

# Organizzare la Sicurezza nei Sistemi Informatici

Claudio Di Benedetto

Direttore Servizio Elaborazione Dati

Istituto Superiore di Sanità

Tel. +39 06 49903372

Fax. +39 06 49387176

E-mail: [dibene@iss.it](mailto:dibene@iss.it)

# Introduzione

- Scopo della presentazione è quello di illustrare i punti fondamentali del tema “sicurezza informatica” e l’impatto organizzativo che ne deriva sulla struttura aziendale.
- La sicurezza del sistema informatico, difatti, non dipende solo da aspetti tecnici, ma soprattutto da quelli organizzativi.

# Organizzazione funzionale della gestione della sicurezza

- Da un punto di vista organizzativo la realizzazione di un sistema di sicurezza, si può ricondurre a ***tre specifiche funzioni***:
  - ◆ Definizione delle Politiche di Sicurezza in materia informatica;
  - ◆ Attuazione delle Politiche definite al punto precedente;
  - ◆ Verifica della corretta attuazione e della efficienza delle misure adottate (Audit di sicurezza).

# Definizione delle Politiche

- Tale funzione ha caratteristiche eminentemente strategiche in quanto definisce le finalità e gli obiettivi che si intendono raggiungere.
- Le indicazioni dovranno essere coerenti con le norme vigenti in tema di sicurezza informatica definite dal Governo.
- Particolare attenzione dovrà essere posta al fine di contenere i costi, coerentemente con il valore del patrimonio informativo da proteggere.

# Attuazione

- Tale funzione ha il compito di progettare, realizzare e mantenere in efficienza le misure definite al punto precedente.
- I principali compiti sono:
  - ◆ Individuazione dei beni da proteggere e le minacce a cui i detti beni sono sottoposti;
  - ◆ Mappa dei rischi;
  - ◆ Analisi costi/benefici;
  - ◆ Implementazione del sistema di sicurezza;
  - ◆ Aggiornamento e manutenzione;

# Verifica e controllo

- Tale funzione ha il compito di controllare le misure adottate, verificandone l'efficacia nel tempo (audit di sicurezza).
- Richiede autonomia operativa ed un alto livello di conoscenze tecniche.

# Piano per la Sicurezza Informatica

Da un punto di vista implementativo e secondo l'approccio globale è necessario che ogni struttura dotata di Sistemi Informativi automatizzati definisca un Piano di Sicurezza la cui articolazione prevede le seguenti attività:

- Analisi del rischio
- Definizione delle politiche di sicurezza
- Gestione del rischio
- Il piano operativo
- Audit
- Formazione

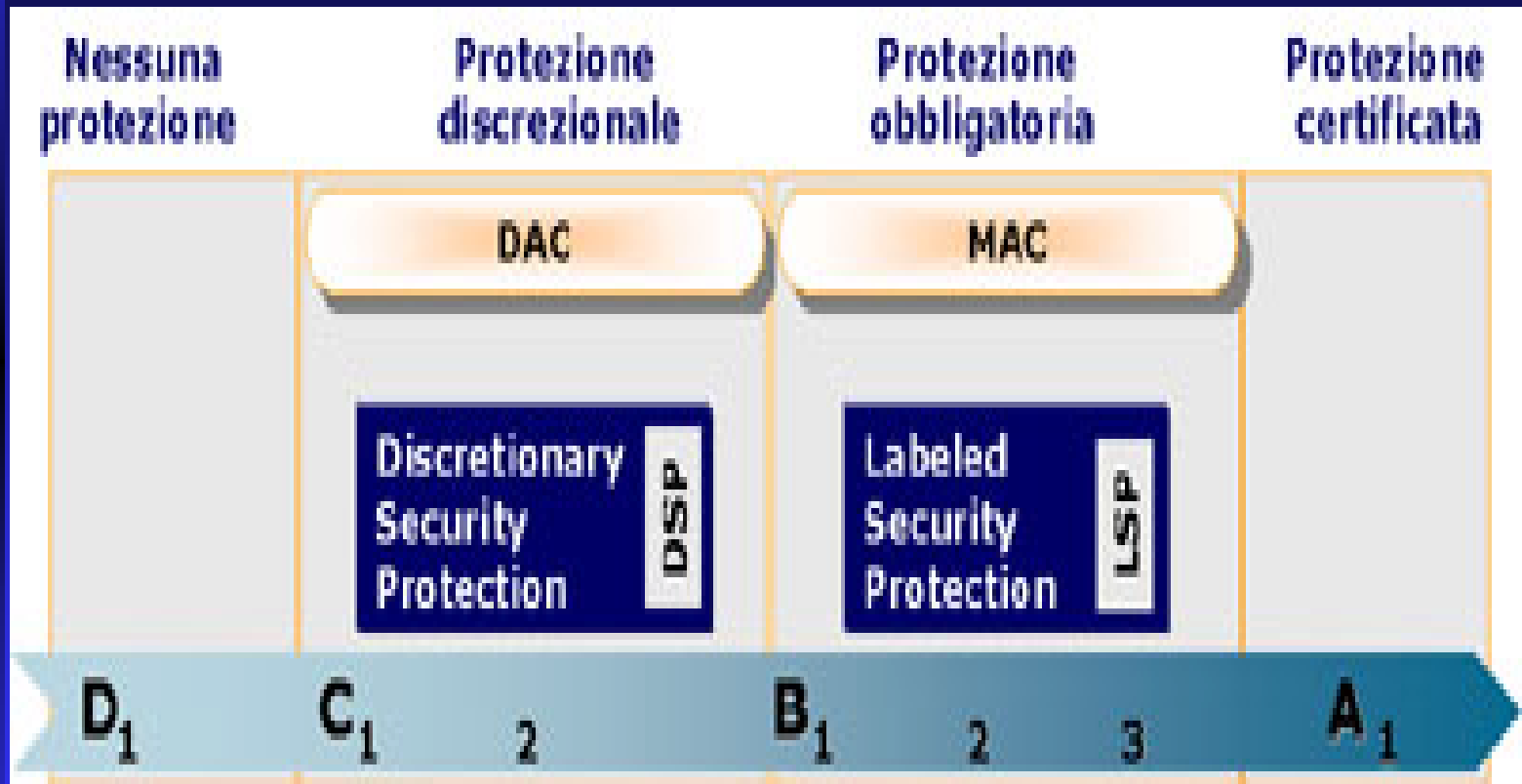
# Scopi e obiettivi di un Piano per la Sicurezza

