Prevenzione di problemi e loro soluzione.
Introduzione

Scopo di questa sezione è introdurre alcune delle metodiche e delle tecnologie che consentono di attuare politiche, efficaci e lineari, di prevenzione dei guasti. Un approccio globale alla protezione dei dati e delle risorse deve essere basato principalmente su politiche di tipo proattivo, ovvero su attività di prevenzione che mirano a ridurre al minimo le **vulnerabilità** del sistema. Alle politiche proattive devono poi essere associate attività di tipo reattivo, che consentano, in caso di danno ormai verificato, di ripristinare il corretto funzionamento del sistema.

In generale, è obiettivo dell'amministratore e del responsabile dei sistemi evitare qualunque minaccia, ovvero qualunque evento o entità che possa danneggiare il sistema compromettendo i dati o i servizi critici. Esistono numerose categorie di minacce, che vanno dagli eventi catastrofici, naturali e non (incendi, terremoti, alluvioni), agli incidenti che coinvolgono le infrastrutture, casuali o intenzionali (taglio di cavi, sospensione dell'erogazione di corrente), ai veri e propri attacchi alla **sicurezza del sistema**.

La valutazione generale dei danni va fatta tenendo in considerazione diversi aspetti:

- gli aspetti tecnici e le tecnologie di supporto alla prevenzione;
- gli aspetti organizzativi, ovvero la definizione di ruoli e procedure che specifichino aree d'azione, limiti e responsabilità, anche attraverso opportune attività di formazione del personale;
- gli aspetti economici e legali.

In questa breve trattazione introdurremo alcuni degli aspetti tecnici, trattando le principali tecniche e procedure per la prevenzione dei problemi e la loro soluzione. È disponibile un approfondimento sulla **sicurezza come forma di prevenzione**, che tratta in modo più specifico le problematiche relative alla sicurezza delle informazioni.

Multiutenza

La protezione dei dati e delle risorse inizia con una fase di definizione dei ruoli in cui a ogni utente sono associati un insieme di criteri di accesso. Il sistema operativo che viene utilizzato deve quindi consentire di definire a quali risorse può accedere ogni utente, proteggendo le altre risorse da eventuali accessi non autorizzati. Deve inoltre offrire un meccanismo di identificazione, tipicamente attraverso uno **username** e una **password**, che consenta di verificare l'identità degli utenti. Ogni persona che vuole accedere alle risorse del sistema deve farsi riconoscere come utente noto e lo fa specificando l'identificativo (*username*) con cui il sistema lo individua. Deve inoltre fornire la *password* privata associata allo *username*, in modo che il sistema possa verificare la sua identità.

In presenza di ambienti con molti utenti che hanno ruoli differenziati è dunque essenziale optare per sistemi operativi che offrano supporti al controllo degli accessi e all'implementazione di politiche di accesso articolate. Indispensabile è definire a priori quali sono i criteri di accesso alle risorse da parte degli utenti. Sistemi operativi e applicazioni a uso personale, che non prevedano politiche di accesso ai *file* e alle risorse, ma consentano a tutti gli utenti l'accesso a tutte le risorse (quali per esempio *Microsoft Windows98*), rendono impossibile la realizzazione di politiche di protezione e prevenzione significative.

In presenza di utenti che condividono risorse e attività è opportuno definire a priori un insieme di politiche di accesso a postazioni, *file*, stampanti, eccetera, che consenta all'amministratore di semplificare le diverse fasi della gestione. I sistemi operativi multiutente permettono di definire politiche molto articolate, sfruttando come meccanismo base quello dei **gruppi**. Ogni gruppo viene associato alle proprie politiche di accesso alle risorse ed ogni utente viene poi inserito in uno o più

gruppi. In questo modo, quando ad un gruppo vengono estesi o ridotti i permessi, la modifica viene applicata automaticamente a ogni utente che ne fa parte.

