ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
BRESCIA

VADEMECUM N. 3

LA SICUREZZA DEI DATI

a cura di Filippo Fornari e Luca Calzolari

Commissione Consultiva Organizzazione dello Studio e Informatica

Coordinatore: Gianantonio Poli. Delegato del Consiglio: Elisabetta Migliorati. Membri: Maurizio Bacchiega, Aldo Bertana, Francesca Bertelli, Luca Calzolari, Davide Felappi, Filippo Fornari, Stefano Guerrini, Biagio Notario, Alberto Odorici, Aldo Massimo Rossi, Marco Scardeoni, Paolo Tebaldini, Carlo Valetti e Fabio Zotti.

LA SICUREZZA DEI DATI

PREMESSA

La facilità con cui vengono sempre più padroneggiate le tecnologie informatiche all'interno dei nostri studi non deve far dimenticare la vulnerabilità di tale patrimonio di conoscenze che potrebbe venire trafugato, manomesso o distrutto (si parla di "ricchezza fragile" dell'era digitale) se non vengono implementate opportune strategie volte a preservare la confidenzialità, l'integrità e la disponibilità dei sistemi informativi.

Confidenzialità è la caratteristica di una informazione ad essere accessibile esclusivamente a coloro che sono autorizzati. Di tale caratteristica si occupano, ad esempio, i sistemi di autenticazione delle credenziali, cioè la *userid* e *password* a cui viene associato un sistema di credenziali oppure i *firewall* che filtrano le transazioni tra la rete locale LAN (*Local Access Network*) e la rete WAN (*Worldwide Access Network*) secondo opportune regole di sicurezza.

Disponibilità è la caratteristica di una informazione ad essere disponibile per tutti coloro che sono autorizzati quando la richiedano mentre integrità è la caratteristica di una informazione che sia corretta, completa e correttamente elaborata.

Di tale ultime due caratteristiche si occupano, ad esempio, i sistemi di *mirroring* dei dischi, i sistemi di alimentazione secondaria, i sistemi di replica dei server, i sistemi di back-up dei dati e le procedure di ripristino dei dati.

La sicurezza informatica deve essere intesa come un sistema di processi atto a valutare l'impatto della vulnerabilità delle informazioni e dei sistemi di processazione delle stesse e della probabilità che esso si avveri.

Tale attività di valutazione deve dare guida alla predisposizione di misure e processi che servano ad individuare, controllare e minimizzare i rischi derivanti dalla vulnerabilità dei sistemi informativi ad un costo accettabile.

Tra le principali misure da tenere in considerazione per l'implementazione di un sistema di sicurezza possiamo elencare:

1. Inventario e monitoraggio delle risorse del sistema, e cioè le apparecchiature a disposizione, i sistemi operativi, i programmi utilizzati ed i database e *data files* rilevanti, con la loro ubicazione ;

2. Sicurezza e controllo sul personale che accede ai sistemi informativi, che deve essere adeguatamente formato anche sulle corrette modalità d'uso del sistema informativo per evitare rischi ;
3. Sicurezza fisica e perimetrale, sia dei locali dove sono custoditi i server, sia delle connessioni alle reti esterne con i firewall ;
4. Equipaggiamento adeguato delle risorse del sistema, quali cablaggio certificato, connessioni *wireless* criptate, alimentatori di sicurezza (UPS), periodico aggiornamento del sistema operativo delle macchine e apparecchiature installate ;
5. Procedura di sicurezza per la dismissione di apparecchiature o per il loro riutilizzo ;
6. Sistemi di difesa dai programmi maligni (antivirus) costantemente aggiornati ;
7. Sistemi di autenticazione e log degli accessi degli operatori ;
8. Back-up dei dati rilevanti , dei principali software e dello stato dei sistemi ;

Ma soprattutto la maggior sicurezza consiste nell'affidare ad un professionista esperto l'implementazione e la sorveglianza di un sistema di sicurezza per evitare di fare investimenti in tecnologie avanzate, come un necessario firewall, dimenticandosi poi la "porta aperta" per avere un modem in risposta automatica dimenticato in rete o disporre di un sofisticato sistema di accesso ai dati a mezzo credenziali di autenticazione e poi assegnare a tutti gli utenti gli stessi diritti.