Fornire servizi che abbiano le seguenti proprietà:

- **Confidenzialità o Riservatezza** : ove necessario l'accesso ai dati avverrà previa autorizzazione (meccanismi di autenticazione forte: dispositivi biometrici, psw dinamiche, certificati digitali..);
- **Disponibilità** : fruibilità della risorsa da parte dell'utente autorizzato;
- **Integrità** : certezza che le informazioni non siano state manipolate (conformazione originale);
- **Autenticità** : certezza sulla provenienza dei dati (identità dell'autore del messaggio);
- **Non ripudiabilità**: il mittente (destinatario) di una transazione non può negare di averla inoltrata (ricevuta).

# Standard di sicurezza

- Il primo standard che stabilisce i diversi livelli di sicurezza utilizzati per proteggere l'hw, il sw e l'informazioni memorizzate in un sistema è rappresentato dal Trusted Computer System Evaluation Criteria (TCSEC) redatto dal Dipartimento della Difesa degli Stati Uniti: il famoso Orange Book.
- I criteri di valutazione TCSEC dividono in quattro categorie il tipo di protezione assicurato da ogni livello:
  - ◆ D: nessuna protezione
  - ◆ C: protezione discrezionale
  - ◆ B: protezione obbligatoria
  - ◆ A: protezione certificata



# Analisi del rischio : individuazione delle risorse da proteggere e relative minacce

- **Risorse hw** (server, workstation, linee di comunicazione con particolare riguardo alle apparecchiature di rete). Crash hardware accidentali, ma anche sabotaggi ed intercettazioni;
- **Risorse sw**: integrità dei s.o., ma anche del software applicativo. Utilizzo di software non certificato (acquisti o download da Internet). Applicativi non opportunamente testati. Infezioni da virus (sempre più via e-mail, ma anche da Internet).

## Analisi del rischio (2)

- ***Dati***: l'accesso alle banche dati sia da parte di utenti interni, sia (soprattutto) da parte di utenti esterni deve essere controllato con strumenti di autenticazione forte. Intrusioni e danneggiamenti via rete, ma anche modifiche accidentali da parte di utenti autorizzati ad accedere a banche dati;
- ***Persone*** : amministratori di rete, sistemisti, programmatori ecc, possono essere oggetto di minacce, ma diventare essi stessi una minaccia per il sistema sicurezza;
- ***Documentazione cartacea***

# Aspetti valutativi: beni e loro vulnerabilità

Questo passo è indispensabile per capire quanto siano importanti le risorse da proteggere all'interno del sistema informativo e quale sia il livello di vulnerabilità delle stesse.

Si possono adottare criteri quantitativi (costi) o qualitativi (perdita d'immagine, di efficacia/efficienza).

# Individuazione del rischio

La misura del rischio cui è esposto il sistema informatico è determinata correlando attraverso una matrice gli elementi di valutazione precedenti:

- ◆ *Valore dei beni;*
- ◆ *Livello delle minacce;*
- ◆ *Livello di vulnerabilità dei beni;*

L'analisi di tale matrice consente di evidenziare l'entità del rischio associata ai diversi beni e di individuare un insieme di contromisure (di seguito indicate nel Piano Operativo) per diminuire consistentemente o abbattere l'entità del rischio stesso.

# Definizione delle Politiche di Sicurezza

Un aspetto fondamentale della realizzazione di un Piano per la Sicurezza è la definizione delle Politiche di Sicurezza che la struttura intende adottare.

- Un buon riferimento sulle politiche di sicurezza si trova in RFC 1244 (“Site Security Handbook”).
- Le Politiche di Sicurezza devono essere approvate ed emanate dai vertici della struttura e applicate a **TUTTI** i dipendenti.
- Il personale deve percepire le politiche di sicurezza come una componente del lavoro quotidiano finalizzata alla protezione delle informazioni e delle apparecchiature.