Backup

Si intende in modo generale con **backup** una copia dei dati destinata all'archiviazione che può essere utilizzata in caso di errore per ripristinare uno stato precedente. Le cause di un errore possono essere innumerevoli, ma sono tipicamente riconducibili a due tipologie:

- l'errore prodotto dal ***software***, che può essere causato da un intervento sbagliato dell'amministratore o dell'utente (per esempio una cancellazione irreversibile di *file*), oppure può essere determinato da un malfunzionamento del *software* (anche provocato da un **virus** o da altri tipi di **attacco** alla **sicurezza del sistema**);
- l'errore prodotto dall'***hardware***, che può essere dovuto a un malfunzionamento intrinseco di supporti e componenti (per esempio un disco fisso che si rompe) o causato da eventi esterni che provocano danni all'*hardware* (compresi fenomeni naturali, come un allagamento o un fulmine).

In tutti questi casi le informazioni (o una loro parte) risultano inutilizzabili e per ripristinare lo stato precedente all'errore è necessaria una copia dei dati che sono stati compromessi. L'operazione di ripristino è detta **restore**.

Perché il ripristino sia effettivo occorre che la copia di *backup* dei dati sia recente. Più tempo intercorre tra il momento in cui è stato effettuato il *backup* e il momento in cui si verifica l'errore, più gravi saranno gli effetti di quest'ultimo. Per questo motivo è importante pianificare un'attività di *backup* regolare che preveda periodicamente, a scadenze fisse, il *backup* generale dei dati e giornalmente il *backup* dei dati critici. Sono disponibili sistemi che consentono di automatizzare la procedura di *backup* e di avviarla automaticamente quando le risorse sono parzialmente o completamente inutilizzate (per esempio di notte) e sistemi che permettono di centralizzare il *backup* di più macchine in rete.

Tipi di backup

Le procedure di **backup** dipendono dal sistema operativo utilizzato, ma, generalmente, è prevista la possibilità di fare *backup* solo dei dati (per esempio della posta elettronica o dei *file* degli utenti), oppure di fare *backup* anche del sistema e delle applicazioni. In questo caso si mantiene copia anche dei *file* di configurazione e dei *file* di sistema, in modo da intervenire sempre esclusivamente con un *restore*. Quest'ultima opzione non sempre è consigliabile poiché esistono diverse occasioni (un esempio tipico è quando l'errore è causato da un attacco alla sicurezza) in cui può essere opportuno reinstallare il sistema operativo.

Il *backup* dei dati è tipicamente una operazione lunga, a causa della grande mole delle informazioni da copiare e della relativa velocità dei **supporti di backup**. Per questo motivo non viene sempre effettuato un *backup* completo dei dati, ma vengono a volte utilizzate metodologie di stratificazione delle copie che consentono di effettuare salvataggi parziali. In generale si parla di:

- **backup completo**: quando i dati vengono copiati interamente (dal supporto originale al *backup*) e per ripristinarli occorre semplicemente effettuare la copia in senso inverso (dal *backup* al supporto originale). Questo tipo di *backup* è consigliabile quando i dati cambiano molto frequentemente, ma risulta inutilmente lento se i dati sono sostanzialmente stabili e cambiano raramente;
- **backup incrementale**: vengono copiati i *file* creati o modificati dall'ultimo *backup* completo o incrementale. Qualora si faccia un successivo *backup* incrementale, questo farà comunque riferimento al precedente. La procedura di *restore* deve quindi prevedere una ricostruzione

stratificata a partire dall'ultimo *backup* completo, che passa attraverso tutti i *backup* incrementali effettuati;
- **backup differenziale**: vengono copiati i *file* creati o modificati dall'ultimo *backup* completo. Qualora si faccia un successivo *backup* differenziale, questo farà comunque riferimento al *backup* completo e non si avvarrà del *backup* differenziale precedente. La procedura di *backup* è quindi un po' più lenta rispetto al *backup* incrementale, ma è più semplice e veloce la procedura di *restore*, che prevede il recupero dell'ultimo *backup* completo e di un solo *backup* differenziale.

