LA SICUREZZA

La Sicurezza in Azienda

- La sicurezza del Lavoratore
- La sicurezza dei dati

La Sicurezza in Azienda

- La sicurezza del Lavoratore
- La sicurezza dei dati

Gestione dei Rischi

La sicurezza dei dati

- implementazione di soluzioni che facciano in modo che i dati siano “sicuri” e “al sicuro”, garantendo la:
  - disponibilità:
    - i dati devono essere sempre accessibili;
  - riservatezza:
    - i dati devono essere protetti da accessi da parte di utenti non autorizzati;
  - integrità:
    - i dati devono essere protetti da modifiche non autorizzate

La sicurezza dei dati

- Eventi accidentali
  - Eventi non prevedibili (incendi, terremoti, alluvioni, guasti, …..)
- Eventi intenzionali
  - Eventi che mirano al furto e/o al danneggiamento dei dati

BACKUP e RESTORE

- Creazione di una copia del contenuto dei dischi su supporti rimovibili (nastri magnetici, dischi ottici,...) che possono essere conservati in luoghi sicuri

- **Completo**
  - copia dell'intero sistema;
- **Incrementale**
  - copia dei dati in base alle differenze che ci sono tra i dati in uso e quelli che sono già stati copiati precedentemente.
- **Differenziale**
  - quando vengono salvati solo i dati che sono stati modificati dopo l'ultimo backup completo.

- L'attività di backup può essere avviata manualmente o automaticamente

GRUPPO DI CONTINUITA’

- U.P.S. – Uninterruptible Power Supply

RAID

- Redundant Array of Inhexpensive Disks

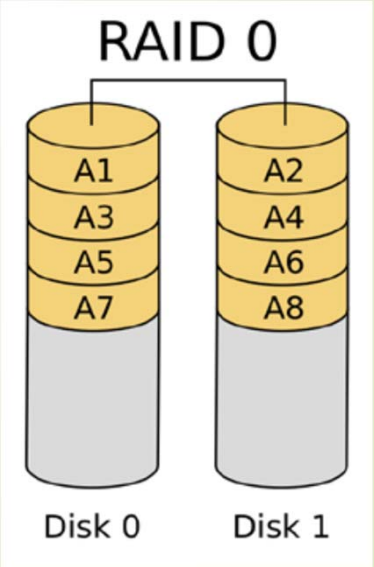
  - tecnica di raggruppamento di diversi dischi rigidi collegati ad un computer che li rende utilizzabili, dalle applicazioni e dall'utente, come se fosse un unico volume di memorizzazione
  - tecnica tipicamente impiegata nei server o nelle workstation che richiedano grandi volumi o elevate prestazioni di immagazzinamento di dati, per esempio per ospitare una base di dati
  - può essere implementato sia con hardware dedicato sia con software specifico su hardware di uso comune.

RAID 0 (striping)

- Il sistema RAID 0 divide i dati equamente tra due o più dischi
- usato generalmente per aumentare le prestazioni di un sistema

- **Vantaggi**
  - costo di implementazione basso;
  - alte prestazioni in scrittura e lettura, grazie al parallelismo delle operazioni I/O dei dischi concatenati.

- **Svantaggi**
  - se un disco si rompe, tutti i dati vengono persi.



RAID 1 (mirroring)

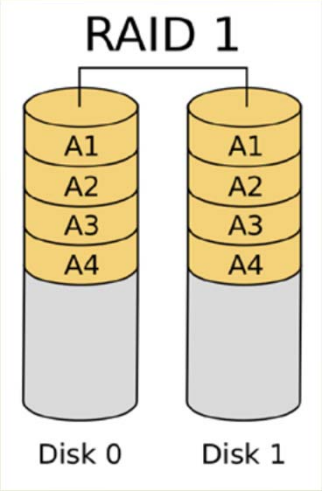
- Metodo per avere un'archiviazione ridondante
- entrambi i dischi contengono sempre gli stessi identici dati, e quando uno dei dischi si rompe tutti i dati sono sempre presenti sull'altro.

Vantaggi

- affidabilità, cioè resistenza ai guasti, che aumenta linearmente con il numero di copie;

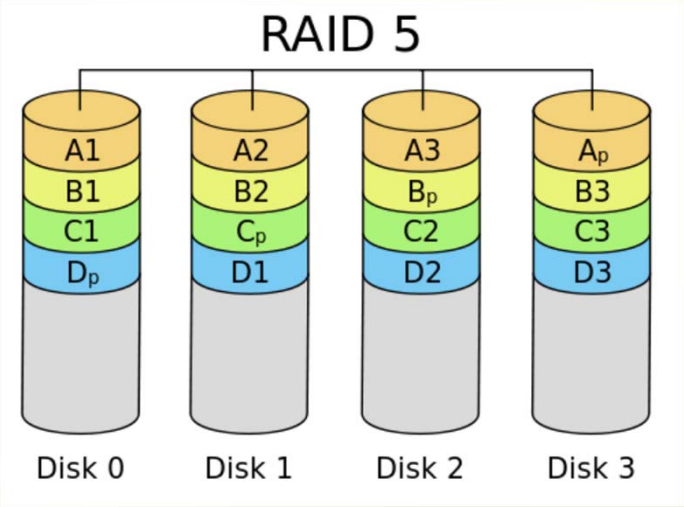
Svantaggi

- costi aumentati linearmente con il numero di copie;
- velocità di scrittura ridotta a quella del disco più lento dell'insieme.