# Definizione delle Politiche di Sicurezza

Le politiche dovrebbero riguardare:

- **Protezione fisica** delle risorse: classificazione delle aree, accesso controllato e sorveglianza delle stesse, rilevazione tempestiva degli incidenti.
- **Protezione logica**: controllo dell'accesso alle informazioni, sviluppo del software applicativo, controllo delle porte di rete.
- **Piano di Continuità Operativa**: prevedere le risorse necessarie per il ripristino dell'attività lavorativa in caso di emergenza.
- L'applicazione delle Politiche di Sicurezza richiede la definizione dei processi che descrivono gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi stabiliti nelle Politiche.

# Il Piano Operativo

- Consente di determinare l'insieme delle contromisure di natura diversa (fisica, logica, organizzativa) idonee a gestire il livello di rischio precedentemente determinato.
- Ci soffermiamo principalmente sull'aspetto della *Sicurezza Logica* intendendo con ciò l'insieme delle contromisure di carattere tecnologico che concorrono nella realizzazione del livello di sicurezza da raggiungere.

# Accorgimenti tecnologici (1)

- Sistemi RAID e sottosistemi storage (NAS, SAN)
- Back-up, Disaster Recovery
- Rendere il canale di comunicazione sicuro attraverso i seguenti strumenti:
  - ◆ *protocollo IPSEC*, consente la cifratura dei messaggi in uscita (oltre all'autenticazione dell'utente e integrità dei dati);
  - ◆ *protocollo SSL*, è sostanzialmente una libreria di routine richiamabili attraverso linguaggi di programmazione volte a realizzare applicazioni client/server "sicure";

# Accorgimenti tecnologici (2)

- *VPN* consente di far viaggiare i dati in modo protetto sull'infrastruttura pubblica, è una buona alternativa alle reti dedicate, specie quando si vuole connettere sedi remote di una stessa realtà distribuita sul territorio. E' basato su IPSEC, si può implementare in modo sw o hw (vantaggi e svantaggi);
- *Firewall* (principale strumento di *access control* alle reti basate su TCP/IP);

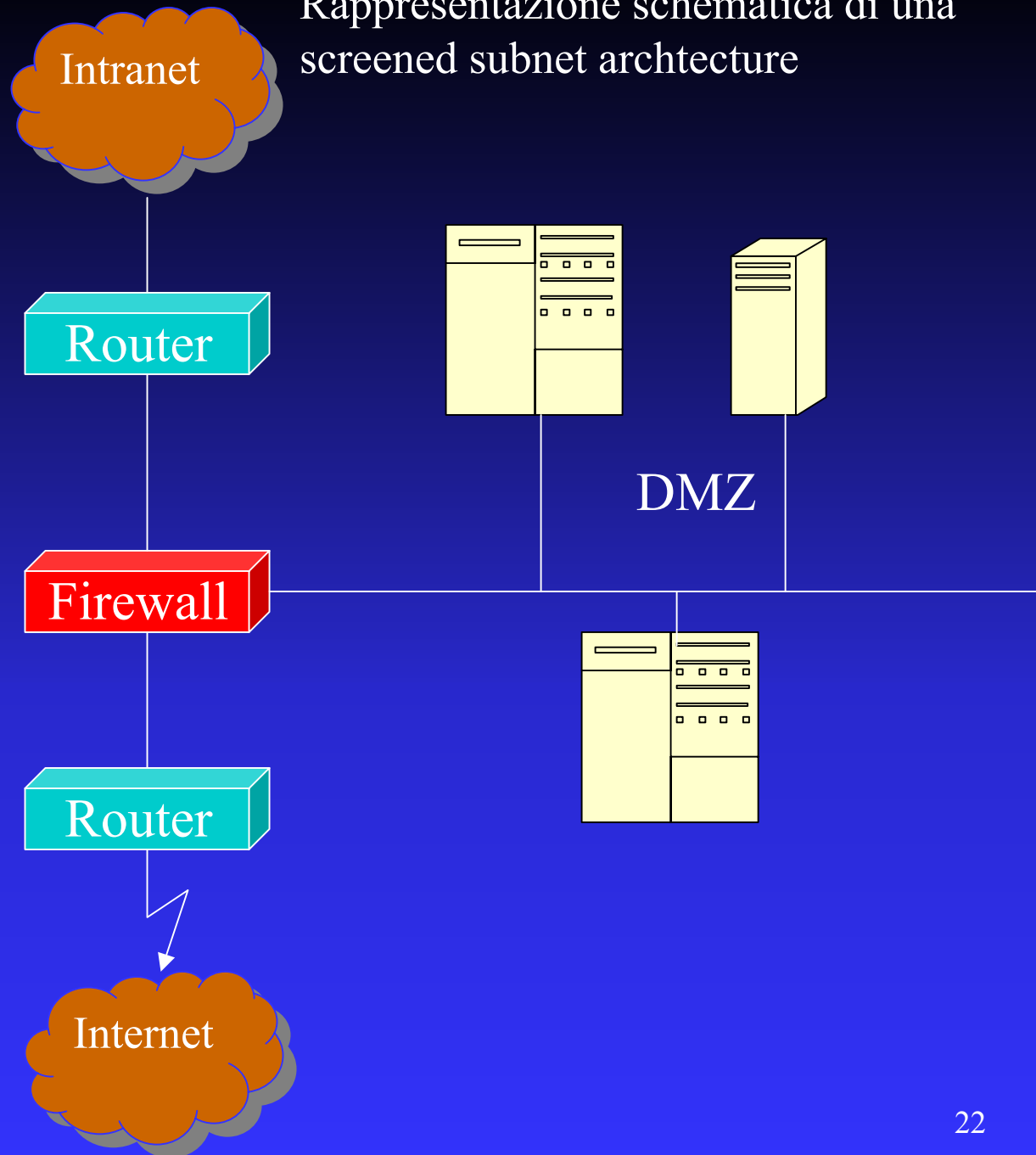
# Accorgimenti tecnologici (3)

