

Altre misure di sicurezza

Prevenzione dei danni e backup

Ombretta Pinazza

Altre misure di sicurezza

Prevenzione dei danni e backup :

- Strumenti di protezione hardware
- Sistemi anti intrusione
- Backup: supporti e operazioni
- La conoscenza del proprio PC
- Domande e Risposte

Strumenti di protezione HW: i server

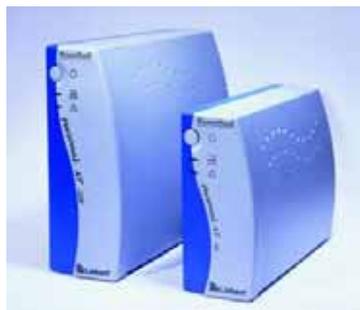
Localizzazione ed accesso ai server

- Ambienti protetti
 - sistemi di condizionamento
 - sistemi antincendio
 - sistemi che garantiscano la continuità dell'energia elettrica (UPS, prese elettriche con controllo delle sovratensioni, ecc.)
- Accesso controllato
 - stanze chiuse a chiave
 - server ancorati a pareti o pavimento

Strumenti di protezione HW: i PC

- I rischi più frequenti per i PC
 - danneggiamento
 - furto
- raccomandiamo almeno:
 - prese di corrente protette
 - UPS
 - sistemi di condizionamento
 - uffici chiusi a chiave

Strumenti di protezione HW: esempi



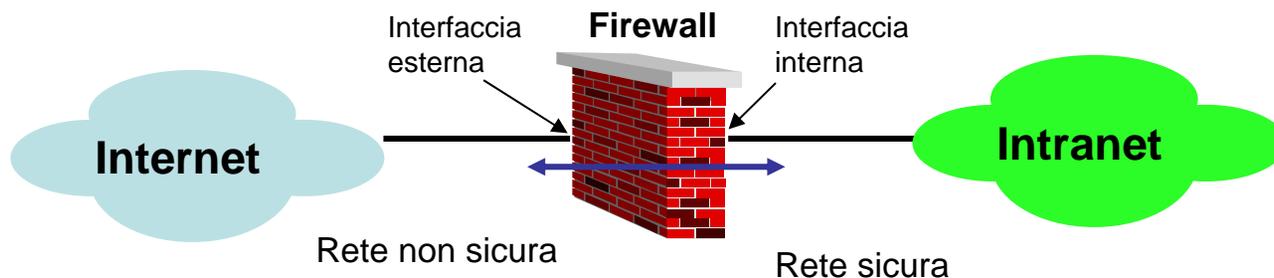
Sistemi anti-intrusione

Filtri

- per filtri si intendono programmi e configurazioni che permettono di controllare (accettare o bloccare) le comunicazioni di un *host* con il resto della rete
- si possono implementare filtri in ingresso e in uscita
- esistono semplici programmi (alcuni anche gratuiti) che permettono di farlo per varie piattaforme
- non sempre sono facili da usare (e da comprendere)
- periodicamente devono essere aggiornati e controllati