Come insidie che possono influenzare un sistema informativo i più potrebbero ricordare i programmi maligni, comunemente noti come virus, trojan …, gli attacchi da internet ma sono altrettanto insidiosi la sottrazione o manipolazione di dati da parte del personale interno oppure collassi strutturali quali incendio o terremoto, eventi non certo probabili ma il cui verificarsi potrebbe causare ingenti ed irreparabili danni anche ai sistemi informativi.

LA NORMATIVA SULLA CONSERVAZIONE DEI DOCUMENTI FISCALI

Ai fini fiscali in generale, i documenti rilevanti devono essere conservati almeno per i quattro anni successivi alla presentazione della dichiarazione dei redditi e IVA di riferimento (articoli 43 DPR 600/73 e 57 DPR 633/72). Nel caso di omessa dichiarazione il termine è aumentato di un anno.

Questi sono i termini "normali" entro cui può essere notificato l'atto di accertamento ai fini delle imposte sui redditi e del valore aggiunto. E' da ricordare, inoltre, che l'art. 5 bis comma 1 lett. e) del D.L. n. 282/2002 ha prorogato i termini di due anni per tutti i soggetti che non si sono avvalsi delle norme relative al concordato per gli anni pregressi, dichiarazione integrativa e condono tombale di cui alla Legge 27/2003 che ha convertito il D.L. in parola. Conviene inoltre prolungare prudentemente i termini di conservazione anche per tener conto delle proroghe, previste appunto in casi di sanatorie o condoni, per l'esercizio dell'attività di controllo.

In realtà per il caso della perdita, distruzione accidentale o di furto dei documenti contabili manca una norma specifica che ne disciplini le conseguenze. L'unico caso preso in considerazione è quello dell'articolo 39 comma 2 lettera c), secondo il quale qualora le scritture contabili non siano disponibili per "causa di forza maggiore" si attribuisce all'Ufficio il potere di determinazione induttiva del reddito, avvalendosi anche di presunzioni semplici, nonché prive dei requisiti di gravità, precisione e concordanza. Ricordiamo che la causa di forza maggiore è quella in cui l'evento si manifesta malgrado l'adozione di un comportamento diligente.

Per effetto di tale situazione normativa, è evidente come sia abbastanza oscuro il comportamento che il contribuente deve seguire nel caso in cui le scritture, per motivi indipendenti dalla propria volontà, vengano perdute. L'unica conclusione che si può trarre, a fronte della citata norma, è che, nel caso di smarrimento (ipotesi che non può certamente annoverarsi tra le cause "di forza maggiore" che è, al contrario, il caso del sisma), l'Ufficio dovrà applicare l'accertamento analitico e non quello induttivo.

Ciò non può dirsi, invece, per i casi di furto o di distruzione per incendio o sisma, che rientrano nei casi di forza maggiore.

Questo non vuol dire, ovviamente, che il contribuente, nonostante la propria buona volontà abbia avuto distrutti o rubati i documenti e le scritture contabili, sia esonerato dal fare alcunché per rimediare al danno. Al contrario, la giurisprudenza pare

concorde nell'affermare che il contribuente, successivamente all'evento dannoso, abbia il dovere di adoperarsi per ricostruire i dati e gli elementi contenuti nelle scritture andate distrutte. In particolare la R.M. n. 445366 del 27/7/91 ha previsto l'obbligo della ricostruzione contabile: è del tutto evidente che un comportamento positivo del contribuente improntato alla fattiva collaborazione nella ricostruzione delle scritture contabili, non potrà non essere favorevolmente valutato nell'ambito dell'eventuale contestazione dell'accertamento fiscale.

Nella risoluzione di tale problema, però, un aiuto viene sia dalla considerazione che ormai la contabilità è tenuta in maniera informatica, sia dalla disciplina che ha semplificato la tenuta dei libri contabili. Essa infatti, avendo soppresso l'obbligo della bollatura e vidimazione dei libri diversi da quelli sociali, permette di poter ristampare in qualunque momento le scritture. Per cui, fermo restando che per il passato resta valida la regola disposta dalla succitata risoluzione ministeriale, oggi si può ammettere una nuova istituzione dei libri mancanti. Tutto ciò, si ribadisce, nei limiti in cui si applica la nuova norma semplificatrice, ossia in riferimento ai libri contabili, e non anche a quelli sociali.

