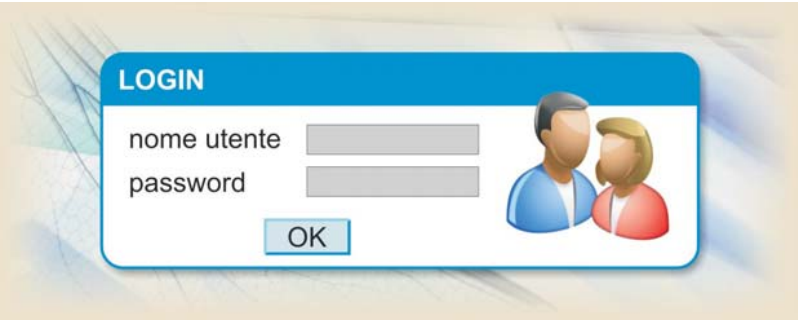
La sicurezza

La gestione di un sistema di elaborazione ha un aspetto cruciale rappresentato dalla necessità di garantire la **consistenza** dei dati in esso memorizzati, sia nel caso di un computer personale, sia nel caso di sistemi informatici aziendali: i dati devono essere significativi ed essere effettivamente utilizzabili nelle applicazioni. I dati devono, quindi, essere protetti per impedire perdite accidentali dovute a improvvise interruzioni dell'attività del sistema, guasti hardware o interventi dannosi da parte di utenti o programmi: la protezione deve riguardare anche gli interventi dolosi sui dati dovuti ad accessi non autorizzati con operazioni di modifica o di cancellazione.

In sostanza **sicurezza** significa impedire che il sistema e i suoi dati vengano danneggiati da interventi accidentali o non autorizzati; **integrità** significa garantire che le operazioni effettuate sul sistema e sui dati da parte di utenti autorizzati non provochino una perdita di consistenza ai dati.

Gli archivi di dati possono essere usati da più applicazioni: perciò il progettista di un'applicazione deve preoccuparsi di definire chi e come può accedere ai dati, ma in un ambiente che comprende tutti i dati aziendali occorre avere una responsabilità centralizzata in grado di distribuire le autorizzazioni e le modalità di accesso.

In generale ad ogni utente viene associato un **profilo**, il cui accesso è controllato mediante l'**identificativo dell'utente** (*user ID* o *username*) e la **parola d'ordine** (*password*): il primo rappresenta il nome, che può anche essere pubblico, con il quale l'utente accede alla procedura di riconoscimento (*login*), mentre la seconda rappresenta la parola chiave, di solito scelta dall'utente stesso, che è privata e riservata. Per questo motivo la password dovrebbe essere non banale (nomi di persona, date di nascita, ecc.) e dovrebbe essere frequentemente cambiata.

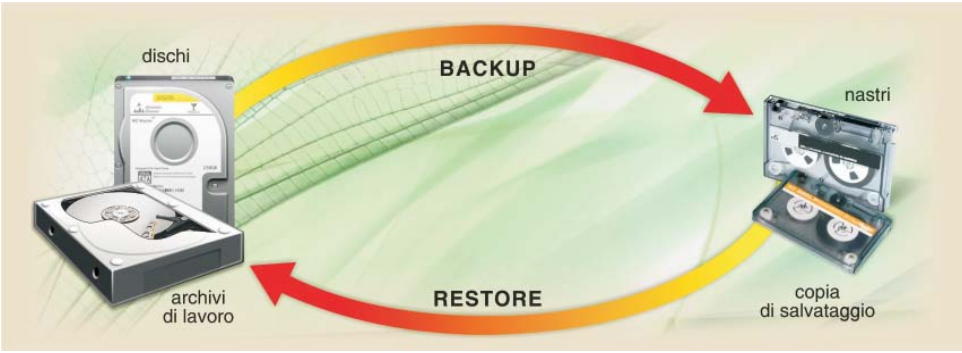


Al profilo sono poi associati i **diritti di accesso**, cioè le azioni, i permessi e i divieti relativi alle attività svolte dall'utente: quali programmi può utilizzare, quali archivi può consultare, quali permessi su un singolo archivio (solo lettura oppure lettura e scrittura), la possibilità di installare nuovi programmi.

Questi controlli vengono realizzati a diversi livelli: gestione degli archivi di dati, sistemi operativi, reti di utenti. Essi sono gestiti al livello di **amministratore del sistema** (*system administrator*), che nel personal computer coincide con l'utente stesso, mentre per sistemi più complessi o per le reti è una specifica figura professionale del settore informatico.

Gli archivi elettronici hanno più o meno gli stessi problemi degli archivi cartacei, per esempio un'unità a dischi si può rompere provocando la perdita di tutti i dati in essa contenuti, oppure un errore degli operatori può provocare la cancellazione non voluta di uno o più archivi: pertanto si rende necessaria la copia periodica degli archivi e la conservazione delle copie in posti sicuri.

L'attività di copia di archivi grandi ha durate significative e di solito viene eseguita giornalmente: questa attività si chiama **backup** (salvataggio). L'attività opposta si chiama **restore** (ripristino) e serve per ricaricare su disco tutti o parte degli archivi salvati precedentemente.



Nelle situazioni dove non è consentita l'interruzione dell'attività di un sistema di elaborazione (*downtime*), come per esempio in una banca o in un supermercato, la sicurezza viene garantita anche nella parte hardware attraverso la duplicazione di parti o dell'intero sistema: queste tecniche vengono indicate con il termine **fault tolerance** (tolleranza del guasto) e riguardano principalmente le memorie di massa nei server delle reti e nei sistemi di medie e grandi dimensioni.
Di seguito vengono esaminate le **cause** che possono incidere negativamente, e talvolta in modo irreparabile, sulla sicurezza del sistema informatico di un'azienda nel suo complesso.