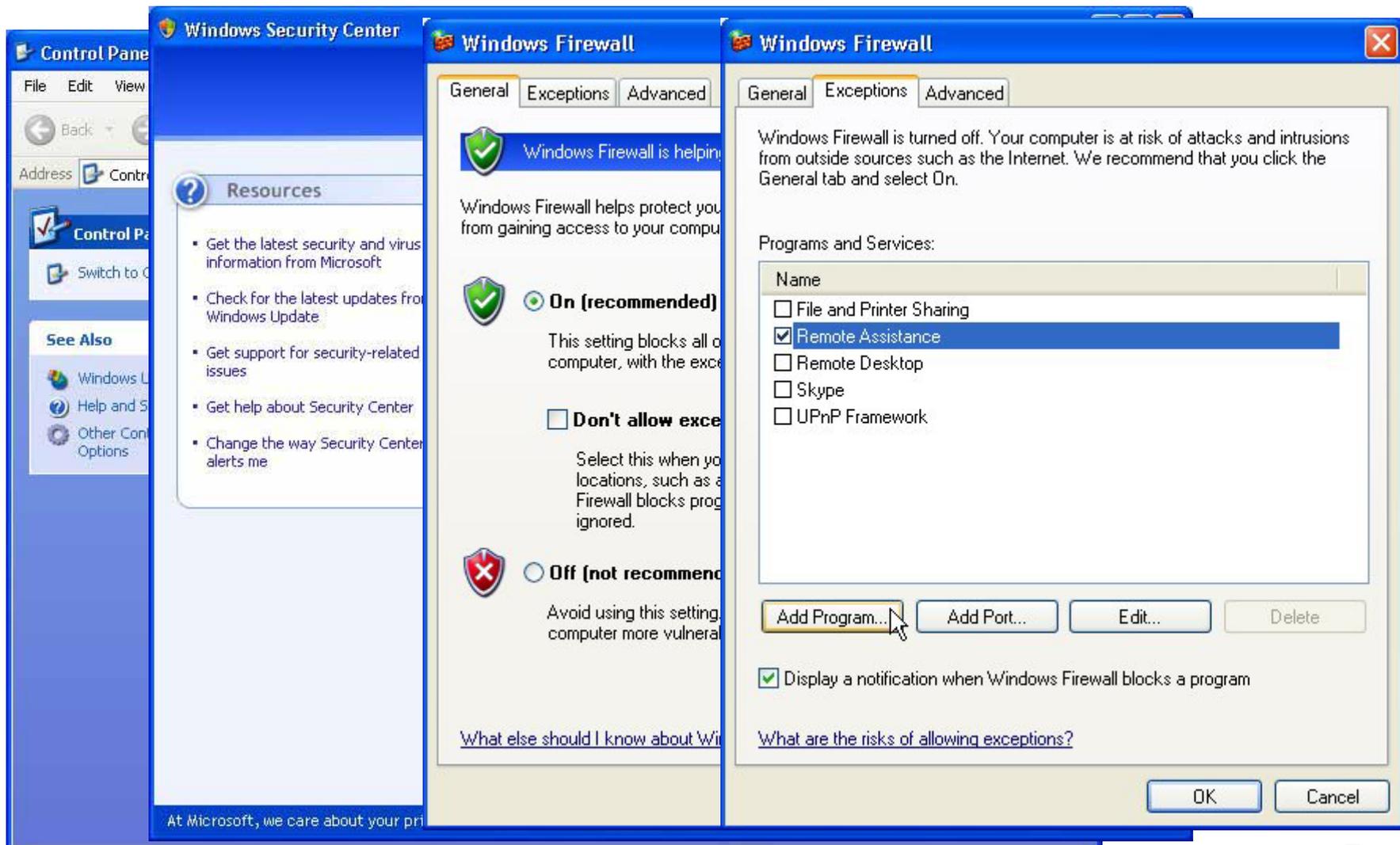
Firewall

- Definizione: “un firewall è un sistema che si frappone tra una parte della rete che deve essere protetta e il resto della rete, svolgendo una funzione di filtro sui pacchetti che lo attraversano”