E' utile, comunque, prima di procedere alla ristampa dei registri che sono andati perduti, procedere con una denuncia alle competenti Autorità di Pubblica Sicurezza. Nel diverso caso in cui la perdita riguardi anche le fatture, e in generale i documenti probatori dei fatti di gestione, il contribuente avrà il difficile compito di contattare gli interlocutori (clienti, fornitori, banche ecc.) per reperire le copie.

E' ovvio che, a questo punto, se è vero che la normativa consente la stampa *ex novo* delle scritture contabili, si rende assolutamente indispensabile il poter disporre di un sistema di archiviazione dei dati che sia garantito da eventi accidentali e, nel caso, anche dal sisma.

Sul sito del GARANTE della PRIVACY è pubblicato il *Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice)*nel caso di trattamento dei dati con strumenti elettronici, ovvero le modalità tecniche da adottare a cura del titolare, del responsabile e dell'incaricato, in caso di trattamento di dati mediante strumenti elettronici. Nel DPS è quindi necessario prendere atto della propria situazione specifica e definire quale sia il sistema di sicurezza che consenta il ripristino dei dati anche nel caso estremo di un vero e proprio disastro.

UNA MISURA NECESSARIA : IL BACK-UP DEI DATI

Con la parola back-up, copia di sicurezza, o copia di riserva nell'informatica indichiamo un'importante operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di stazione di lavoro o di un server.

L'attività di back-up è un aspetto fondamentale della gestione di un sistema informativo: in caso di guasti o manomissioni, ci consente infatti di recuperare i dati dell'utente o degli utenti che utilizzano la postazione; in caso di server o di database, questo recupero può essere essenziale per il lavoro di molte persone.

Il tipo di back-up da utilizzare e la relativa periodicità sono solitamente regolati da una apposita procedura aziendale. Spesso esistono delle procedure automatiche (soggette a verifica periodica) e altre procedure che comportano un intervento manuale.

La progressiva discesa del costo delle memorie informatiche, in base alla *legge di Moore*, pone in secondo piano l'esigenza di ridurre lo spazio richiesto dai back-up, comprimendo i dati; diversamente, può essere una opportunità per aumentare la frequenza delle copie.

Per le aziende, il dato critico è la velocità di back-up, che deve permettere di completare le copie dei dati in notturna, in modo che questa attività non vada a sovrapporsi con l'operatività quotidiana, caricando i sistemi informatici e rallentando i tempi di risposta agli utenti.

Per implementare efficacemente un sistema di back-up bisogna valutare ed effettuare scelte coerenti rispetto ai seguenti elementi:

- scelta del programma e del supporto su cui effettuare il back-up
- selezione dei dati di cui effettuare il back-up
- scelta della periodicità con cui effettuare il back-up

In merito alla scelta del programma si può rilevare che alcune delle principali funzionalità che un programma di back-up dovrebbe fornire, sono:

- Copia immagine di un disco rigido;
- Copia selettiva di directory e singoli file;
- Criteri di selezione per la ricerca dei contenuti backuppati e per la scelta di quelli che devono essere oggetto di back-up (per data, tipo di file, autore della modifica);

- Compressione dei contenuti per ridurre i Gigabyte di memoria richiesti, e per aumentare le velocità di back-up e di *restoring* dei dati;
- Sicurezza: protezione delle copie con password e crittografia.

Oltre al back up completo che copia tutti i file selezionati, vi è il back up differenziale ed il back up incrementale

Il back-up differenziale è un backup cumulativo di tutti i cambiamenti effettuati a partire dall'ultimo back-up completo (o *full backup*). Il vantaggio è il minor tempo necessario rispetto ad un back-up completo. Lo svantaggio è che i dati da salvare aumentano per ogni giorno trascorso dall'ultimo back-up.

Il back-up incrementale è un back-up che contiene tutti i file cambiati dall'ultimo back-up (completo e incrementale). Il backup incrementale è più rapido di quello differenziale ma richiede tempi di *restore* più lunghi poiché è necessario partire dall'ultimo back-up completo e poi aggiungere in sequenza tutti i back-up incrementali.

