Protezione dei dati

Protezione dei dati

- Un hard disk contiene **dati** e **programmi**
- I dati sono **molto** più importanti dei programmi
  - Installazione di Office 2000: 0.5 ore
  - Tesi di laurea, ricerca, progetto AutoCAD: 0.5 *anni*
- 1ª legge dell'affidabilità: "tutto, prima o poi, si guasta"
- Gli hard disk si guastano con una certa frequenza
  - Guasti **fisici**
  - Guasti **logici**
- E' necessario mettere in opera delle **procedure di sicurezza** per non perdere i dati

2

Protezione dai guasti fisici (1)

- Il calcolatore preleva tensione **alternata** dalla rete.
- I circuiti del calcolatore hanno bisogno di tensione **continua**.
- La conversione viene fatta dall'alimentatore
  - Gli sbalzi di tensione sulla rete possono essere risentiti dai circuiti del calcolatore
- Ciò porta a
  - malfunzionamenti (quasi sempre)
  - danni all'hardware (più raramente)

3

Protezione dai guasti fisici (2)

- E' buona norma affiancare ad un calcolatore un UPS (*uninterruptable power source*, gruppo di continuità), tramite il quale:
  - Si filtrano eventuali oscillazioni della tensione di rete
  - Si mantiene una tensione in ingresso al calcolatore anche in caso di black out (per un tempo limitato ma sufficiente al salvataggio dei dati)
  - Si prevengono guasti all'hardware
- Costo di un UPS: ~150 euro
  - Costo di un HD nuovo: ~150 euro

4

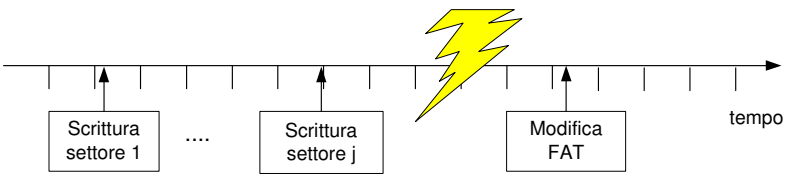
Protezione dai guasti fisici (3)

- Il pulsante di accensione del calcolatore serve **soltanto** per accenderlo (quando si incomincia a lavorare) e spegnerlo (quando si è finito), **non** per "resettare" il calcolatore
  - E' **pericoloso** (per il vostro hardware) cambiare repentinamente lo stato della tensione (e.g., spegnere e riaccendere con due pressioni ravvicinate)
  - Si può danneggiare e rendere inservibile l'hardware
  - Dopo che si è spento un calcolatore (ed un qualunque altro dispositivo elettronico), è bene contare fino a 10 prima di riaccenderlo

5

Guasti logici

- Esempio: salvataggio di un *nuovo* file sul disco
  - Scrittura del contenuto del file in un certo numero di settori
  - Aggiunta di una riga nella tabella di allocazione dei file



6

Protezione dai guasti logici

- Dato un disco di capacità C, è possibile *partizionarlo* in un certo numero di *dischi virtuali*, di capacità inferiore
- Questa operazione va fatta **prima** di installare qualunque cosa sul disco (è distruttiva del contenuto dei dischi, e non reversibile)
- Il sistema operativo vedrà non **un** disco, ma **più** dischi *virtuali* (sempre a parità di capacità totale)
- Ciascun disco virtuale può essere formattato in modo indipendente

7

Protezione dai guasti logici (2)

- Perché partizionare un disco?
  - Se si divide un disco in 2 partizioni, in una si possono mettere il sistema operativo ed i programmi e nell'altra i dati personali
- In tal modo, se ho bisogno di formattare (ad esempio per cambiare il sistema operativo), la partizione dei dati rimane intatta
- Se c'è qualche guasto *logico* che rende inaccessibile la partizione dei programmi, i dati sull'altra partizione possono essere ancora recuperati

8

Backup

- Il miglior modo per proteggere i dati è quello di farne **copie di riserva** (backup) **da qualche altra parte**
- Il backup deve essere
  - **Periodico**
  - Eseguito su media **affidabili**
    - CD-R, DVD-R, etc. **Evitare i floppy disk**
  - Tale da consentire il trasporto dei dati su un altro computer in modo agevole
  - (Possibilmente) incrementale
- **Ridondanza** dell'informazione come mezzo per ottenere affidabilità

9

Virus

- I guasti fisici e logici del disco non sono l'unico problema
- Esistono **programmi** concepiti allo scopo di menomare le funzionalità di un calcolatore
- Tali programmi prendono il nome di **virus**, per la sorprendente analogia con il fenomeno biologico