Supporti per il backup

Il **backup** dei dati viene fatto su supporti di memoria di massa che offrono grande capacità a basso costo (uno stesso supporto può fornire spazio per il *backup* di più dischi) e alta affidabilità (se in presenza di un errore il *backup* risultasse danneggiato, sarebbe impossibile il ripristino). La velocità è un altro fattore rilevante, meno critico rispetto a quelli citati precedentemente poiché i *backup* lunghi sono frequentemente automatizzati e quindi non risulta essere fondamentale il tempo di esecuzione.

Per tutti questi motivi i *device* dedicati al *backup* sono basati su tecnologie a nastro che hanno alta affidabilità a costi contenuti e sono relativamente veloci nell'accesso sequenziale tipico della procedura di copia. La velocità si misura in termini di *byte* trasferiti al secondo (Bps) e arriva a diversi GB all'ora. Questo tipo di *device* ha capacità molto elevate (nell'ordine delle decine di GB) ed è indicato nei sistemi medio grandi che hanno grandi quantità di dati critici di cui fare frequenti *backup*. Alternativamente possono essere utilizzate unità a cartucce magnetiche rimovibili che hanno minori capacità in termini di memorizzazione e velocità, ma sono più economiche e possono essere efficacemente usate per *backup* meno frequenti e di minori dimensioni.

In alternativa possono essere utilizzati anche supporti non dedicati al *backup*, ma che in particolari condizioni si prestano a questo tipo di attività. Per esempio, i supporti ottici (come CD e DVD, scrivibili e riscrivibili) oppure i supporti magneto-ottici possono essere usati per *backup* di dimensioni medio/piccole. Un'ulteriore alternativa è costituita da dischi fissi aggiuntivi, che possono essere inseriti in un sistema per contenere il *backup* dei dati di quel sistema o di altri. Infine, si possono usare i *floppy* per copie di *file* di pochi KB, che costituiscono una forma personale di *backup*.

Immagini dei dischi

Un meccanismo di ripristino molto efficace consiste nel memorizzare una immagine precisa del disco fisso, settore per settore, e nel riversarla su un diverso supporto di memoria di massa, per esempio un altro disco oppure un CD o un DVD. Viene quindi creata una immagine del disco assolutamente identica all'originale e, se il disco originale risulta danneggiato, è possibile ricostruire la situazione iniziale invertendo il processo di copia. Il disco così ricostruito sarà identico all'originale anche a livello fisico, garantendo il funzionamento del sistema. Questo tipo di processo viene tipicamente attuato attraverso *software* appositi che offrono supporto al *backup* e al ripristino dei dati.

Questo meccanismo può essere usato anche in quelle situazioni in cui molte macchine hanno la stessa dotazione *hardware* e *software* e dunque necessiterebbero di tante installazioni identiche. Una condizione di questo tipo si verifica spesso nei laboratori didattici che hanno frequentemente dotazioni *hardware* identiche, quantomeno per lotti, e necessitano anche di dotazioni *software* sovrapponibili per consentire di effettuare la stessa attività didattica su tutte le postazioni. In questo caso è possibile mettere in atto la procedura di installazione su di un *computer* campione, provvedendo a montare sia il sistema operativo che le applicazioni. Il disco o i dischi del *computer* campione costituiscono dunque una valida base per tutte le installazioni dei *computer* identici a

quello scelto e sono perciò candidati a diventare una immagine fisica da ricopiare poi su tutte le postazioni. Partendo dall'immagine del disco (o dei dischi) del *computer* campione è possibile quindi ottenere semplicemente tante installazioni funzionanti con una elementare attività di copia. Questa possibilità consente, a chi gestisce le macchine, di concentrarsi sulla prima installazione, risparmiare tempo sulle successive, ridurre la possibilità che si verifichino errori o si rilevino incompatibilità e infine offre supporto alle installazioni successive che dovessero rendersi opportune a causa di errori.