@netgroup2003

Firewall: Windows XP SP2

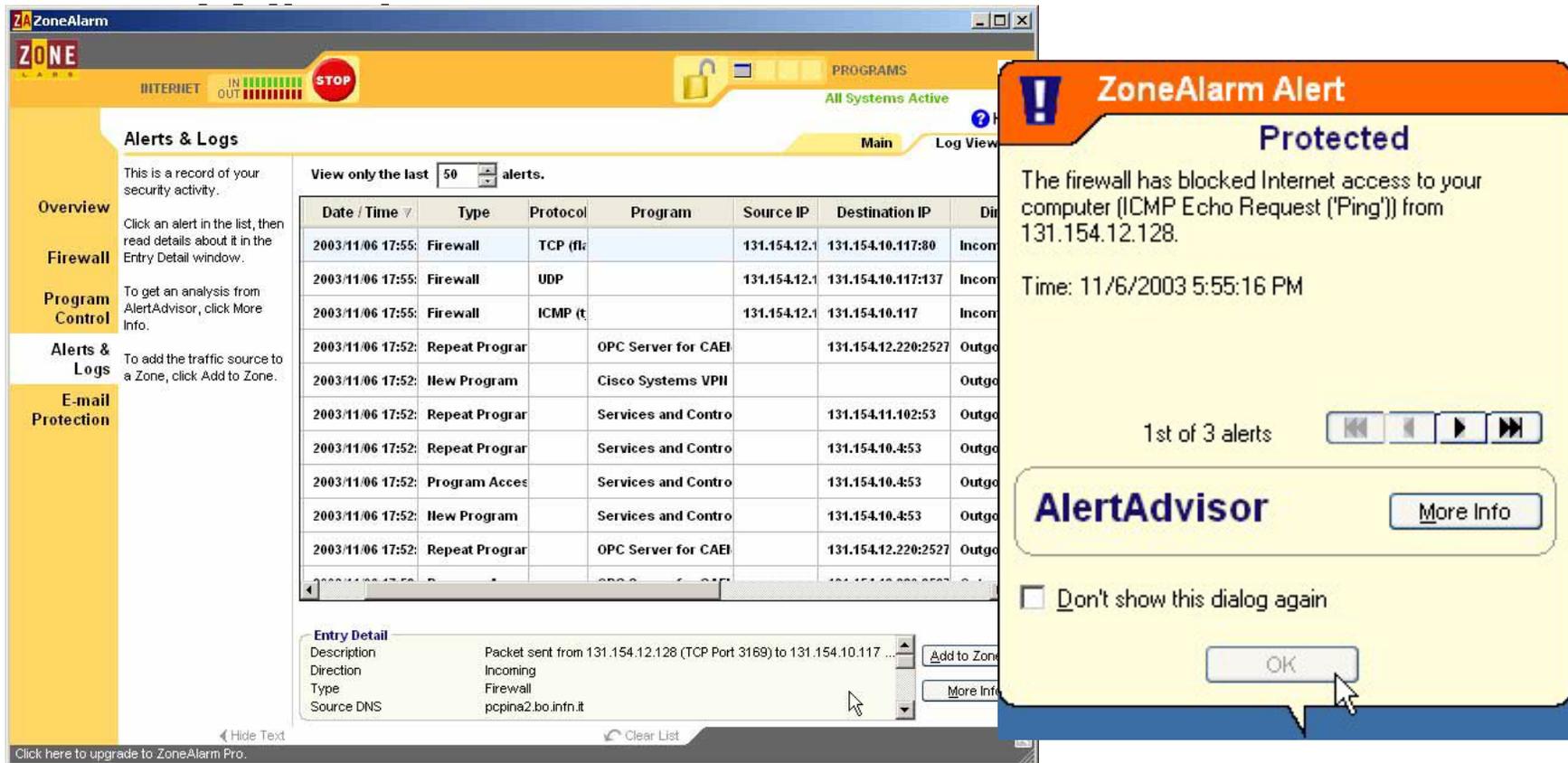


The screenshot displays three overlapping windows from Windows XP SP2:

- Control Panel:** Shows the 'Windows Security Center' link in the 'Control Panel' window.
- Windows Security Center:** Displays a 'Resources' section with links to get security information, check for updates, get support, get help about Security Center, and change alert settings.
- Windows Firewall (Left):** Shows the 'General' tab with 'Windows Firewall is helping' status. The 'On (recommended)' radio button is selected, indicating that the firewall is active and blocking all incoming connections except those for programs and services that you have allowed.
- Windows Firewall (Right):** Shows the 'General' tab with 'Windows Firewall is turned off'. The 'Programs and Services' list includes:
 - File and Printer Sharing
 - Remote Assistance
 - Remote Desktop
 - Skype
 - UPnP Framework
 The 'Add Program...' button is highlighted with a mouse cursor.

Esempio: ZoneAlarm

□ E' un Personal Firewall FREE per



The screenshot displays the ZoneAlarm software interface. The main window shows a list of alerts under the 'Alerts & Logs' section. The interface includes a sidebar with navigation options like 'Overview', 'Firewall', 'Program Control', 'Alerts & Logs', and 'E-mail Protection'. A detailed alert dialog box is overlaid on the right, showing a blocked internet access attempt.

Alerts & Logs

View only the last 50 alerts.

Date / Time	Type	Protocol	Program	Source IP	Destination IP	Dir
2003/11/06 17:55	Firewall	TCP (f)		131.154.12.1	131.154.10.117:80	Incom
2003/11/06 17:55	Firewall	UDP		131.154.12.1	131.154.10.117:137	Incom
2003/11/06 17:55	Firewall	ICMP (t)		131.154.12.1	131.154.10.117	Incom
2003/11/06 17:52	Repeat Program		OPC Server for CAEI		131.154.12.220:2527	Outgo
2003/11/06 17:52	New Program		Cisco Systems VPII			Outgo
2003/11/06 17:52	Repeat Program		Services and Contro		131.154.11.102:53	Outgo
2003/11/06 17:52	Repeat Program		Services and Contro		131.154.10.453	Outgo
2003/11/06 17:52	Program Acces		Services and Contro		131.154.10.453	Outgo
2003/11/06 17:52	New Program		Services and Contro		131.154.10.453	Outgo
2003/11/06 17:52	Repeat Program		OPC Server for CAEI		131.154.12.220:2527	Outgo

Entry Detail

Description: Packet sent from 131.154.12.128 (TCP Port 3169) to 131.154.10.117 ...

Direction: Incoming

Type: Firewall

Source DNS: pcpina2.bo.infn.it

ZoneAlarm Alert

Protected

The firewall has blocked Internet access to your computer (ICMP Echo Request ('Ping')) from 131.154.12.128.

