Sicurezza personale

Proteggere i dati

Misure per prevenire accessi non autorizzati ai dati

Abbiamo visto come sia essenziale proteggere i dati riservati, propri o altrui. Esistono, come vedremo più in dettaglio nei capitoli successivi, specifiche tecniche che possono essere applicate in **via preventiva**, per impedire l'accesso ai dati. Il metodo più usato è l'utilizzo di **Password**: sono stringhe di caratteri usate per l'autenticazione dell'utente, per dimostrare l'identità o ottenere l'accesso a una risorsa.

Nel campo della sicurezza informatica, si definisce autenticazione il processo tramite il quale un computer, un software o un utente, verifica la corretta, o almeno presunta, identità di un altro computer, software o utente che vuole comunicare attraverso una connessione.

La forma di autenticazione più semplice si fonda sull'utilizzo di un **nome utente** (per *identificare* l'utente)e di una **password** (o parola d'ordine, per *autenticare* l'utente).

L'autenticazione tramite nome utente è password è ormai molto diffusa nell'ambiente delle reti e di internet: per accedere alla propria postazione di lavoro in una rete aziendale o addirittura al proprio pc, per accedere alla posta elettronica in remoto, per le operazioni di home banking, per accedere a servizi di messaggistica istantanea, ecc. è sempre necessaria l'autenticazione.

Il motivo è ovvio. Il sistema a cui si vuole accedere deve essere sicuro che l'utente è proprio quello che ne ha il diritto.

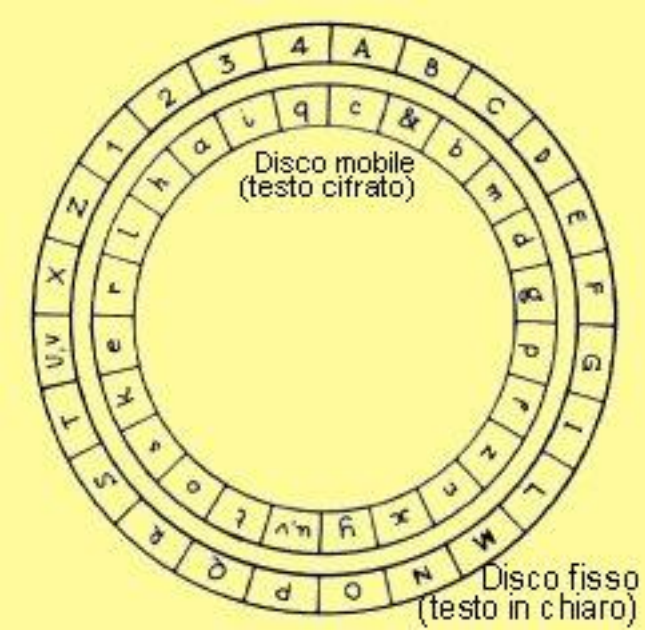
Se per il nome utente non ci sono raccomandazioni particolari, può essere un nome di fantasia semplice da ricordare, la password deve essere scelta in modo oculato, **non deve essere comunicata ad altre persone** e, in casi di dati riservati o importanti, **deve essere cambiata con regolarità.**

Come deve essere una password?

La password deve essere lunga a sufficienza, composta da lettere e numeri e non facilmente associabile alla vita dell'utente: quindi non il proprio nome, cognome, soprannome, data di nascita, indirizzo, ecc.

Ci sono tecniche che impediscono l'utilizzo dei dati se, nonostante le misure preventive, qualcuno sia venuto in possesso di queste informazioni. La **Crittografia** analizza come "offuscare" un messaggio in modo che non sia comprensibile a persone non autorizzate a leggerlo.

Un tale messaggio si chiama **crittogramma** e le tecniche usate per rendere incomprensibile il messaggio si chiamano tecniche di **cifratura**. La crittografia è utilizzata in tutti gli ambiti dove è necessaria la segretezza delle informazioni: informazioni militari (soprattutto in caso di conflitti), informazioni bancarie riservate, comunicazioni tra Stati, spionaggio, ecc. Esistono metodi di crittografia molto sofisticati per l'importanza dei dati che devono trattare.
Un esempio (molto semplice) di tecnica crittografica è il disco cifrante di Leon Battista Alberti, che per primo insegnò a cifrare per mezzo di un con un alfabeto segreto che si ottiene spostando il disco interno di due o tre parole.