- Un Internet firewall è una entità posta tra la rete interna ed Internet allo scopo di limitare l'esposizione alle intrusioni da parte di utenti esterni. Fisicamente è composto da un insieme di componenti hw e sw, dal punto di vista realizzativo fa riferimento a due diverse tecniche per l'intercettazione e l'analisi del traffico di rete: il *packet filtering* e i *proxy system*.
- *Il filtraggio dei pacchetti* è semplice da implementare (liste di access control su router), è economico e non richiede azioni da parte degli utenti. Di contro non è in grado di analizzare il contenuto dei pacchetti, non effettua l'autenticazione degli utenti, rende visibile gli indirizzi della rete interna.

# Accorgimenti tecnologici (4)

- *I firewall basati su proxy server* agiscono a livello di applicazione: possono essere utilizzati per effettuare un filtraggio dall'interno verso siti esterni, posto in DMZ si tramuta in reverse proxy (funziona da gateway verso la rete interna). Ha anche funzionalità di cache. Tra i vantaggi ricordiamo: autenticazione, hiding della rete, content filtering. Tra gli svantaggi il numero limitato di proxy per le principali applicazioni: FTP, HTTP, Telnet..., decadimento delle prestazioni e configurazione degli host della rete protetta.
- L'architettura considerata tra le più sicure è nota come Screened Subnet Architecture o rete Demilitarizzata (DMZ).

# Rappresentazione schematica di una screened subnet architecture

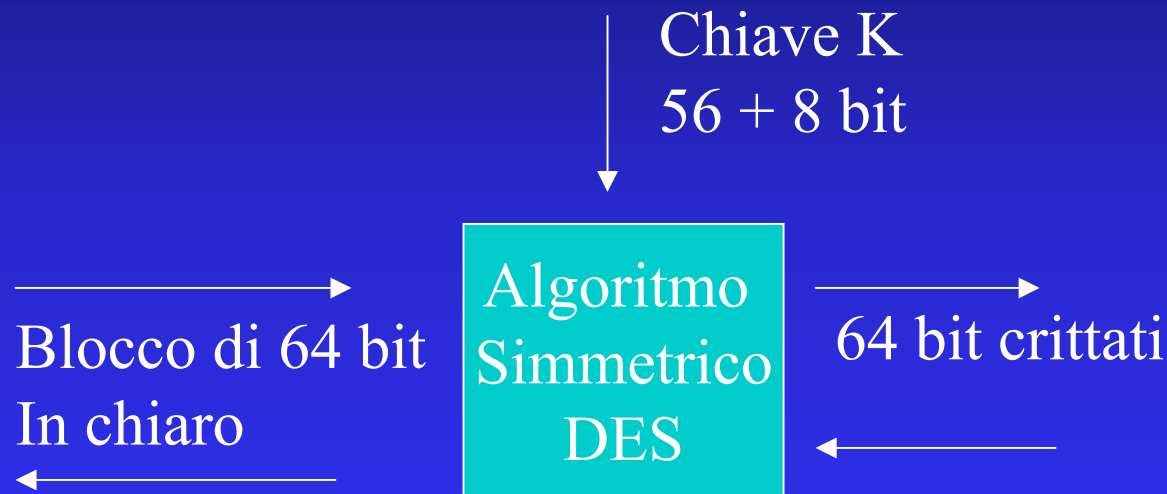


# Accorgimenti Tecnologici (5)

- Sistemi di monitoraggio e di tracciamento (raccolta ed analisi dei file di log);
- Uno degli strumenti di difesa delle informazioni dall'accesso indesiderato è quello della crittografia. Le forme principali sono:
  - ◆ **Crittografia simmetrica** si basa sullo standard DES (Data Encryption Standard), mittente e destinatario usano lo stesso algoritmo e la stessa chiave sia per la cifratura sia per la decodifica. Il testo in chiaro viene diviso in blocchi da 64 bit e successivamente spezzato in due da 32 bit che vengono permutati 16 volte con una chiave segreta di 56 bit effettivi (+ 8 bit per il controllo di parità). Oggi è anche presente il Triple DES con un keyspaces di 128 bit.