Time: 11/6/2003 5:55:16 PM

1st of 3 alerts

AlertAdvisor [More Info](#)

Don't show this dialog again

OK

Sistemi anti-intrusione

Controllo dei *log*

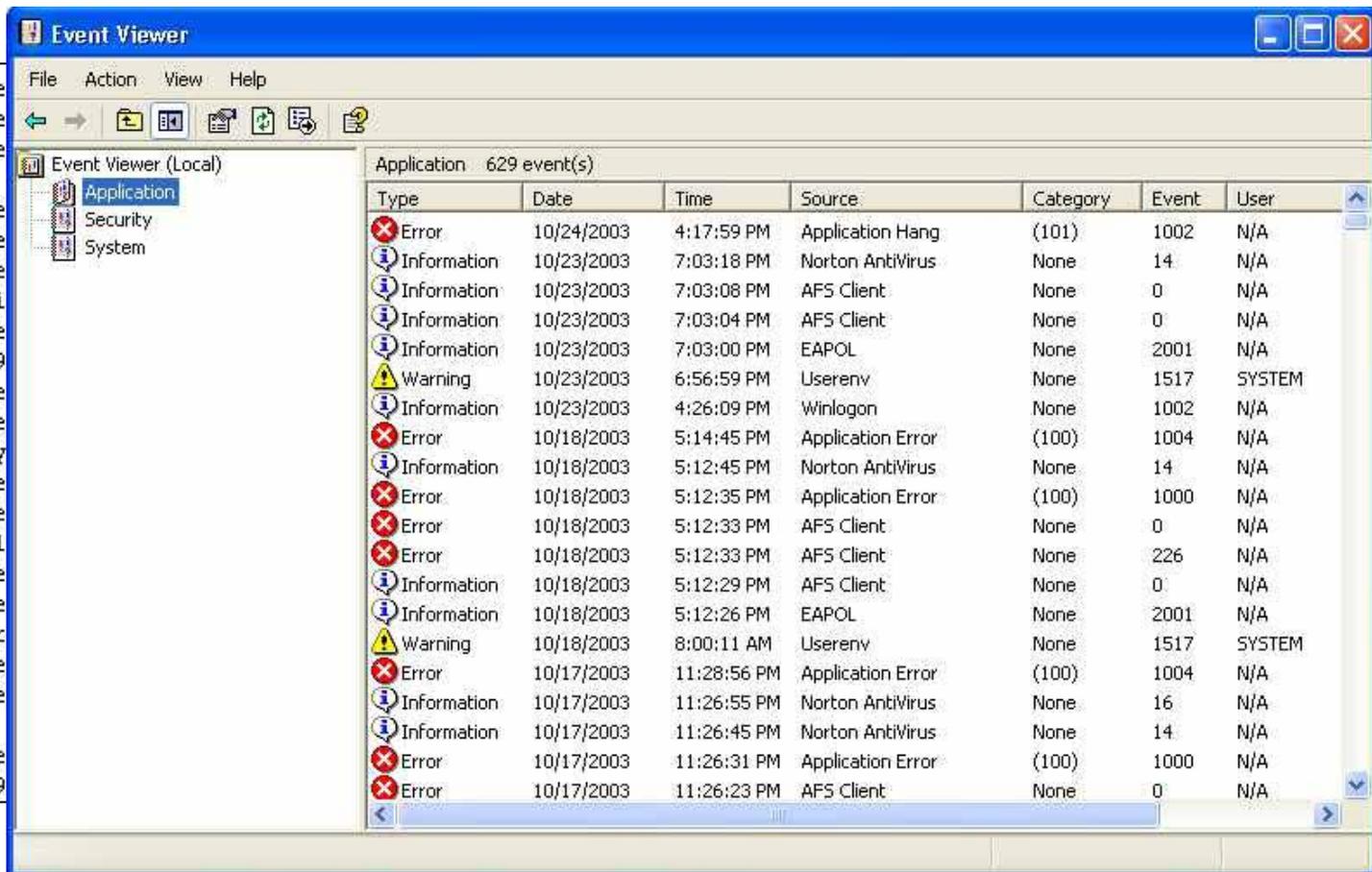
- i log sono messaggi sintetici che memorizzano il verificarsi di un evento, la data, l'ora, ecc.
- sono fondamentali per capire se un sistema sta funzionando male o se è stato compromesso
- non sempre sono facili da comprendere, ma esistono tool in grado di selezionare ed evidenziare i messaggi più importanti

Sistemi anti-intrusione

Esempi di log

```

Oct 21 13:13:20 pcte
Oct 21 13:14:19 pcte
Oct 21 13:14:19 pcte
sh
Oct 21 13:14:54 pcte
Oct 21 13:16:53 pcte
Oct 21 16:59:33 pcte
n last update time i
Oct 22 04:03:05 pcte
90503.h9J535f9009409
Oct 22 04:03:06 pcte
Oct 22 04:03:06 pcte
:00:01, mailer=relay
Oct 22 04:03:06 pcte
Oct 22 04:03:07 pcte
, pri=31348, relay=l
Oct 22 04:03:07 pcte
Oct 22 04:03:08 pcte
=relay, pri=32372, r
Oct 22 04:03:08 pcte
Oct 22 04:03:08 pcte
where
Oct 22 04:06:02 pcte
90506.h9J560oc009479
  
```



The screenshot shows the Windows Event Viewer window. The left pane shows the tree view with 'Application' selected. The right pane displays a list of 629 events for the 'Application' log. The events are listed in a table with columns for Type, Date, Time, Source, Category, Event ID, and User.