Due considerazioni, ovvie, introducono vincoli alla procedura appena illustrata. La prima è che, dopo la copia dell'immagine, è comunque necessaria una fase di configurazione delle singole postazioni, che ha come obiettivo quello di personalizzare le installazioni inserendo quei dati, come l'indirizzo IP o il numero di licenza del *software*, che sono diversi in ogni PC. La seconda è che il ripristino da condizioni di errore, fatto attraverso l'immagine iniziale, produce la perdita di tutti quei dati che sono salvati sul disco locale e dunque è sconsigliato qualora gli utenti non disponessero di spazio disco su *file server*.

RAID

Esistono alcune tecniche di controllo dei dischi che migliorano l'affidabilità operando in modo trasparente. La gestione dei dischi denominata **RAID** (*Redundant Array of Independent Disks*) mira a prevenire i danni e a favorire il recupero automatico dei dati. RAID indica un complesso meccanismo di memorizzazione che utilizza più dischi fissi con l'obiettivo di aumentare le prestazioni della memoria di massa in termini di velocità e/o di affidabilità. In particolare i miglioramenti di affidabilità consentono in alcuni tipi di RAID di recuperare automaticamente e in modo trasparente alcuni errori *hardware*.

Le diverse tipologie RAID combinano alcuni meccanismi base:

- lo **striping**, una tecnica di miglioramento della velocità di lettura/scrittura che consiste nello spalmare i dati di un blocco in più dischi. Il blocco viene diviso in n sottoblocchi, ognuno dei quali è memorizzato su un disco diverso e ogni lettura innesca n letture (da n dischi), riducendo il tempo di trasferimento e di latenza. Questa tecnica di per sé non incide sulla resa dei dischi poiché non inserisce informazioni di controllo.
- Il **mirroring**, in cui ogni disco viene duplicato e dunque esiste una copia di sicurezza di ogni informazione. Il *mirroring*, oltre ad aumentare l'affidabilità, consente l'uso in parallelo dei dischi in lettura. Non migliora invece le prestazioni in scrittura. Le copie vengono gestite direttamente dal sistema, per cui utente e amministratore vedono una sola istanza del *file*. Il *mirroring* prevede una ridondanza totale delle informazioni che dimezza la resa dei dischi.
- I **blocchi di parità**, che consentono di ricostruire porzioni di informazioni andate perse a causa di errori. I blocchi di parità sono blocchi utilizzati per memorizzare informazioni riassuntive (calcolate da apposite funzioni matematiche) sugli n blocchi precedenti e non possono quindi garantire ridondanza totale. Per questo motivo non recuperano da qualunque tipo di difetto, ma solo da errori circoscritti. La ridondanza incide però molto meno del *mirroring* sulla resa dei dischi poiché prevede l'inserimento di un blocco di parità ogni n blocchi dati e dunque una perdita in termini di spazio di un (n+1)-esimo.

Tipologie RAID

Combinando **striping**, **mirroring** e **blocchi di parità** si ottengono sistemi RAID differenti che offrono diversi gradi di affidabilità e l'aumento delle prestazioni in lettura/scrittura. In particolare:

- **RAID 0**: utilizza **striping** per ottenere un miglioramento di prestazioni in lettura e scrittura. È tipicamente utilizzato su dischi di uguali dimensioni in modo da non avere perdite di capacità complessiva. Se si utilizzano 5 dischi da 10 GB si riesce a usare tutti i 50 GB disponibili, che vengono visti come un unico disco, e si velocizzano le letture e le scritture di 5 volte. RAID 0