E' poi essenziale conoscere quali siano i dati di cui effettuare le copie, ma non solo. E' infatti strategico, per affrontare una situazione di "disastro", essere in grado di riprodurre lo stato dei sistemi informativi, cioè dei programmi che sono in uso per interpretare i dati e rendere nuovamente funzionante l'intero sistema informativo e cioè le macchine,il sistema operativo, i programmi ed i dati (previsione di un DRP - *Disaster Recovery Plan*). E' perciò necessario effettuare delle copie anche dei programmi al loro stato di funzionalità, generalmente con dei *disck image*.

A seconda del grado di sviluppo della rete, i dati possono essere ordinatamente archiviati in un solo server oppure sparsi un po' su tutte le risorse della rete. Comunque in entrambi i casi è necessario analizzare il proprio sistema informativo per selezionare i files da sottoporre a back-up.
Ovviamente se i dati sono sparsi sarà necessario o implementare processi per ogni risorsa oppure condividere correttamente le risorse in modo da accentrare il processo di back-up.

Un'altra considerazione da fare è sulla periodicità con cui effettuare le copie. Necessario frequentemente per i dati che cambiano frequentemente, con una cadenza più ampia per lo stato dei sistemi o i dati meno strategici.
Per stabilire la periodicità con cui effettuare le copie ed il numero di supporti su cui effettuare le copie, tenuto conto delle risorse economiche a disposizione, è opportuno valutare da quale rischio ci si voglia proteggere. Diverso è infatti voler avere sempre una copia aggiornata dei dati per poter ripristinare un sistema allo stato attuale oppure disporre di più copie, anche lontane nel tempo che mi permettano di ripristinare un file così come era precedentemente.
Per esempio se si dispone di un solo supporto e si fa una copia giornaliera si ha tempo

solo un giorno per accorgersi che un file è stato magari accidentalmente danneggiato se sullo stesso supporto si effettuano copie settimanale si ha invece una settimana di tempo, perdendo però ovviamente le altre modifiche buone effettuate nel frattempo.

E' opportuno che siano presenti più supporti su cui effettuare le copie al fine di poter disporre di un più ampio spettro di supporti da cui effettuare il *restore* che copra anche un orizzonte temporale più lungo. Per esempio se si disponesse di 5 supporti su nastro su cui effettuare i back-up, si potrebbero dedicare una cassetta o CD per ogni giorno lavorativo della settimana da lunedì a venerdì ed effettuare giornalmente un back-up. In questo modo si potrebbe coprire uno spazio temporale all'indietro di massimo una settimana.
Se invece si dedicassero sempre le stesse 5 cassette o CD uno per il venerdì su cui effettuare una copia ogni venerdì e le altre prima, seconda, terza e quarta settimana del mese su cui effettuare un back-up a metà settimana, in questo modo, pur avendo sempre una copia settimanale aggiornata, si potrebbe coprire uno spazio temporale all'indietro di un mese, pur avendo sempre utilizzato 5 supporti.

E' poi fondamentale che il responsabile della sicurezza sia tenuto ad effettuare periodicamente i controlli su buon esito delle procedure di backup ed effettui delle verifiche di ripristino dei dati. E'anche opportuno annotare i controlli periodici e gli interventi sui sistemi.

Infine i supporti devono essere periodicamente sostituiti.

La conservazione dei supporti di backup in posizioni fisicamente distinte e separate dai sistemi in uso è strettamente necessaria, per evitare che in caso di furto, incendio, alluvione o altro evento catastrofico, le copie vadano perse insieme agli originali.

E'inutile sottolineare come tutte le attività di backup possono essere pianificate e fatte funzionare in automatico dal sistema informatico stesso.

I supporti su cui effettuare i back-up

I supporti su cui effettuare correttamente i back-up devono essere dei supporti sicuri ed inalterabili come i CD-R, CD riscrivibili, DVD-R, DVD riscrivibili, Digital Audio Tape, cartucce a nastro, proprio perché il supporto su cui si affidano le copie di sicurezza deve essere esente dai possibili rischi di rottura.

Appurato però che le copie sicure devono essere effettuate sui supporti descritti sopra, può essere utile aumentare il numero di copie effettuate ed effettuarle su altri tipi di supporto connessi direttamente alla rete decisamente più veloci nelle operazioni di scrittura e lettura ma anche con una più alta probabilità di rottura o rischio di accesso fraudolento.

Ora che il costo dell'hardware ha reso accessibile a prezzi molto ridotti tecnologie che fino a qualche anno fa erano molto costose, sicuramente l' acquisto di un NAS di rete è una soluzione ora più economica.