Type	Date	Time	Source	Category	Event	User
Error	10/24/2003	4:17:59 PM	Application Hang	(101)	1002	N/A
Information	10/23/2003	7:03:18 PM	Norton AntiVirus	None	14	N/A
Information	10/23/2003	7:03:08 PM	AFS Client	None	0	N/A
Information	10/23/2003	7:03:04 PM	AFS Client	None	0	N/A
Information	10/23/2003	7:03:00 PM	EAPOL	None	2001	N/A
Warning	10/23/2003	6:56:59 PM	Userenv	None	1517	SYSTEM
Information	10/23/2003	4:26:09 PM	Winlogon	None	1002	N/A
Error	10/18/2003	5:14:45 PM	Application Error	(100)	1004	N/A
Information	10/18/2003	5:12:45 PM	Norton AntiVirus	None	14	N/A
Error	10/18/2003	5:12:35 PM	Application Error	(100)	1000	N/A
Error	10/18/2003	5:12:33 PM	AFS Client	None	0	N/A
Error	10/18/2003	5:12:33 PM	AFS Client	None	226	N/A
Information	10/18/2003	5:12:29 PM	AFS Client	None	0	N/A
Information	10/18/2003	5:12:26 PM	EAPOL	None	2001	N/A
Warning	10/18/2003	8:00:11 AM	Userenv	None	1517	SYSTEM
Error	10/17/2003	11:28:56 PM	Application Error	(100)	1004	N/A
Information	10/17/2003	11:26:55 PM	Norton AntiVirus	None	16	N/A
Information	10/17/2003	11:26:45 PM	Norton AntiVirus	None	14	N/A
Error	10/17/2003	11:26:31 PM	Application Error	(100)	1000	N/A
Error	10/17/2003	11:26:23 PM	AFS Client	None	0	N/A

Operazioni di backup

Consapevolezza dell'importanza del backup

BACKUP = copia di sicurezza dei dati e/o del OS con lo scopo di ripristinare una situazione precedente (ad es. in caso di cancellazione accidentale o meno dei dati)

Operazioni di backup

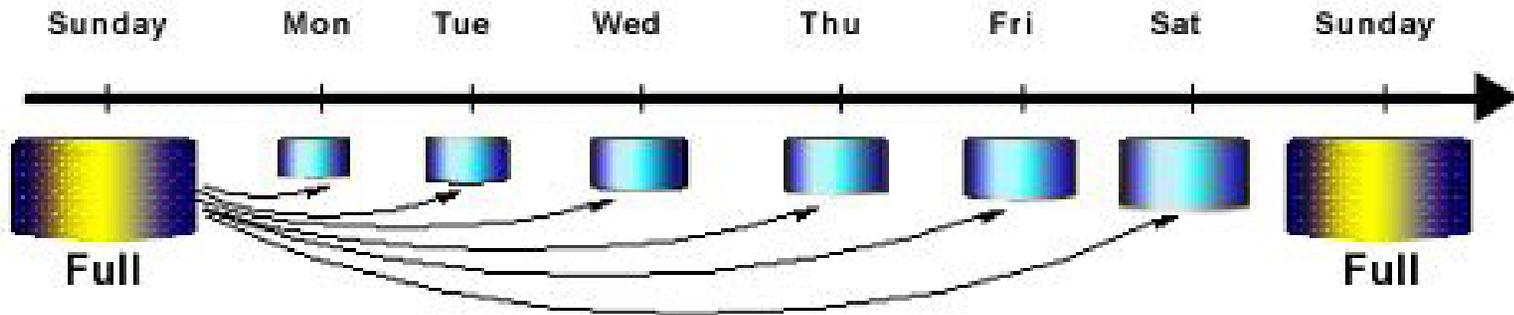
Modalità di salvataggio

- Backup storico
 - copia completa
- Backup differenziale
 - sono i file che sono stati modificati dopo l'ultimo backup completo
- Backup incrementale
 - solo i files che sono stati modificati dall'ultimo backup (storico o differenziale)

