad altri eventi quasi sempre distruttivi per il materiale magnetico (per motivi, tuttavia, precipuamente meccanici) come le alluvioni.

Varie sono le avvertenze da osservare in caso di backup su CD (ma anche su cassetta): ad esempio, nei backup periodici su supporto riscrivibile, si dovrà avere cura di non sovrascrivere mai il backup

immediatamente precedente. In caso di malfunzionamento durante il backup si rischierebbe infatti di perdere non solo i dati attuali ma anche quelli della copia di riserva più recente.

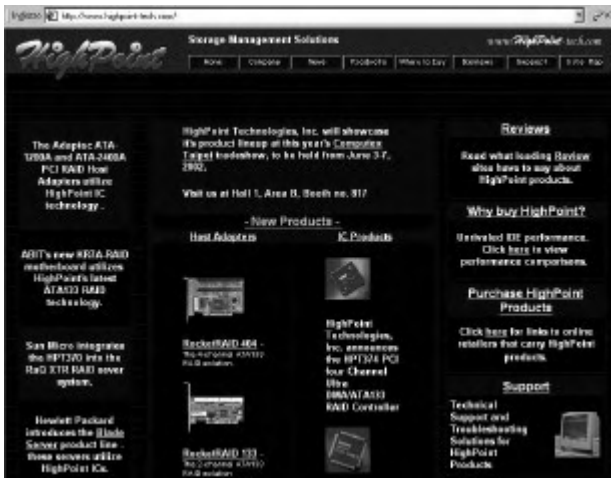

Figura 3

Seconda avvertenza: fare possibilmente una doppia copia di backup su supporti di produttore diverso (per minimizzare l'effetto di eventuali incompatibilità e/o difetti di produzione) e conservarli in luoghi fisici diversi dei quali uno tassativamente lontano dall'ubicazione del Personal Computer (per evitare che, nel caso di furto, incendio, alluvione o terremoto possano andare distrutti sia l'archivio principale che i backup).

Terza avvertenza: verificare sempre la correttezza della copia dopo la scrittura confrontando l'originale con il CD masterizzato.

Quarta avvertenza: pianificare adeguatamente la periodicità dei backup rispettando con scrupolo le consegne. È anche possibile utilizzare "scheduler" automatici ed effettuare i backup in maniera semiautomatica, limitando l'intervento degli operatori alla sostituzione dei CD e/o cassette.

Il vetusto backup su floppy disk è senz'altro da evitare: non solo perché la capacità di un floppy è minima, ma anche perché l'affidabilità di un hard disk è sensibilmente superiore a quella di un floppy.

Si noti che la conservazione di una copia di backup al di fuori dei locali aziendali può indubbiamente avere ripercussioni per quanto concerne le misure minime di protezione dei dati personali, specie se sensibili. Ma, in questa sede, si è voluto porre l'accento unicamente sulla salvaguardia dei dati.

E per finire un buon antivirus

Le misure sin qui esposte possono mettere al riparo - in parte e indirettamente - anche di fronte all'azione maliziosa ed eventualmente dolosa di un virus. Ma ignorare il problema sarebbe irresponsabile: oggi i virus più diffusi sono in realtà "worm" che si propagano a macchia d'olio via posta elettronica, codici progettati con grandi acume e scaltrezza e in grado talora di arrecare danni assai gravi anche di immagine e con conseguenze potenzialmente penali, diffondendo - ad esempio - documenti riservati presenti nel PC dell'ignaro utente infettato.

Anche in questo caso la prevenzione costa assai meno del "restore", a patto di utilizzare strumenti idonei.

Le stesse misure minime di protezione dei dati personali prescrivono l'installazione di un software antivirus da aggiornare almeno ogni due mesi. Va tuttavia sottolineato il fatto che - se si vuole che l'antivirus funzioni correttamente - gli aggiornamenti delle impronte virali vanno effettuati almeno una volta alla settimana. Nulla è più dannoso di un antivirus non aggiornato che veicoli una falsa sensazione di protezione.

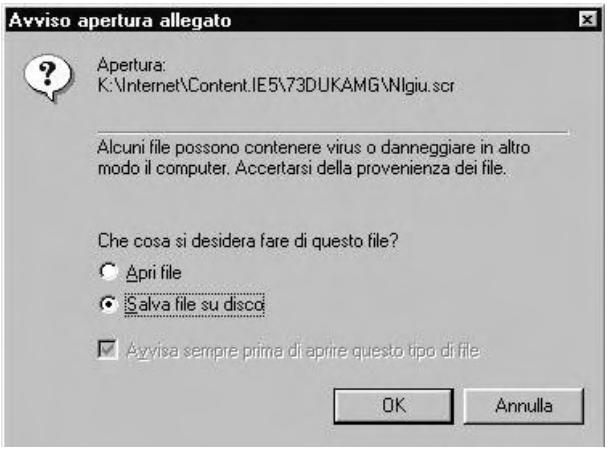

Figura 4

Inoltre va regolarmente verificata anche l'esistenza di "patches" ("pezze" correttive software) per i programmi di posta elettronica: soprattutto se si utilizza Microsoft Outlook Express si dovrà visitare con regolarità il sito http://windowsupdate.microsoft.com facendo attenzione alle "security patches" in genere incluse negli "aggiornamenti importanti" e in quelli "critici".