Il NAS di rete non è altro che un disco fisso (per lo più in *mirroring* ovvero *due* dischi fissi in un unico chassis che viaggiano in modo perfettamente sincronizzato e speculare tra di loro) dotato di quel minimo di sistema operativo tale da consentirgli di essere collegato direttamente alla rete senza bisogno di essere a sua volta collegato ad un personal computer.

Questo disco è condiviso dagli utenti secondo regole di autenticazione stabilite dall' amministratore della rete (che, quindi, volendo, potrebbe assegnare a ciascun utente una specifica cartella senza dare all'utente stesso accesso alle altre cartelle), e può accogliere le copie quotidiane dei dati provenienti da ogni macchina connessa alla rete stessa. Il fatto di essere collegato alla rete in modo diretto non solo consente un risparmio in termini economici, ma soprattutto consente di poter accedere alla piena velocità di rete, quindi 100 Megabit teorici, e di essere, quindi, estremamente veloce.

I limiti di questa soluzione: se il vantaggio del disco NAS è quello dell'innegabile velocità e sicurezza nella trascrizione dei dati, tuttavia esso presenta il limite che, essendo connesso fisicamente alla rete, in caso di disastro (incendio o principio di incendio, crollo di muri, furti, ecc) il disco subirà la medesima sorte del resto della nostra rete e quindi potrebbe venire, a sua volta, danneggiato o distrutto.

In termini di sicurezza potrebbe quindi essere utile pensare ad un dispositivo che possa essere capiente - sono quindi escluse le chiavette USB che hanno ancora evidenti limiti di capienza, lentezza e sicurezza hardware - ma al tempo stesso che sia removibile.

Due sono le possibilità più immediate:

a) Il disco fisso removibile.
   Il disco fisso removibile è un disco fisso di piccole dimensioni collegato direttamente alla porta USB senza necessità di alimentazione: un solo cavetto porta, infatti, sia i dati sia l'alimentazione. Il disco viene alternato ad un suo gemello. In pratica ogni mattina si

scollega uno dei due dischi e lo si ripone in borsa sostituendolo con un altro analogo. Anche questi dischi fissi hanno un costo orami molto modesto, nell'ordine di poche decine di euro, e non occupano più spazio di un moderno telefonino multimediale. Il fatto di essere riposto in un luogo fisicamente distante dal resto della rete rendono questa soluzione, pur molto economica, comunque molto efficace in termini di sicurezza.

b) Spazio web virtuale.

Grazie alle connessioni internet sempre più veloci è possibile usufruire di spazi protetti ed inaccessibili a terzi su Internet nei quali andare a riversare i nostri dati. Lo svantaggio di un maggior tempo necessario per il salvataggio pur in presenza della compressione dei dati, è ampiamente compensato dalla quasi assoluta certezza di poter rientrare in possesso dei nostri dati anche di fronte al peggiore degli eventi: i server di queste società, oltre ad essere dislocati a migliaia di chilometri di distanza, sono collocati in stanze di sicurezza ad alto livello di protezione fisica e spesso collegate a loro volta tra di loro in sistemi di *copia sicura* distanti tra di loro anche molte migliaia di chilometri.

Potrebbe sembrare una soluzione avveniristica a prima vista, ma in realtà questo tipo di salvataggio non solo è già attivo da diverso tempo ma ha anche già costi bassissimi: si parla, infatti, di poche decine di euro per disporre di uno spazio riservato e personale di 150 Gigabytes sul quale riversare i dati.

A volte il vero problema delle copie non sta tanto nella volontà di farle, ma nel fatto che esse richiedono tempo, quindi la copia viene per lo più procrastinata; paradossalmente questo accade proprio nei periodi di più intenso impegno di studio, essendo assai facile che non si riesca materialmente a fermare i lavori di tutti gli operatori per il tempo necessario all'esecuzione delle copie e questo avviene proprio in un periodo in cui la sicurezza dei dati diventa ancor più critica.

In questo caso può essere molto utile, utilizzando le funzioni presenti in Windows, programmare l' esecuzione di copie in modo del tutto automatico in orari in cui non interferiscano con il lavoro di studio.