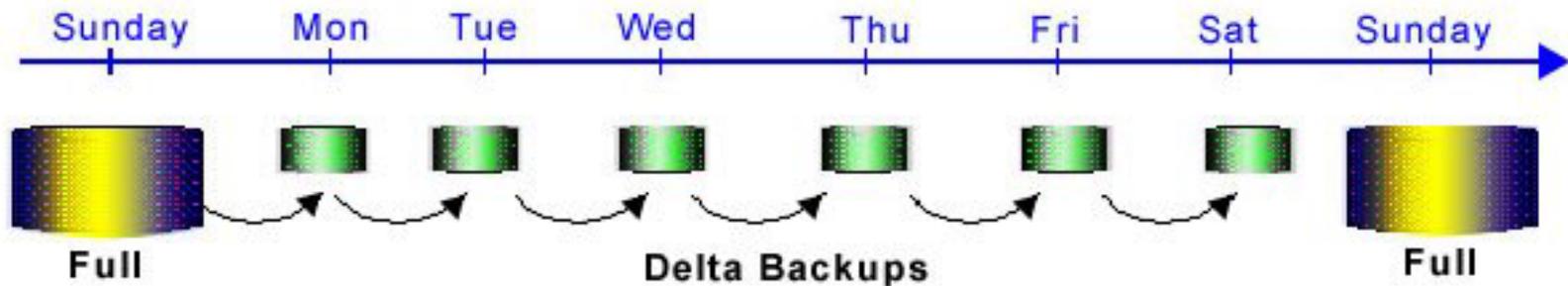
Modalità di ripristino

- per ripristinare completamente un sistema:
 - recuperare le informazioni dal backup storico
 - aggiungere le informazioni dell'ultimo backup differenziale o degli incrementali
- per ripristinare pochi file o una parte del sistema
 - può essere sufficiente cercare fra gli ultimi backup incrementali

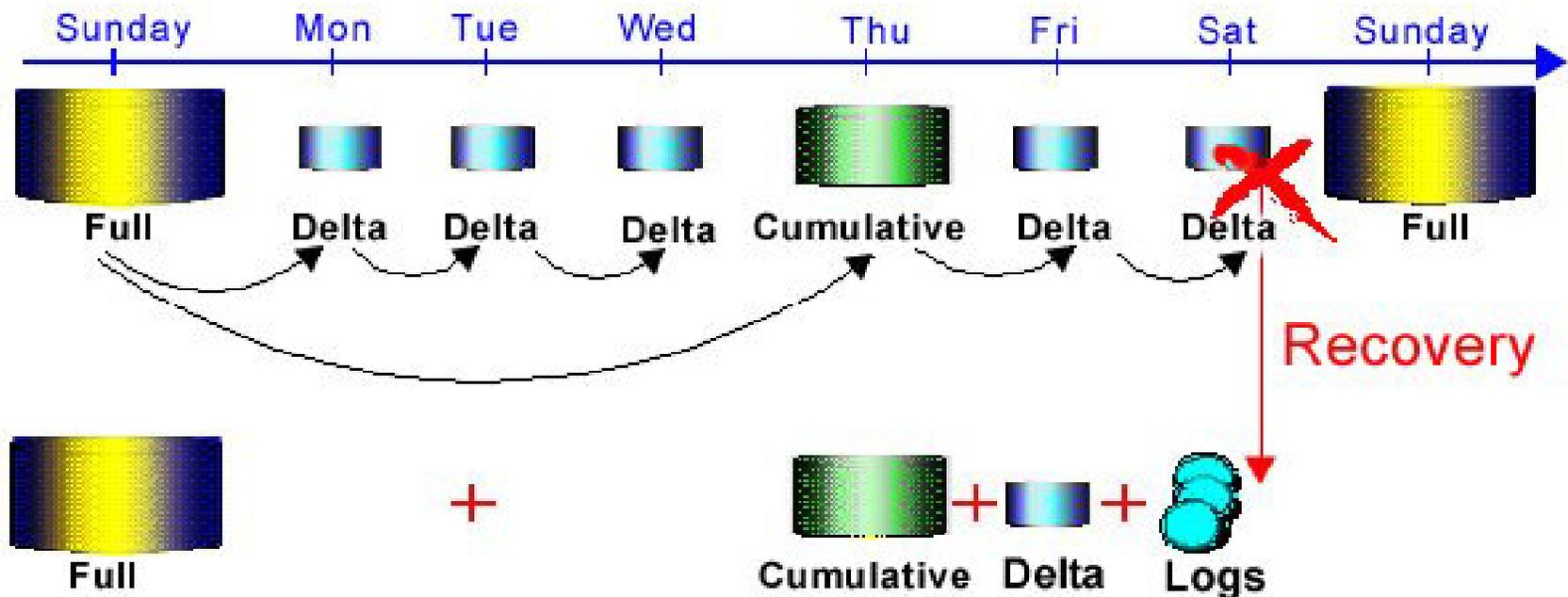
Esempio 1: Backup differenziale



Esempio 2: Backup incrementale



Esempio 3: backup & recovery



Operazioni di backup (dal punto di vista tecnico)

- **Importanza del backup**
 - in particolare per i dati che non possono essere ricavati da altre fonti
- **Conservazione dei supporti**
 - i diversi supporti si degradano nel tempo, alcuni anche abbastanza velocemente
- **Prove di ripristino**
 - effettuare periodicamente delle prove di ripristino da backup

