Sicurezza

Guarantire sicurezza significa proteggere i dati e le risorse garantendo

- Segretezza (*Confidenzialità*) L'informazione può essere rilasciata – direttamente o indirettamente – solo a utenti autorizzati a conoscerla.

  Privacy: diritto di un individuo di stabilire se, come, quando e a chi l'informazione che lo riguarda può essere rilasciata.

- Integrità Le informazioni (e le risorse) non devono essere modificate, cancellate o distrutte in modo non autorizzato o *improprio*.

- Disponibilità (*Availability* –no *denials-of-service*) Non deve essere impedito agli utenti gli accessi propri e per i quali hanno la autorizzazione necessaria.

Vulnerabilità, minacce, difese

- Vulnerabilità Debolezza del sistema che potrebbe permettere violazioni alla sicurezza

  Esempi: dipendenza da una sola sorgente di energia; personale poco competente; protezione della rete inadeguata

- Minaccia Circostanza o evento che potrebbe causare violazioni alla sicurezza

  Esempi: Intrusori; Utenti interni; Malware (malicious software)

- Difesa (contromisura) Tecnica, procedura o altra misura che *riduce la vulnerabilità*

  Esempi: Autenticazione; Controllo degli accessi; Backup

Applicazione della sicurezza

Non esiste sicurezza in senso assoluto, le misure di sicurezza possono

- Ridurre le possibilità che una violazione avvenga
- Ridurre i danni che una violazione può portare

La sicurezza ha un costo in termini di:

- Acquisto, applicazione e gestione di misure aggiuntive
- Aumento del carico del sistema $\Rightarrow$ diminuzione delle prestazioni

La mancanza di misure di sicurezza ha un costo (il sistema ed il suo funzionamento sono a rischio)

La applicazione di misure di sicurezza va bilanciata rispetto al valore delle risorse da proteggere ed al danno che una violazione a questi porterebbe

Controlli di sicurezza

- Sicurezza fisica: Es., Allarmi anti-incendio, tesserine magnetiche, ...
- Sicurezza organizzativa: Procedure per la corretta amministrazione delle autorizzazioni e degli accessi.
- Sicurezza logica: Controllo dell'accesso alle risorse da parte di utenti che sono correttamente "entrati nel sistema"

.... Non è solo un problema di tecnologie...

Servizi di sicurezza

- Identificazione e Autenticazione Fornisce al sistema la abilità di identificare gli utenti e verificarne l'identità.
- Controllo dell'accesso valuta le richieste di accesso alle risorse fatte da utenti autenticati e, sulla base di regole definite, determina se permettere o negare l'accesso.
  - controlla solo gli accessi *diretti*. Può essere arricchito con controlli *di flusso*, *inferenza* e *non-interferenza*
- Audit permette una valutazione a posteriori delle richieste e degli accessi avvenuti per determinare se ci sono state (o sono state tentate) violazioni.
- Crittografia assicura che i dati memorizzati nel sistema o spediti lungo la rete possano essere decifrati solo dal legittimo ricevente.
  Nella comunicazione su rete può anche essere utilizzata per stabilire l'autenticità delle informazioni trasmesse o delle parti coinvolte.

Servizi di sicurezza