Come creare copie di back-up in automatico

Per automatizzare il processo di copia, a parte l'utilizzare specifici programmi di backup (non mancano quelli gratuiti o comunque a costo molto basso) è possibile creare una semplice procedura che va a copiare ciò che riteniamo importante salvare sul disco remoto e poi fare in modo che questa piccola procedura venga eseguita dal sistema senza bisogno di alcun ulteriore intervento da parte nostra.

Le fasi sono due:

a) creare la procedura di copia
b) fare in modo che venga eseguita in modo automatico

a) **La creazione del file di copia**

La creazione di una procedura "*batch*" non presenta particolari difficoltà, soprattutto per coloro che hanno lavorato, al tempo, con quel vecchio DOS, che la Microsoft non ha mai completamente abbandonato proprio perché offriva caratteristiche operative particolarmente versatili che Windows non è mai riuscito ad implementare.

In un punto noto del disco fisso (ed esempio c:\ ) andiamo a creare con il WordPad un file di testo che denomineremo SALVA.BAT

Questo comando *batch* non fa altro che indicare al computer, riga dopo riga, quale cartella copiare con le relative sottocartelle, e dove copiarla (nell'esempio la copia avviene su di un disco G: nella cartella \COPIE), con l' aggiunta di alcuni *switch* (/S/E/R, eccetera) che consentono di ottimizzare questa copia.

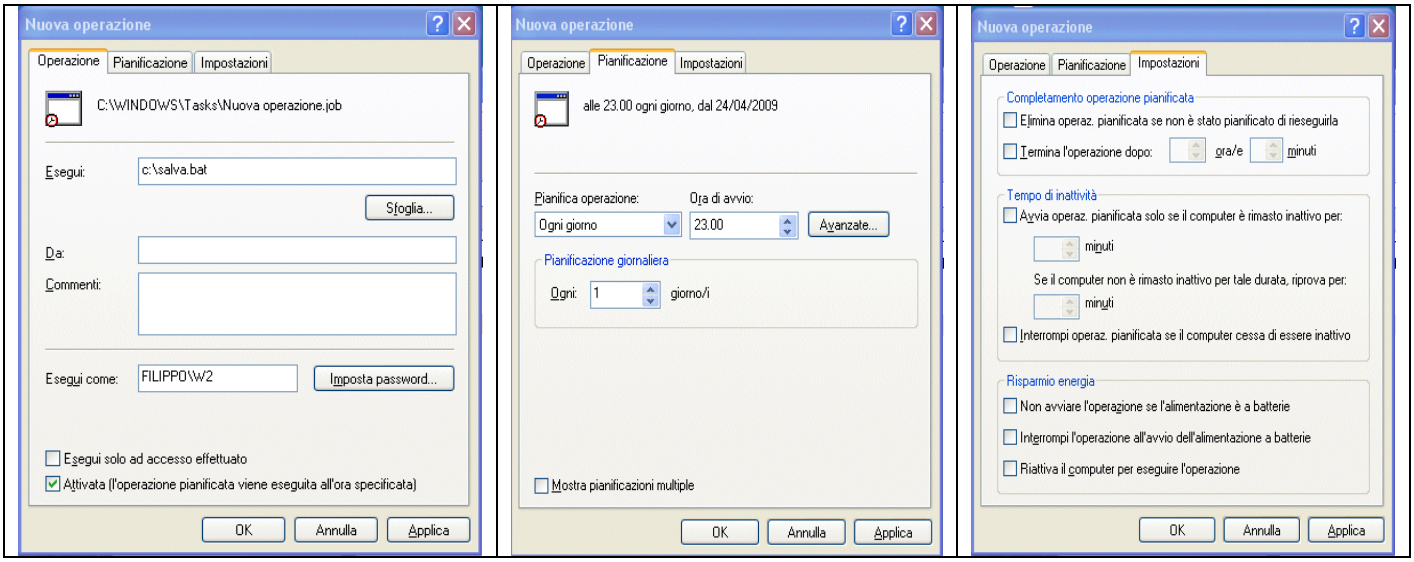
Al termine dell'esecuzione un comando (*echo*) non fa altro che visualizzare un testo e bloccare l'esecuzione del file batch (*pause*) in modo che l'operatore possa verificare la correttezza dello svolgersi delle operazioni eseguite nelle righe precedenti prima di chiudere il tutto.