# Simmetria del DES

- algoritmo semplice basato su una combinazione di tecniche tradizionali di trasposizione e sostituzione



# Accorgimenti tecnologici (6)

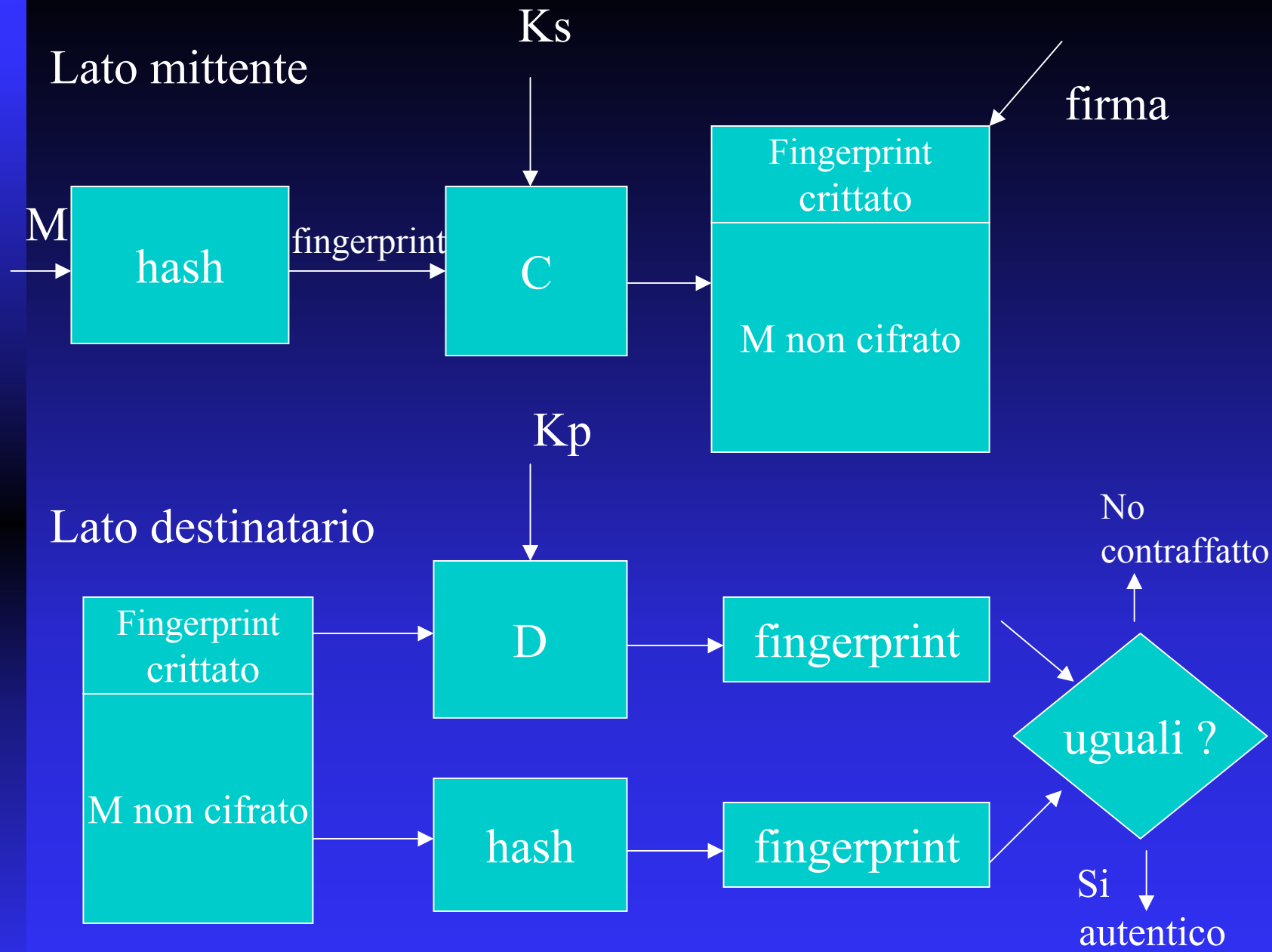
- ◆ **Crittografia asimmetrica** si basa sulla presenza di una coppia di chiavi (pubblica e privata). Questa forma di autenticazione garantisce il non ripudio e prevede la presenza di una CA (Certification Authority) che garantisce l'abbinamento identità personale-chiave pubblica ( $K_p$ ) assegnata attraverso il rilascio di un certificato digitale. La chiave privata ( $K_s$ ) deve essere custodita dal possessore, (una buona custodia è rappresentata dalle smart card). Gli algoritmi più noti sono:
  - ◆ Diffie-Hellman (ricercatori che lo hanno sviluppato nel 1976);
  - ◆ RSA (Rivest, Shamir e Adleman);

## Accorgimenti tecnologici (7)

- Una applicazione dei sistemi crittografici a chiavi pubbliche è la firma digitale. Il differente uso delle chiavi garantisce:
  - ◆ **la privacy.** La  $K_p$  (del destinatario) viene usata dal mittente per cifrare, mentre il destinatario usa la sua  $K_s$  per recuperare il messaggio  $M$ ;
  - ◆ **L'autenticazione del mittente** che codifica il messaggio ( $M$ ) con la propria  $K_s$ . Chiunque avendo accesso alla  $K_p$  può decodificare  $M$ , se ciò riesce si è sicuri sull'identità del mittente.