Operazioni di backup (dal punto di vista “legale”)

■ Importanza del backup

- custodire e controllare i dati personali è un obbligo, per limitare i rischi di perdita, distruzione o accesso non autorizzato

■ Conservazione dei supporti

- il codice prevede che gli incaricati ricevano istruzioni sulla conservazione, il corretto utilizzo e la distruzione dei supporti

■ Prove di ripristino

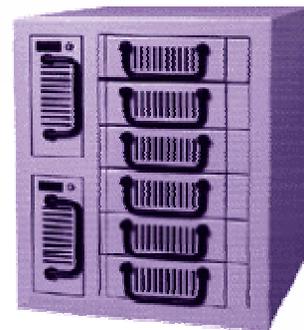
- deve essere garantito il ripristino dell'accesso ai dati (dati sensibili: “... in tempi certi ... non superiori a sette giorni”)

Supporti utilizzabili per il backup

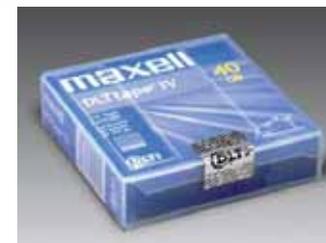
Apparati per backup



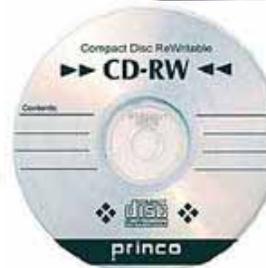
Backup su disco



Backup su nastro



Altri supporti

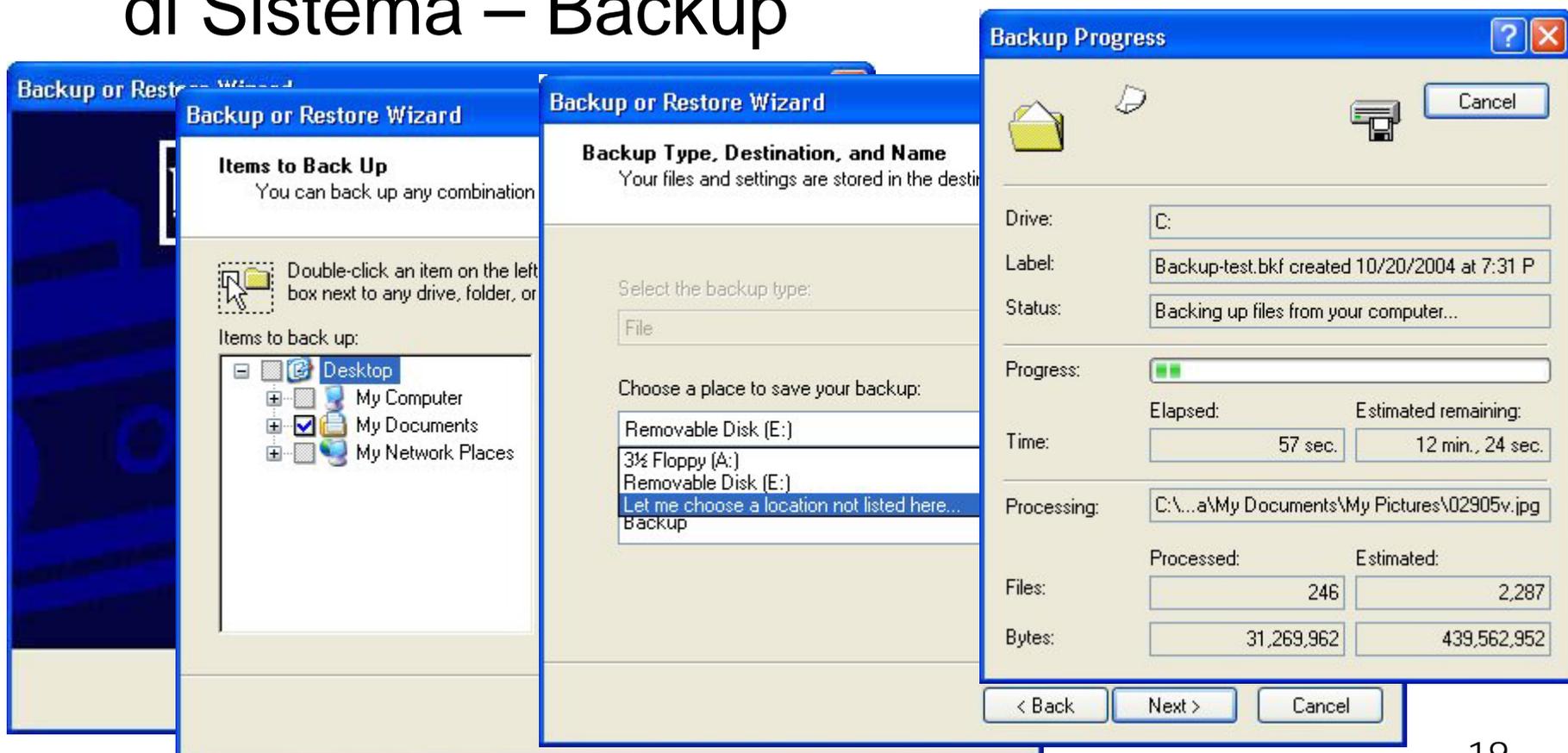


Software per backup



Funzione backup di Windows XP/2000

- Start – Programmi – Accessori – Strumenti di Sistema – Backup



The image displays three overlapping windows from the Windows Backup utility:

- Backup or Restore Wizard - Items to Back Up:** Shows a tree view of items to back up, including Desktop, My Computer, My Documents (checked), and My Network Places.
- Backup or Restore Wizard - Backup Type, Destination, and Name:** Shows the backup type set to 'File' and the destination set to 'Removable Disk (E:)'. A list of other drives is visible below.
- Backup Progress:** Shows the progress of the backup. The drive is C:, the label is 'Backup-test.bkf created 10/20/2004 at 7:31 P', and the status is 'Backing up files from your computer...'. The progress bar is partially filled. The elapsed time is 57 seconds, and the estimated remaining time is 12 minutes and 24 seconds. The file being processed is 'C:\...a\My Documents\My Pictures\02905v.jpg'. The processed files are 246 and the estimated total is 2,287. The processed bytes are 31,269,962 and the estimated total is 439,562,952.

Conoscenza approfondita del proprio PC

Gli incaricati del trattamento dei dati non devono essere degli esperti informatici!
Però è importante che:

- siano in grado di valutare il livello di sicurezza in cui operano
- possano capire se il PC che utilizzano è stato manomesso o meno
- e soprattutto, sappiano a chi rivolgersi in caso di dubbi o problemi!

Conoscenza approfondita del proprio PC

Come controllare che il PC non sia stato manomesso

- non sottovalutare comportamenti anomali (spegnimenti improvvisi, surriscaldamento, ecc.)
- verificare regolarmente i messaggi di errore e i log di sistema