Infine il comando "*dir d:*. >G:\copie\quando.txt*" non ha altra funzione se non quella di creare un file di testo con un contenuto qualsiasi il cui scopo reale è quello di memorizzare la data e l'ora in cui viene creato: sarà quello il nostro promemoria dell'ultima data di esecuzione della copia.

b) Automatizzazione dell'esecuzione

Creato il file *batch* che fa eseguire al computer una serie di comandi in sequenza, oltre che eseguirlo in modo diretto manuale, è possibile fare in modo che il computer vada ad eseguire questo comando in modo del tutto automatizzato secondo un calendario prefissato.

Questo avviene utilizzando il comando "OPERAZIONI PIANIFICATE" presente nel PANNELO DI CONTROLLO di Windows. Qui di seguito le impostazioni che consentono di eseguire automaticamente il comando usato come esempio, ovvero C:\SALVA.BAT , ogni giorno alle ore 23.



La procedura si attiverà quindi in modo del tutto trasparente per l'utente alle ore 23 di ogni giorno. Tra i vari comandi disponibili (Avanzate….) vi è anche, volendo, l'opzione relativa allo spegnimento del computer ad operazione conclusa, ma è opinione condivisa tra tutti gli esperti di informatica che i personal computer vadano spenti il meno possibile essendo stati concepiti per l'utilizzo continuativo.

ALCUNE SOLUZIONI AVANZATE

La sicurezza dei dati oltre che riguardare eventi disastrosi o di rottura delle macchine, dovrebbe preservare anche l'accidentale perdita di dati danneggiati o modificati in buona fede da un operatore.

Per affrontare questo problema di sicurezza, se si dispone di un Sistema Operativo Microsoft Windows si può utilizzare Shadow Copy (chiamata anche Volume Snapshot Service o VSS, o Previous Versions/Versioni Precedenti in Windows Vista) una caratteristica introdotta con Windows XP SP1, Windows Server 2003 e disponibile in tutte le versioni successive.
Shadow Copy permette, per le risorse condivise in rete da un Windows Server 2003 la creazione manuale o automatica di copie di backup di un file, di una cartella o di uno specifico volume ad un dato momento di tempo e, se si dispone di spazio disponibile riesce a tenere copie dei file come erano prima degli aggiornamenti successivi.

Se la criticità dei dati da preservare fosse molto alta e pertanto fosse giustificabile un elevato investimento (o si avessero già a disposizioni due LAN a distanza e connesse

da una connessione dedicata o da VPN) si potrebbe pensare alla implementazione di un sistema di replica, sincrona asincrona o mista, dei dati e delle configurazioni.

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.

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 50 km e i 150 km.
Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre allora spesso alla tecnica di copia asincrona. 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.
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*.
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 (distanza< 100 km) e una copia asincrona su un sito a grande distanza.

Come abbiamo già commentato sono da considerare elementi critici di un sistema informativo non solo i dati ma anche le configurazioni delle macchine, pertanto è opportuno stabilire delle procedure per effettuare copie della configurazioni delle macchine ritenute sensibili, per esempio i server o particolare PC su cui siano installati programmi delicati.

Per ovviare a questo problema, ed ai costi necessari alla reinstallazione di una macchina può essere utile pensare alla virtualizzazione, cioè alla replica su immagine di un intera macchina da far partire poi su di una altra macchina anche più potente.

Per virtualizzazione si intende la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. Qualunque risorsa hardware o software può essere virtualizzata: sistemi operativi, server, memoria, spazio disco, sottosistemi. Un tipico esempio di virtualizzazione è la divisione di un disco fisso in partizioni logiche.

In origine, il termine *virtual machine* veniva usato per indicare la creazione di una molteplicità di ambienti di esecuzione identici in un unico computer, ciascuno con il proprio sistema operativo. Lo scopo di questa tecnica era quello di dividere tra più utenti l'uso di un singolo computer dando ad ognuno l'impressione di esserne gli unici utilizzatori, oltre ad avere vantaggi che le macchine reali non hanno.

E’ da considerare poi che la virtualizzazione è già presente a nostra insaputa su tutte le nostre macchine che fanno uso dei programmi Java della *Sun Microsystem*. I programmi scritti in Java vengono infatti compilati (cioè tradotti) nel linguaggio *bytecode*, che gira sulla *Java Virtual Machine*.