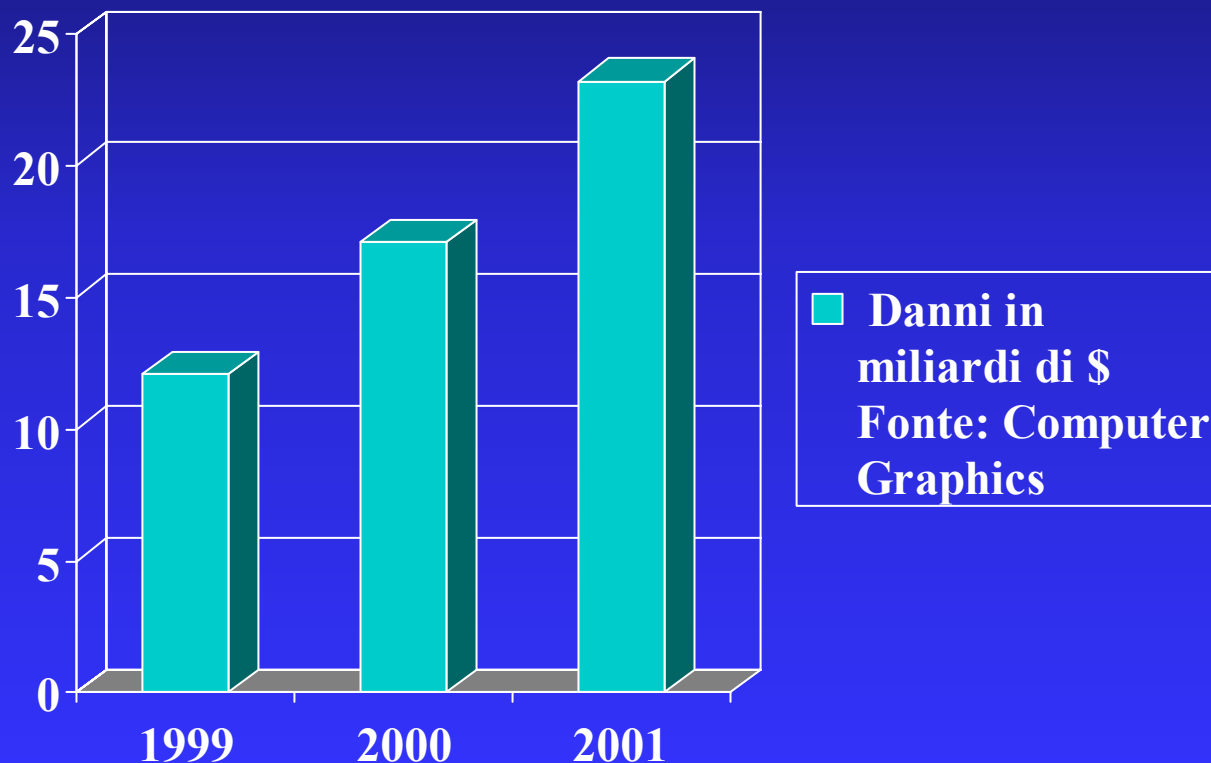
## Accorgimenti tecnologici (8)

- Nella firma digitale in realtà  $M$  non è in genere cifrato, viene invece firmato una sorta di “riassunto” ( $X$ ) detto anche “impronta” ottenuto con  $f(x)$  matematiche che rendono trascurabile la probabilità che una variazione del testo dia luogo alla stessa impronta.
- La normativa italiana conferisce ad un documento elettronico firmato digitalmente, la stessa valenza probatoria di un documento cartaceo munito di firma olografa.



# Accorgimenti tecnologici (10)

- **Sistema Antivirus** (meglio se il sistema di gestione è del tipo client/server con console centralizzata)
- **Impatto dei virus sui S.I. mondiali**



# Gli aspetti organizzativi

- Accanto alle misure tecnologiche precedentemente illustrate è necessario definire una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del Piano di Sicurezza, questi riguardano principalmente:
  1. L'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate : Piano di continuità, Verifica della Sicurezza attraverso :
    - a. *Monitoraggio delle misure di sicurezza;*
    - b. *Audit delle misure di sicurezza*
  2. La definizione di ruoli, compiti e responsabilità di tutte le fasi del processo di sicurezza.

# Gli aspetti organizzativi: ruoli principali

- *Gestore della sicurezza di rete (security manager).*
  - ◆ Ispeziona i log e le informazione derivanti dal sistema anti intrusioni (se attivo).
  - ◆ Adotta un sistema di filtering (basato su database o algoritmi intelligenti). Il fine è limitare il consumo di *banda passante* per fini non istituzionali.
  - ◆ Controlla la consistenza ed affidabilità degli apparati. Interviene nei progetti di estensione e di adeguamento tecnologico della rete.
- *Postmaster.*
  - ◆ Cura in particolare gli aspetti della sicurezza riferiti alla posta elettronica (gestione account, liste di distribuzione, e-mail all ecc).

# Gli aspetti organizzativi: ruoli principali

## ■ *Sistemista di rete (network manager).*

- ◆ Ha il compito di rendere il sistema operativo della rete rispondente alle esigenze della struttura (DNS, DHCP, server clustering ecc).
- ◆ Programma le politiche dei firewall e dei router.
- ◆ Applica gli aggiornamenti software ai sistemi operativi residenti sui server e al software delle apparecchiature.
- ◆ Predisporre il piano operativo del sistema di salvataggio dei dati (frequenza, ora, personale).
- ◆ Lavora in stretto contatto con il security manager.