10

Virus (2)

Biologico		Informatico
– Ha bisogno di cellule per riprodursi	⟺	– Ha bisogno di programmi per riprodursi
– Inietta il proprio DNA nel nucleo di cellule sane	⟺	– Inserisce il proprio codice nei programmi
– Le cellule infette diventano veicoli di diffusione del virus	⟺	– I programmi infetti diventano veicoli di diffusione del virus

11

Come agisce un virus

- Fase 1: *Infezione*
  - Un virus si "attacca" ad un programma
  - Quando l'utente esegue il programma infetto, il virus va in esecuzione **prima** del programma
  - Il virus si copia in memoria, e si *replica* in tutti i programmi che vanno in esecuzione
  - I programmi (anche quelli infetti) passano di mano in mano, o peggio ancora, viaggiano in rete…
  - A volte, un virus si copia nel **boot sector**
    - In tal modo, va in esecuzione automaticamente ogni volta che il computer viene acceso
    - La maggior parte dei computer consente di **proteggere** da scrittura il boot sector

12

Come agisce un virus (2)

- Fase 2: *attacco*
  - Al verificarsi di una particolare condizione (e.g. data, n. di repliche, etc.), un virus può lanciare un *attacco,* ad esempio:
    - Cancellare files
    - Formattare dischi
    - Occupare risorse (e.g., memoria, disco, CPU)
    - Spegnere il computer ogni 5 minuti
    - Inondare un server di rete di richieste di servizio, mandando in tilt tutta la rete
    - Spedire e-mail a nome vostro

13

Come si prende un virus

- Un virus si prende **mandando in esecuzione del codice**.
- Si può trovare del codice in:
  - File eseguibili (.exe, .com, .bat, .vbs, .sys)
  - **Documenti** scritti con Office
- Si può mandare in esecuzione del codice
  - Aprendo allegati di posta elettronica
  - Cliccando su collegamenti di pagine web
  - Aprendo documenti Office
- Se non siete sicuri della provenienza di un file, non apritelo

14

Macro Virus

- I documenti di Office (.doc, .xls, .mdb, .ppt, .dot etc.) possono contenere **macro** scritte in Visual Basic
- Una macro è una sequenza di istruzioni in un linguaggio ad alto livello, che può servire (ad esempio) ad automatizzare compiti ripetitivi
- Le macro vanno in esecuzione **automaticamente** all'apertura di un documento Office
- E' possibile disabilitare l'esecuzione automatica delle macro
  - Strumenti -> Macro –> Protezione

15

Worms

- Un **worm** è un virus che si diffonde sfruttando errori di programmazione nei sistemi operativi e nelle applicazioni
- se un calcolatore è connesso alla rete, è possibile che qualcuno sfrutti delle "falle" del sistema operativo o di un'applicazione per eseguire del codice sul vostro calcolatore
- Esempio: worm **sasser**
  - Nel 2004 ha infestato mezzo mondo
  - Si prende sfruttando una vulnerabilità dei sistemi Windows
  - Non c'è bisogno di far niente, basta essere attaccati ad Internet

16

Trojan Horses

- I trojan horses sono programmi che “dicono” di fare una cosa (buona) e ne fanno *anche* un’altra (dannosa)
  - giochi fatti in flash, scaricabili dalla rete
  - “novità assolute ed entusiasmanti” su siti di dubbia fama o su reti peer-to-peer
- Evitate di mandare in esecuzione programmi dei quali non siete in grado di verificare l’origine

17

E-mail Virus

- Sono virus che si diffondono per posta elettronica
- Di norma, sfruttano programmi MS (Outlook, Outlook Express), perché sono più diffusi
- I programmi di posta contengono un indirizzario (“contatti”)
- Questi virus confezionano e spediscono messaggi di posta – contenenti allegati infetti – agli indirizzi contenuti nell’indirizzario
- Molto spesso, si camuffano inserendo informazioni plausibili nel campo “mittente”, “oggetto” e nel testo del messaggio
- Altre volte spediscono a terzi lettere che si trovano nella casella di posta

18

Antivirus

- Programma che, una volta installato, **sorveglia** il calcolatore (es. Norton 200X)
  - Esaminano qualunque cosa venga copiata o mandata in esecuzione sul calcolatore
  - Se trovano del codice “poco limpido”, ne impediscono l’esecuzione
- Un antivirus rallenta (spesso tangibilmente) le prestazioni del sistema
- Deve essere continuamente aggiornato, perché *quotidianamente* appaiono nuovi virus

