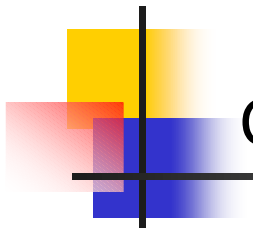

Gestione della Sicurezza Informatica

Giancarlo Galluzzi

Giancarlo.Galluzzi@unimi.it

Gestione della Sicurezza Informatica

- Di cosa si occupa la sicurezza Informatica?
  - Tutto quello che viola le regole imposte da
    - Leggi dello Stato
    - AUP GARR
    - AUP Locali
  - Tutto quello che riguarda l'uso corretto dello strumento informatico
  - Tutto….

Gestione della Sicurezza Informatica

- Cosa deve considerare un 'sistema' che si occupa della Sicurezza informatica?
  - Abusi e Misusi degli strumenti informatici (e basta? … C'è dentro tutto!)
- Cosa bisogna fare
  - Misure di prevenzione (attività di controllo)
  - Eventuali verifiche (attività forense)
  - Soluzione agli 'incidenti' (attività di ripristino/risoluzione)
- Categorizzazione degli incidenti
  - Esterno -> Interno
  - Interno -> Esterno
  - Interno -> Interno

Gestione della Sicurezza Informatica

- In cosa consiste il 'fare' (1)
  - Misure di prevenzione
    - Sicurizzazione dei sistemi
    - Gestione delle basi dati
    - Strumenti di analisi
    - Attività di filtro
    - Accesso agli strumenti autenticato e personalizzato
  - Verifiche
    - Rintracciabilità dell'utenza interessata (intesa sia come sistema che come responsabile)
    - Tracciabilità degli eventi
    - Analisi e correlazione degli eventi

Gestione della Sicurezza Informatica

- In cosa consiste il 'fare' (2)
  - Soluzione agli 'incidenti'
    - Messa in sicurezza dei sistemi
    - Identificazione del responsabile
    - Recupero della funzionalità del sistema
- Come affrontare l'epica impresa?
  - Strumenti adeguati
  - Personale qualificato
  - Sensibilizzazione ed educazione dell'utenza

Gestione della Sicurezza Informatica

- Come si è mossa e si muove l'Università di Milano
  - Sistemi di gestione della banda (rete)
  - Sistemi IPS ed IDS (rete)
  - Software Antivirus e antispam
  - Sistema di autenticazione centralizzato (Radius/ldap)
  - Autenticazione accesso in rete (802.1x sia wired che wireless)
  - Hardening dei sistemi informatici centralizzati
  - Politiche di filtering sugli accessi semi-pubblici (aule informatiche, hotspot…)
  - AUP dettagliate
  - Formazione e responsabilizzazione di referenti 'locali'

Gestione della Sicurezza Informatica