non prevede ridondanza e se si verifica un guasto su un disco vengono compromesse anche informazioni contenute in *stripe* sugli altri dischi.
- **RAID 1**: utilizza **mirroring** per aumentare l'affidabilità del sistema. Recupera da situazioni di danno totale dei dischi. Se si utilizzano 4 dischi da 10 Giga si usano effettivamente solamente 20 GB.
- **RAID 1+0**: utilizza **striping** e **mirroring** combinati nel modo seguente: i dischi vengono messi in *mirror*, ovvero metà dei dischi sono predisposti per essere copia dell'altra metà. Sono dunque visibili n/2 unità che vengono messe in *striping* per migliorare le prestazioni. È sia molto affidabile (di ogni disco in *stripe* esiste una copia ridondante) che molto veloce. Se si utilizzano 8 dischi da 10 Giga si possono velocizzare le letture e le scritture di 4 volte usando però effettivamente solo 40 GB, visti come un'unica unità.
- **RAID 5**: utilizza **striping** e **blocchi di parità** combinati per ottenere un miglioramento di prestazioni e di affidabilità. È meno affidabile rispetto a RAID 1+0, ma rende disponibile all'utente una quantità maggiore di memoria. Se sono disponibili 5 dischi da 10 GB, ne usa uno per la parità e 4 per i blocchi dati effettivi, col risultato che si usano 40 GB e si velocizzano le letture e le scritture di 4 volte. Rispetto alla soluzione con RAID 1+0 si ottengono risultati analoghi con 30 GB in meno. È tollerante rispetto al guasto di un solo disco.

Le tecniche RAID possono essere realizzate via *hardware*, utilizzando appositi *controller* che gestiscono le singole azioni di lettura e di scrittura implementando una strategia RAID, oppure via *software*, attraverso il sistema operativo, che consente di definire politiche di gestione dell'*hardware* che attuano metodiche RAID.

UPS

Gli eventi esterni che più frequentemente provocano danni ai sistemi sono quelli imputabili alle fluttuazioni nella distribuzione di energia elettrica. Si tratta in alcuni casi di interruzioni improvvise dell'erogazione di corrente (*blackout*) e in altri di sovratensioni e sottotensioni. Tutte queste tipologie di eventi possono provocare seri danni, in particolare agli alimentatori, alle *motherboard*, alle schede di rete e ai dischi.

Per ovviare a questo tipo di problema si possono dotare i sistemi più critici (per esempio i *server*) di un gruppo di continuità (in inglese *Uninterruptible Power Supply*, **UPS**), ovvero di un sistema di alimentazione che ha l'obiettivo di fornire energia anche quando non viene direttamente rifornito perché l'erogazione della rete elettrica si interrompe o è instabile.

Per offrire questo tipo di servizio l'UPS è dotato di batterie, ovvero di accumulatori di energia che forniscono corrente quando la rete non alimenta o quando fornisce energia al di fuori dei limiti di tolleranza ammessi.

Esistono fondamentalmente due tipi di UPS:

- **UPS *off line***: la componente che converte la corrente continua della batteria in quella alternata della rete normalmente è disattivata e gli apparati si alimentano direttamente dalla rete. Viene attivato solo quando manca l'alimentazione elettrica.
- **UPS *on line***, in cui la componente che converte la corrente continua della batteria in quella alternata della rete è sempre attiva e gli apparati si alimentano solo dalle batterie. Questo tipo di UPS tipicamente si occupa anche di stabilizzare l'energia elettrica ovvero di fornire un'alimentazione con tensione stabile e costante e con frequenza fissata. Rispetto agli UPS *off line* ha anche il vantaggio di non dover effettuare commutazioni nel momento del *black out* e di non introdurre dunque interruzioni nell'erogazione.

Virus

I virus fanno parte di una famiglia di attacchi alla sicurezza nota come **malicious software** (*malware*), che comprende altri tipi di programmi caratterizzati dal fatto che si diffondono da un *computer* all'altro con lo scopo di produrre danni ai sistemi.

In realtà i virus più recenti mescolano le caratteristiche di diversi tipi di *malware* con lo scopo di diventare più difficili da individuare e più efficaci nel diffondere l'infezione e in particolare spesso sono **virus** e **worm**, ovvero *software* che hanno i medesimi meccanismi riproduttivi dei virus, ma che utilizzano (come i *worm*) la rete per propagarsi. Questa caratteristica accomuna la maggior parte dei virus recenti poiché lo scambio di *file* (che è il meccanismo base per il propagarsi dell'infezione) avviene ormai prevalentemente attraverso la rete.