RAID 5

- minimo di tre dischi
- **Vantaggi:**
  - quando un disco di un RAID 5 si rompe, tutti i dati possono essere letti, sebbene ci sia un calo prestazionale.
  - Un dato mancante viene ricostruito con le informazioni di parità distribuite, ma c'è un calo prestazionale.
- **Svantaggi:**
  - scritture lente a causa della modifica e del calcolo della parità.



FAULT TOLERANCE

- Tolleranza ai guasti
  - UPS
  - RAID
  - Duplexing
  - duplicazione dell'unità di controllo dei dischi (controller) oltre che dei dischi
  - duplicazione dell'intero sistema

EVENTI INDESIDERATI

- Qualsiasi accesso (a servizio o informazione) che non sia esplicitamente permesso dalla politica di sicurezza del sistema
- Attacchi deliberati che mirano al furto e/o al danneggiamento dei dati, per il semplice gusto di arrecare danni o per averne dei tornaconto personali
  - A livello fisico
  - A livello logico

ATTACCHI A LIVELLO FISICO

- principalmente tesi a sottrarre o danneggiare risorse critiche
  - furto: prevedibile per nastri di backup, dischi o interi server; è un attacco alla disponibilità ed alla riservatezza;
  - danneggiamento: attacco tipicamente condotto contro apparecchiature e cavi di rete, più raramente contro calcolatori server in quanto questi sono generalmente confinati in locali sicuri; è un attacco alla disponibilità ed alla integrità

ATTACCHI A LIVELLO LOGICO

- principalmente tesi a sottrarre informazione o degradare la operatività del sistema.
  - intercettazione e deduzione (attacco alla riservatezza);
  - intrusione (attacco alla integrità ed alla riservatezza);
  - disturbo (attacco alla disponibilità).

ATTACCHI DI INTERCETTAZIONE

- Gli attacchi di intercettazione possono richiedere un attacco preventivo a livello fisico per installare dispositivi pirata o per agganciarsi alla rete
- Tecniche comuni:
  - analizzatori di traffico su rete;
  - applicazioni di analisi del traffico su rete (sniffing);
  - server pirata che si spacciano come router (spoofing);
  - programmi che emulano servizi del sistema (tipicamente il login, durante il quale l'utente digita username e password) registrando al contempo le informazioni riservate digitate dall'utente

ATTACCHI DI INTRUSIONE

- Gli attacchi di intrusione mirano a entrare in ambienti protetti da password
  - Individuazione delle password utilizzando programmi appositamente progettati per generare sistematicamente combinazioni di caratteri semi-casuali e verificarle come password tentando l'accesso al sistema in modo automatico
  - Attacchi di questo tipo devono il loro successo al fatto che gli utenti scelgono come password parole di uso comune, e quindi, in definitiva, ad una debolezza nella politica di sicurezza o nella sua attuazione da parte del personale

ATTACCHI DI DISTURBO

- Gli attacchi di disturbo mirano a degradare la operatività del sistema. Sono considerabili come atti di sabotaggio, e minacciano tipicamente la integrità e la disponibilità dei dati

  - Virus
  - Worm
  - DOS

ATTACCHI DI DISTURBO : VIRUS

- I virus sono programmi auto-replicanti, spesso inseriti nel sistema come cavalli di Troia, generalmente pericolosi per la integrità del file-system e per la disponibilità dei servizi
- I virus sono principalmente caratterizzati:
  - dal modo in cui arrecano danno al sistema,
  - dal modo di camuffare i danni causati come problemi nell'hardware o nel software di base del calcolatore colpito
  - dal modo in cui si inseriscono e si duplicano nel sistema
  - dal modo in cui si sottraggono alla identificazione da parte dei programmi anti-virus

ATTACCHI DI DISTURBO : WORM

- I worm sono virus particolari che si limitano a degradare le prestazioni del sistema, ad esempio lanciando molte immagini di uno stesso processo.

ATTACCHI DI DISTURBO : DOS

- Denial of Service.
- Famiglia di tecniche tese a fare in modo che il sistema neghi l'accesso a servizi ed informazioni anche ad utenti regolarmente autorizzati.
- Gli attacchi che usano queste tecniche minacciano quindi i requisiti di disponibilità del sistema.
- Due tipiche tecniche "denial of service":
  - paralizzare il traffico sulla rete generando falsi messaggi di errore
  - Intasare il traffico sulla rete con traffico di disturbo generato appositamente

STRUMENTI DI PROTEZIONE - 1

- Password
  - Semplice o complessa?
- WiFi
  - Password WPA-WPA2
  - SSID
  - Black list
  - White list

STRUMENTI DI PROTEZIONE - 2

- Crittografia
- Steganografia
- Firewall
- Buon senso….

PHISHING

Gentile Titolare,

Il sistema ha rilevato che la password per accedere al Portale scadrà tra 2 giorni.
Ti consigliamo di procedere con la modifica altrimenti l'accesso al Portale può essere limitato fino a quando non avrai eseguito la modifica.
È possibile che ti venga chiesto di inserire il codice di conferma: 841650.

Tra qualche istante sarai reindirizzato automaticamente sul Portale Titolari per procedere con la scelta della nuova password.

Se non vieni reindirizzato automaticamente al Portale entro alcuni secondi, fai clic qui .

Cordialmente,
Servizio Clienti CartaSi

Per favore, NON rispondere a questa mail, questo è un MESSAGGIO AUTOMATICO: per eventuali comunicazioni accedi alla tua area riservata del Sito Internet di CartaSi e scrivici allo "Lo sportello del Cliente", è il modo più semplice per ottenere una rapida risposta dai nostri operatori. Grazie della collaborazione.

http://www.index-jspid001931330.com/avvia.sessione.cookie/titolari.cartasi.it