Questo perché molti virus - con alcune versioni base di Outlook Ex-

Da	A	Oggetto
selelzionepersonale	nbsoft@hotpop.com	Some questions
polito	nbsoft@infinito.it	How are you
uffper	nbsoft@libero.it	Worm Klez.E immunity
barbara	nbsoft@libero.it	A humour game
nbsoft	nbsoft@tiscalinet.it	Worm Klez.E immunity
rosario22	nbsoft@hotpop.com	Border
postmaster	nbsoft@libero.it	Returned mail--"border"

Figura 5

press - si attivano anche se il messaggio sospetto non viene effettivamente aperto. Ecco quindi che il tipico messaggio popup (in figura 4 uno di quelli generati dal famoso Klez.h) non viene nemmeno proposto all'utente e il virus è attivato fin dall'anteprima del messaggio.
Da notare, anche, che le precauzioni - pur indispensabili - di porre attenzione al mittente del virus, di non aprire mai mail sospette e così via, diventano sempre più ardue da applicare (si vedano ad esempio i messaggi in figura 5, nei quali i mittenti sono

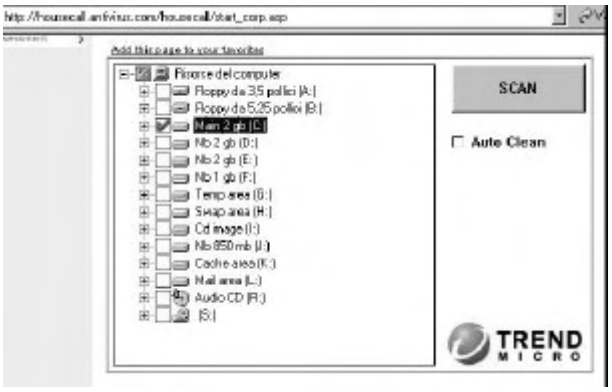

Figura 6

stati parzialmente oscurati in ossequio al rispetto della privacy: tutti veicolano un virus, anche quelli che promettono di immunizzare dal Klez.E).
Si rimarca quindi l'esigenza di dotarsi di un prodotto antivirus residente, in grado di intercettare sul nascere gli accessi maligni al sistema.
In fase decisionale è possibile procedere a scansioni gratuite (ad esempio collegandosi al sito http://housecall.antivirus.com/, figura 6), oppure scaricare programmi gratuiti ma più efficaci di molti celebrati prodotti commerciali nel verificare la presenza di alcuni dei virus maggiormente diffusi e rimuoverli effettivamente (in primis l'ottimo CLRAV scaricabile all'indirizzo http://www.questar.it/download/clrav.com) o, infine, downloadare versioni di prova valevoli trenta giorni come, ad esempio, quella offerta da F-Prot (http://www.complex.is), un software antivirale che si distingue per la politica commerciale particolarmente aggressiva e allettante nel caso in cui si debbano proteggere più Personal Computer: la licenza-base annuale costa appena quaranta dollari e copre fino a venti PC. Per ogni PC in più, sino a 2500, il "fee" è di due dollari aggiuntivi per ciascuno.

Firma digitale in fermento

Rilevanti novità sul fronte della firma digitale. La pubblicazione sul bollettino 6/2002 dell'Autorità per l'Informatica nella Pubblica Amministrazione (http://www.aipa.it) dell'editoriale sul recepimento della Direttiva UE sulla Firma Digitale del 1999 ha reso ancor più ufficiale presso gli addetti ai lavori di quanto già non fosse con la pubblicazione del D.L. n.10 emanato il 23 gennaio scorso e pubblicato sulla Gazzetta Ufficiale n.39 del 15 febbraio il nuovo quadro normativo al quale – necessariamente - ha dovuto uniformarsi anche l'Italia.
Ecco quindi apparire nuovi scenari concernenti il "documento informatico" tout court (senza alcuna sottoscrizione elettronica) che ora ha l'efficacia probatoria prevista dall'art. 2712 del C.C.
Per i certificatori - che possono far parte di qualsiasi paese dell'UE - non è più richiesta l'autorizzazione preventiva.
Vengono inoltre introdotte tre diverse tipologie di firma: firma elettronica (la sua ammissibilità sarà sottoposta alla valutazione del giudice), firma digitale e firma elettronica avanzata, sulle peculiarità delle quali ci si soffermerà nei prossimi numeri anche alla luce delle trasformazioni che subirà l'AIPA stessa.
Con l'istituzione dell'Agenzia nazionale per l'Innovazione tecnologica, l'AIPA - fino ad ora l'unico e autentico punto di riferimento in Italia per quanto concerne normativa ed esegesi legislativa - confluirà infatti nella neonata struttura che - presumibilmente - giocherà un ruolo fondamentale nello sviluppo della carta d'identità elettronica e della carta nazionale dei servizi.