Errori del personale
L'enorme sviluppo dell'elettronica moderna consente di accumulare grandi quantità di dati in spazi molto piccoli e secondo modalità che non sono quasi mai simili alle operazioni svolte secondo la gestione manuale, per cui anche errori banali possono produrre disastri.
Le norme per prevenire tali eventualità di solito consistono in:
- una netta separazione tra l'ambiente di esercizio e l'ambiente di sviluppo del software, per evitare che il programmatore durante le sue prove inquini o peggio distrugga i dati che servono per le procedure aziendali;
- copia periodica di tutti i dati aziendali su supporti di backup da conservare in luogo sicuro per un successivo ripristino se richiesto: normalmente vengono conservati più salvataggi di giornate differenti al fine di una maggiore protezione;
- intervento di livelli professionali differenti in caso di ripetizione dell'errore in modo da evitare qualsiasi rischio;
- definizione di regole organizzative e figure professionali preposte a verificare tutte le anomalie nei dati di input o di output.

Pirata informatico
Il termine *pirata informatico* sta ad indicare una persona che si collega, con sistemi di elaborazione, sfruttando i meccanismi di rete senza avere l'autorizzazione all'accesso. Questi inserimenti indesiderati con messaggi o programmi possono anche portare alla paralisi del sistema. Anche in questo caso la difesa è costituita dal controllo degli accessi, tenendo conto del fatto però che l'elemento più fragile è rappresentato dall'uso di password banali e facilmente prevedibili. Per questo è opportuno integrare i sistemi di controllo degli accessi con l'uso di tessere magnetiche di riconoscimento.

Virus
I *virus* sono programmi chiamati così perché sono stati costruiti con lo scopo di:
- "infettare" un programma senza alterarne il funzionamento
- rendersi visibili in qualche modo
- autoriprodursi nell'ambiente in cui sono inseriti creando un'"epidemia" che può essere dannosa (distruzione di dati e programmi) o solo contagiosa estendendosi a tutti i programmi e a tutti i computer.

Possono essere prodotti per gioco oppure talvolta con finalità ricattatorie.
Non esiste un modo attraverso il quale distinguere un programma da un virus e quindi un virus diventa tale solo dopo la sua scoperta e la sua denominazione.
La protezione contro i virus può essere realizzata attraverso il controllo sistematico di tutti i supporti che vengono usati e attraverso il controllo degli accessi della rete.
Esistono poi organizzazioni che si sono specializzate nelle identificazioni dei virus e degli effetti che producono, e nella costruzione di programmi antivirus (*vaccino*) per eliminarli.
In alcuni casi la rimozione del virus può richiedere la cancellazione dei programmi danneggiati: pertanto diventa fondamentale il lavoro di filtro sugli accessi, sui dati e sul software, con scopi di prevenzione.

I principali tipi di virus per computer sono:
- Virus che provocano *infezione sui file*, in particolare sui file eseguibili .COM o .EXE e che vengono caricati nella memoria del computer ogni volta che il programma viene eseguito. Sono tipi di virus che si solito arrivano sul computer attaccati ad altri programmi o come allegati a messaggi di posta elettronica.
- Virus che attaccano il sistema e in particolare il *boot-record* del disco, cioè il blocco del disco che contiene le informazioni sull'avvio del computer.
- Virus per le *Macro*, che sono comandi simbolici costruiti dall'utente all'interno dei programmi Office (Word, Excel, Access) e che consentono di eseguire una sequenza di operazioni elementari frequentemente utilizzate. L'infezione di questo tipi di virus provoca malfunzionamenti nei programmi Office.
- Cavalli di Troia (*Trojan*): sono programmi all'apparenza normali che possono però distruggere i file sul disco oppure l'intero disco. A differenza dei virus precedenti, non replicano se stessi su altri computer.
- I virus *Worm* sono programmi autoreplicanti che hanno come caratteristica principale la capacità di diffondersi rapidamente sulla rete di computer e in Internet.

Regole pratiche per prevenire l'infezione dei virus per computer

1. Installare e usare un buon programma antivirus.
2. Aggiornare frequentemente le definizioni dei virus, scaricando gli aggiornamenti dal sito Internet del fornitore del software antivirus.
3. Non aprire messaggi di posta elettronica di dubbia provenienza.
4. Non aprire allegati contenuti all'interno di messaggi di posta elettronica con mittente sconosciuto o non sicuro.
5. Fare la scansione dei supporti di memoria provenienti da fonte insicura prima di usare i file e i programmi in essi contenuti.
6. Non scaricare musiche, file multimediali o filmati da un sito Internet che non offra garanzie di sicurezza.
7. Dopo aver scaricato un programma da Internet, effettuare il controllo antivirus prima di installarlo ed eseguirlo.
8. Operare con cautela la condivisione di file e musiche con altri utenti della rete; durante la connessione con condivisione di cartelle sul disco, il computer è aperto all'ingresso non autorizzato e all'attacco da parte di utenti esterni.
9. Effettuare frequentemente copie di sicurezza (su altri dischi o chiavi USB) dei documenti e file che riteniamo importanti per il nostro lavoro.

Furti di apparecchiature mobili

Un aspetto particolare della sicurezza riguarda il rischio per l'azienda derivante dal furto di computer portatili o telefoni cellulari. Queste apparecchiature possono essere facilmente asportate in modo furtivo e possono contenere dati, archivi, contatti, password e numeri telefonici riservati o confidenziali. L'uso fraudolento di queste informazioni può provocare gravi danni a una singola persona o a un'azienda, ben più gravi del valore commerciale dell'apparecchiatura rubata.