19

Come funziona un antivirus (1)

- Fase 1: scansione
  - Ogni virus ha la propria “sequenza di DNA”
  - Un antivirus ha una base di dati contenente tutte le sequenze di DNA note
  - Il programma esamina i file per vedere se contengono sequenze di DNA virale
  - Esistono tecniche sofisticate per rendere efficiente questa operazione
  - Aggiornare l’antivirus significa aggiungere nuovi record alla base di dati

20

Come funziona un antivirus (2)

- Fase 2: riparazione
  - Se viene trovato un file “infetto”, si intraprende una qualche azione
    - Lo si cancella
    - Lo si mette “in quarantena” (se ne vieta l’esecuzione)
    - Si cerca di ripristinare il file originale (difficile)
- Un antivirus rimuove le infezioni, **non** i danni causati delle infezioni

21

Aggiornamento dei sistemi operativi

- Un antivirus può fare molte cose, ma non può tappare le falle dei sistemi operativi
- Può dirvi se avete un worm (ed eventualmente rimuoverlo), ma difficilmente può impedirvi di prenderlo
- Per questo, ci sono le case che distribuiscono i sistemi operativi, che periodicamente mettono a disposizione delle **patch** (toppe) che chiudono qualche falla
- E’ **molto importante** tenere aggiornato il sistema, con cadenza simile a quella con la quale si aggiorna l’antivirus

22

Hoax

- Un **hoax** (*scherzo*) e' un messaggio allarmante, che arriva per mail, contenente informazioni su fantomatici attacchi virali informatici
- Di norma, contiene anche contromisure da prendere per non essere vulnerabili a tali attacchi (per esempio, cancellare un particolare file sul disco)
- Quasi sempre, il tono del messaggio e' tale per cui chi lo riceve si sente in dovere di rimandarlo a tutte le persone che conosce (a volte il messaggio lo richiede esplicitamente)

23

Hoax - Esempio

Verificare se avete, nel vostro PC, il virus: jdbgmgr.exe. Per favore controllate se avete questo virus, a me l'hanno passato, e di lui si conosce soltanto che s'inserisce e si nasconde nella rubrica d'indirizzi.

E' molto probabile che sia già nascosto nel Vs. computer.

Il virus si chiama jdbgmgr.exe e si trasmette automaticamente tramite Messenger ed anche attraverso la Rubrica degli Indirizzi.

Il virus NON è deletabile per McAfee o Norton e rimane in letargo durante 14 giorni prima di recare danni all'intero sistema.

Può essere cancellato prima che possa eliminare le rubriche e /o archivi del computer; per poterlo eliminare bisogna eseguire le seguenti operazioni:

1. Iniziare, cliccando sullo schermo in basso a sinistra "Avvio o Start"
2. Cliccare su "Trova" o "Cerca", andare da "Files o Cartelle" e scrivere il nome(del virus): jdbgmgr.exe
3. Assicurarsi che dovrà cercare sul disco "C"
4. Cliccare su "Cerca ora"

24

Hoax – Esempio (2)

5. Se appare il virus (l'icona è un orsacchiotto) che corrisponde al nome di jdbgmgr.exe NON APRIRE PER NESSUN MOTIVO.
6. Cliccare sul pulsante destro del vostro Mouse ed ELIMINARE (andrà sul vostro cestino)
7. Andare poi al vostro Cestino e Cancellare definitivamente o svuotare il cestino.

SE AVETE TROVATO IL VIRUS NEL VOSTRO COMPUTER, INVIARE QUESTO MESSAGGIO A TUTTE LE PERSONE CHE SI TROVANO SULLA VOSTRA RUBRICA D'INDIRIZZI O E-MAILS, PRIMA CHE POSSA ATTIVARSI E CAUSARE DANNI A QUESTE PERSONE.

25

Hoax – come difendersi

- Usare il **cervello**
  - Verificare l'attendibilita' delle informazioni ricevute
  - Esistono siti dedicati a smascherare finti allarmi (e.g., hoaxbusters.ciac.org, ma anche I siti dei distributori di antivirus commerciali)
- Se abboccate
  - danneggiate il vostro sistema
  - diffondete l'infezione a molte persone
- Il virus siete **voi**

26

In ultima analisi…

- Esistono strumenti di protezione da virus molto efficienti
- Nessuno di questi garantisce l'immunità se chi usa il computer abbocca ad ogni amo
  - "I cretini sono sempre piu' furbi delle precauzioni che si prendono per impedir loro di nuocere", legge di Murphy

27