Caratteristiche fondamentali della sicurezza delle informazioni

Riassumendo, i dati personali e/o riservati per essere sicuri, devono avere un alto fattore di **confidenzialità**, cioè devono essere protette da accessi o divulgazione non autorizzati.
Queste protezioni non devono comunque essere di ostacolo all'**integrità** dell'informazione, la quale deve essere affidabile cioè integra, completa, senza modifiche rispetto all'originale.
È fondamentale poi la **disponibilità** dell'informazione al momento del bisogno: non avrebbe senso esasperare la sicurezza dei dati se poi, quando servono, per qualche motivo non si riesce a recuperarli nei tempi necessari.

Principali requisiti per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia

Nel gennaio 2012, la Commissione Europea ha approvato la proposta di un regolamento sulla protezione dei dati personali, in sostituzione della direttiva 95/46/CE valida per i 27 stati membri dell'Unione Europea e una direttiva che disciplina i trattamenti per finalità di giustizia e di polizia (attualmente esclusi dal campo di applicazione della direttiva 95/46/CE).

In accordo con questo regolamento sulla protezione dei dati personali in Italia è stato emesso Decreto Legislativo n. 5 del 9 febbraio 2012 che ha preso il posto del precedente Dlgs 196/2003.

Il decreto contiene un articolato pacchetto di interventi volto ad alleggerire il carico degli oneri burocratici gravanti sui cittadini e sulle imprese, con una semplificazione delle procedure amministrative, ad esempio per il cambio di residenza, comunicazioni di dati tra le amministrazioni, partecipazione a concorsi, ecc.

Importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT.

Vista l'importanza dell'argomento, ci sono delle specifiche linee guida e politiche per l'uso dell'ICT, delle regole chiare che forniscono uno standard che deve essere seguito dagli utenti e disciplinano l'utilizzo delle tecnologie informatiche e delle telecomunicazioni (ICT) per preservare i dati, personali e aziendali, dal furto, dallo smarrimento e da un utilizzo non consentito. Assicurano una posizione chiara su come dovrebbe essere usata l'ICT per assicurare la protezione dei dati aziendali. In questo modo le aziende (come i privati) possono tutelarsi e devono, a loro volta, tutelare i propri dipendenti, clienti e fornitori.

Alcune di queste linee sono:

- Non lasciare che i dettagli dei principali conti aziendali siano di pubblico dominio, così che i frodatori possano ottenere dettagli sufficienti per intaccarli.
- Predisporre un'accurata politica di gestione e archiviazione dei documenti: è il primo passo per proteggere l'azienda e i dipendenti contro il furto di identità.
- Distruggete tutti i documenti riportanti dati sensibili: le aziende hanno il dovere di conservare e proteggere le informazioni dei propri clienti e dei propri dipendenti oltre che l'obbligo. Abbiamo visto che in Italia è in vigore il Decreto Legislativo n. 5 del 9 febbraio 2012 che dichiara che "chiunque per motivi professionali conserva o tratta dati sensibili altrui (e quindi, tutte le organizzazioni, le aziende, gli enti pubblici, i professionisti …) è soggetto alle cautele e agli obblighi previsti dalla legge in quanto responsabile civilmente e penalmente anche in modo oggettivo di ogni danno cagionato al titolare o a terzi da un trattamento non corretto; il trattamento dei dati è considerato un' attività pericolosa e come tale gode dell'inversione dell'onere della prova (art. 2050 Codice Civile): è il responsabile del trattamento dei dati che ha l'onere di dimostrare il corretto utilizzo per evitare di incorrere in sanzioni civili e penali. L'ufficio del Garante della Privacy può richiedere alle autorità di polizia di effettuare controlli e le sanzioni per il mancato rispetto della legge possono arrivare a 80.000 euro (articoli da 161 a 172 del decreto).
  La legge elenca 17 possibili operazioni di trattamento dei dati. In particolare, i dati su supporti cartacei o multimediali una volta cessato il trattamento devono essere distrutti

(art. 16, c. 1-a). Distruggere i supporti, cartacei e non, è infatti il modo migliore per evitare che i criminali possano avere accesso ai dati sensibili.

- Mettere i dipendenti a conoscenza dei rischi di frode di identità aziendale: questo può garantire che rimarranno vigili.
- Assicurarsi che la procedura di gestione dei documenti sia comunicata e correttamente eseguita da tutti i dipendenti. Fare in modo che siano cauti nel fornire le informazioni dell'azienda on-line o via telefono, verificando con chi effettivamente hanno a che fare.
- Assicurarsi che il sistema operativo antivirus e firewall (che vedremo nei capitoli successivi) siano tenuti aggiornati. In questo modo i dipendenti possono aprire in sicurezza gli allegati delle e-mail ricevute.