I virus possono essere classificati in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui propaga l'infezione e si sviluppa il virus. Sono distinguibili in questa ottica diverse tipologie di virus:

- i **boot virus**, che infettano il *Boot Sector* o il *Master Boot Record* dei dischi in modo da essere caricati all'avvio del sistema;
- i **file virus**, che infettano, con modalità molto varie, i *file* eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;
- i **macrovirus**, che sono scritti in VBA (*Visual Basic for Application*) un linguaggio per la scrittura di macro negli ambienti applicativi *Office*;
- i ***network* virus**, che si diffondono sfruttando le **vulnerabilità** dei protocolli di Internet.

Su virus e antivirus è disponibile un **approfondimento**.

Antivirus

La migliore difesa contro i virus è ovviamente la prevenzione che va affrontata sia in termini tecnologici che comportamentali. In particolare per prevenire i virus occorre:

- evitare comportamenti rischiosi, quali scambio e *download* di *file* sospetti, installazione di pacchetti non licenziati, apertura degli *attach*. Quest'ultima precauzione è molto importante per difendersi dai macrovirus poiché, se l'allegato non viene eseguito, il virus rimane latente. Aprire i messaggi di posta elettronica può diventare causa di infezione solo se il *client* di posta è impostato per eseguire gli allegati in automatico. Per questo motivo è opportuno disabilitare l'anteprima dei messaggi.
- Aggiornare il *software* in modo da ridurre le vulnerabilità al minimo. L'attacco dei virus viene infatti condotto sfruttando errori nel *software* o nei protocolli e tutte le azioni volte a ridurre il numero di errori presenti nei programmi (come per esempio l'installazione delle *patch*) sono forti forme di prevenzione dei virus.
- Utilizzare un *software* antivirus, ovvero un *software* in grado di identificare i virus e rimuoverli prima che entrino in azione. Per rilevare la presenza di un virus i *software* antivirus cercano all'interno della memoria (centrale e di massa) particolari sequenze di *byte* che costituiscono l'impronta identificativa del virus. La continua produzione di nuovi virus rende quindi indispensabile un aggiornamento continuativo del *software* antivirus per garantirne l'efficacia nel tempo. Alcune volte i *software* antivirus sono in grado di rilevare anche virus di cui non conoscono la sequenza di *byte* identificativa, riscontrando su base probabilistica comportamenti anomali o sospetti.
- Effettuare comunque un *backup* periodico dei dati, in modo da poter ripristinare efficacemente il sistema anche in caso di danni.

Le attività dei *software* antivirus rallentano le prestazioni del sistema, richiedendo continue scansioni della memoria e del disco. Per esempio, è possibile effettuare scansioni periodiche non automatiche

di tutto il *filesystem* da attivare in momenti in cui il sistema non è utilizzato. Per questo motivo alcune attività di verifica vengono attivate su richiesta.

Su virus e antivirus è disponibile un **approfondimento**.

Conclusioni

Questa sezione dell'introduzione ha offerto una panoramica molto veloce su alcune delle tecnologie che vengono utilizzate per prevenire i guasti e preservare la disponibilità delle informazioni. In particolare sono state introdotte soluzioni che offrono supporto a tipologie molto differenti di problemi, dall'attacco alla sicurezza dei dati prodotto da un virus ai danni *hardware* che possono essere conseguenza di uno sbalzo di tensione nell'erogazione della corrente elettrica. L'elenco dei problemi, così come quello delle tecnologie che supportano la prevenzione e il recupero, non vuole essere esaustivo, ma vuole invece toccare alcuni dei guasti più frequenti.

Sono stati inoltre evidenziati alcuni aspetti correlati alle tecnologie che hanno in realtà forte impatto su tematiche di tipo organizzativo, quali la gestione degli utenti o la programmazione periodica delle attività di aggiornamento del *software* o delle procedure di *backup*.

Sono disponibili approfondimenti:

- sulla **sicurezza come forma di prevenzione dei problemi** (consigliato per profilo C1)
- su **virus e antivirus**.