# Verifica della sicurezza

- In un contesto tecnologico in continua evoluzione è necessario sottoporre a continua verifica la adeguatezza del Sistema di sicurezza realizzato. Ciò si ottiene attraverso due distinte attività:
  - ◆ *Monitoraggio delle misure di sicurezza;*
  - ◆ *Audit delle misure di sicurezza.*

# Monitoraggio delle misure di sicurezza

- Si concretizza in un controllo continuo delle misure adottate. Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log. Attraverso questa analisi (che nel caso di sistemi complessi deve essere effettuata con strumenti di automatici) è possibile individuare i tentativi di accesso al sistema e l'esecuzione di operazioni sospette.

# Verifica delle misure di sicurezza

- Sono test specifici che si effettuano con l'ausilio di moderni strumenti automatizzati di network scanning. È importante affiancare a queste attività una serie di attacchi di tipo intrusivo (test di penetrabilità). Tale verifiche che vengono indicate come *audit di sicurezza* debbono essere svolte, a differenza delle attività di monitoraggio, da personale che non abbia responsabilità di gestione del sistema di sicurezza oggetto della verifica (meglio se in *outsourcing*). Gli audit di sicurezza debbono essere eseguiti secondo il rispetto di un piano formale che comprenda fasi ben individuate.

# Audit di sicurezza

- Preparazione.
- Audit.
- Report.
- Azioni correttive.

# Audit di sicurezza fase 1 : preparazione

- In questa fase è consigliabile rivedere la consistenza delle scelte iniziali delle Politiche di Sicurezza. Queste dovrebbero contenere l'indicazione della periodicità dell'Audit (una buona regola è l'annualità).
- È indispensabile avere il consenso da tutti i responsabili dei settori interessati all'Audit, facendo attenzione ad evitare gli orari in cui l'attività del sistema è più intensa.
- Per quanto riguarda “l'oggetto” in genere ci si rivolge a tre categorie: host, network, firewall.
- Scegliere un tool che abbia una rappresentazione grafica intuitiva e una buona reportistica. Gli strumenti sono di due categorie: manager/agente e scanner di rete.

## Audit di sicurezza fase 2 : l'auditing

- Si procede con il test vero e proprio (audit tecnico) e si effettuano interviste con il personale per verificare la conoscenza ed il rispetto delle regole previste dalle *policies* (audit non tecnico).
- Anomalie da ricercare:
  - ◆ Tentativi multipli di accesso falliti;
  - ◆ Stesso utente che accede da postazioni diverse;
  - ◆ Attività fuori orario.

## Audit di sicurezza fase 3 : report

- La quantità di dati generata può essere rilevante anche se il numero di nodi testati è basso (<20). I dati raccolti devono essere analizzati con molta cura dagli amministratori di rete e della sicurezza.

## Audit di sicurezza fase 4 : azioni.

- Inserire tutte le nuove informazioni nell'analisi dei rischi e nel protocollo di sicurezza. Ricordarsi sempre che la sicurezza è un processo continuo.

# Formazione e coinvolgimento

- Generalmente l'alta dirigenza costituisce l'ostacolo principale per la realizzazione di un Piano per la Sicurezza. Fare comprendere ed accettare ai vertici aziendali un progetto per la sicurezza informatica è impresa non semplice.
- La **formazione** assume quindi un **valore strategico**. Ne saranno fruitori due diverse tipologie di utenti:
  - ◆ *I Dirigenti* al fine di diffondere una consapevolezza ampia delle problematiche della sicurezza. I corsi conterranno cenni sulla normativa, definizione delle responsabilità, l'analisi dei rischi e dei costi.
  - ◆ *Il personale operativo* che dovrà conoscere le operazioni da svolgere quotidianamente e i comportamenti da intraprendere in caso di emergenza (gestione degli accessi, virus, intrusioni ecc).

## Formazione e coinvolgimento (2)

- Le politiche di sicurezza non rappresentano un carico delle attività, ma contribuiscono a garantire il personale dal rischio di perdere in parte o tutto il lavoro fatto. E la formazione può costituire la chiave di volta per la loro diffusione e per *minimizzare la resistenza al cambiamento* che è sempre presente quando si debbono introdurre nuove regole che inducono cambiamenti comportamentali nei processi lavorativi.
- È inoltre importante rivedere i piani di formazione in relazione allo sviluppo della tecnologia e alle mutate esigenze aziendali.

# Qualità del Servizio, Costi e Sicurezza (1)

- Per ridurre l'impatto sulla sicurezza, un'organizzazione può intraprendere due iniziative:
  - ◆ **Riduzione** del valore esposto alle violazioni di sicurezza;
  - ◆ **Implementazione** di misure di sicurezza sempre più efficaci.
- La prima iniziativa non può che offrire margini limitati di azione.
- Più che ridurre il valore, è possibile ridurne (limitatamente) l'esposizione. Ad esempio, una diffusione controllata delle informazioni tra i dipendenti, può, permettere di preservarle meglio da attacchi. L'azione è limitata dalla attività lavorativa stessa, non si può pensare di evitare completamente i rischi: un negozio è soggetto a rapine, ma se lo chiudo non vendo più nulla.