- installare e configurare filtri e programmi di protezione del OS (secondo le indicazioni del SCR locale)
- in caso di dubbi consultare il SCR, che ha le competenze e gli strumenti per effettuare controlli approfonditi

Conoscenza approfondita del proprio PC

Come mantenere il proprio PC

*** CONSIGLI GENERALI ***

- installare le patch di sicurezza e gli aggiornamenti del OS
- installare e mantenere aggiornati SW antivirus
- configurare l'accesso al BIOS e al sistema tramite password non banali da cambiare periodicamente

Conoscenza approfondita del proprio PC

Come mantenere il proprio PC

*** consigli specifici per gli INCARICATI ***

- effettuare regolari backup dei dati
- custodire e conservare (o distruggere, quando previsto) i supporti utilizzati per il backup
- accedere ai dati personali solo nelle modalità consentite
- evitare se possibile di installare SW non strettamente necessario al trattamento dati
- configurare limitazioni d'accesso tramite PWD dove possibile

Conoscenza approfondita del proprio PC

In caso di dubbi consultatevi con i Servizi di Calcolo locali e seguite le loro indicazioni:

- possono predisporre per voi filtri e aree condivisibili ad accesso controllato
- possono impostare sistemi di backup e restore centralizzati o mirati ai vostri sistemi
- sanno installare, configurare e mantenere aggiornati OS, SW antivirus, personal firewall ecc. ecc.
- a volte possono organizzare seminari informativi e corsi di aggiornamento

Conoscenza approfondita del proprio PC

Valutare il livello di sicurezza: è un processo di scala

- l'Ente mantiene un Documento Programmatico sulla Sicurezza, con il quale ogni anno individua i criteri, le procedure e lo stato delle misure di sicurezza relative al trattamento dei dati personali
- ogni anno le unità operativa compilano una scheda di autovalutazione
- gli incaricati al trattamento contribuiscono alla compilazione riportando le loro conoscenze specifiche

Conclusioni

- è importante essere consapevoli
 - del tipo di dati che vengono trattati
 - della loro localizzazione
 - della specifica procedura di backup e restore
 - dello stato di conservazione dei dati e dei supporti
 - dello stato di sicurezza generale in cui si opera

Infine

- se ritenete di non operare in sicurezza, avete dubbi o incertezze
 - parlatene con il responsabile del trattamento
 - chiedete il supporto del Servizio di Calcolo e Reti
 - richiedete ulteriore formazione in materia informatica
 - **chiedete a noi: corsodpss@na.infn.it**

FINE!

Domande & risposte