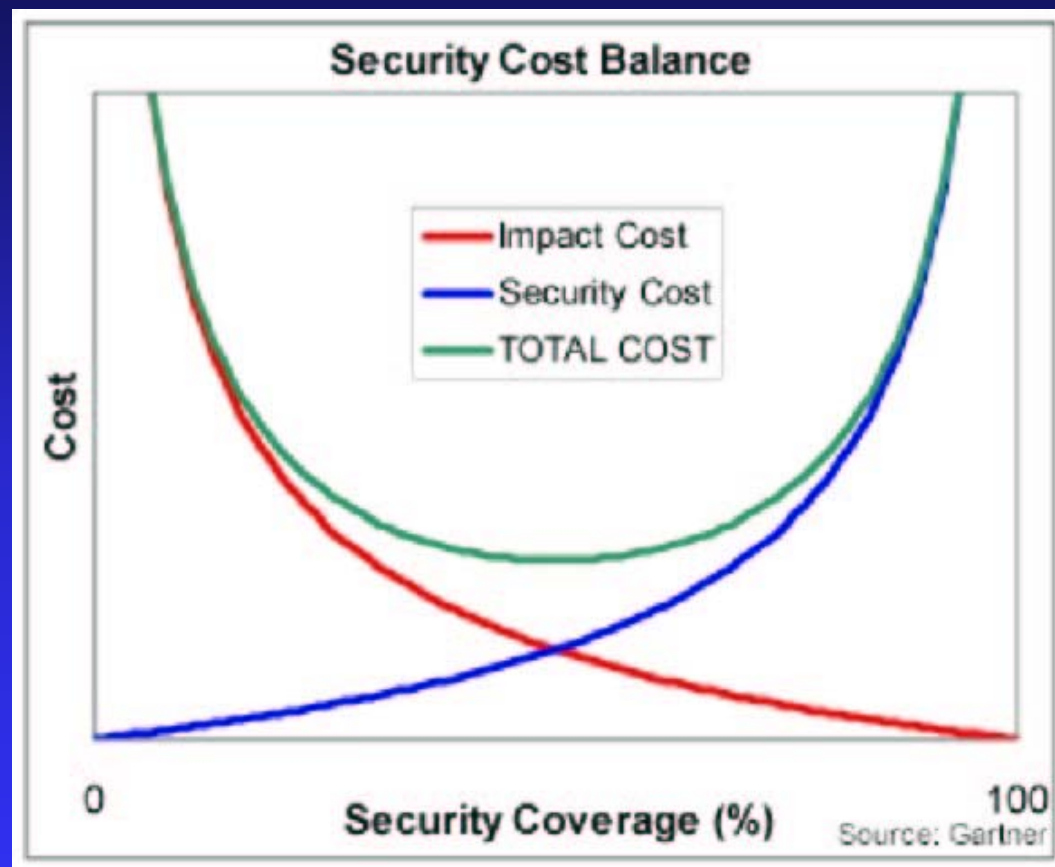
## Qualità del Servizio, Costi e Sicurezza (2)

- La seconda iniziativa mira all'adozione di misure di sicurezza, per una riduzione significativa del rischio è necessaria la realizzazione di un piano di sicurezza calibrato sulla realtà della specifica organizzazione e sul mantenimento di standard minimi di QoS che si vogliono offrire.
- La riduzione dell'impatto sulla sicurezza non cresce linearmente con l'incremento degli sforzi profusi nell'allestimento di misure di sicurezza.
- Le prime misure di sicurezza intraprese da un'organizzazione saranno più efficaci in termini di riduzione dell'impatto.
- Man mano che gli investimenti aumenteranno, sarà sempre più difficile ottenere ulteriori miglioramenti.

## Qualità del Servizio, Costi e Sicurezza (3)

- Un piano di sicurezza perfetto avrebbe un costo infinito e non costituisce quindi una strategia praticabile. Quella che ogni organizzazione deve individuare è la situazione di compromesso migliore tra entità degli sforzi effettuati ed efficacia dell'azione intrapresa. Tale posizione di compromesso rappresenta la situazione nella quale si ottiene il costo complessivo minore.
- Una volta analizzati il livello di rischio, il valore esposto dall'organizzazione, e l'impatto risultante, sarà possibile identificare le aree d'azione più critiche. Da queste sarà necessario iniziare, per intraprendere immediate azioni correttive.

# Diagramma rapporto costo/sicurezza



# Conclusioni

- La sempre maggior presenza di applicazioni distribuite in rete richiede un approccio sistemico al problema della sicurezza.
- Il sistema di sicurezza va mantenuto sempre aggiornato.
- Sempre più ingenti sono gli investimenti effettuati dalle aziende nel settore della sicurezza.
- Una interruzione di un servizio dovuta ad una intrusione, oltre ai problemi legati alla perdita d'immagine, può provocare seri danni non quantificabili a priori.

Schema di protezione presso l'Istituto Superiore di Sanità

