

Classificazione dei servizi in funzione dei requisiti di sicurezza



Il progetto di sicurezza di un sistema di servizi



Requisiti

Individuare con precisione

- Ruolo degli operatori
- Responsabilità degli utilizzatori
- Operatività sulle informazioni
- Sensibilità dei dati



I vincoli

Tenere sempre presente

- L'offerta del mercato
- La normativa vigente
- L'organizzazione esistente
- La complessità del servizio da erogare



Le funzionalità operative

Fermo restando il precedente percorso metodologico che consente di individuare i ruoli delle persone, le tipologie di dati, i vincoli di carattere tecnologico e normativo, le operatività che si possono considerare sono:

- decisionale
- progettazione
- controllo
- applicazione



Regole elementari

Applicare una netta separazione tra

- chi produce i dati e chi deve fornirli
- chi progetta il sistema di sicurezza e chi lo realizza
- chi realizza il sistema di sicurezza e chi ne fa auditing

	decisione	progettazione	controllo	applicazione
manager	X			
organizzativo		X	X	
tecnologico		X	X	
fruitore				X



Gli attori

I principali attori di un sistema di servizi sono:

- Ente/amministrazione/azienda (possessore del servizio)
- Cittadino/altro ente (fruitore del servizio)
- Risorsa informatica/applicazione



Le relazioni

Le principali relazioni tra gli attori sono:

- Ente erogatore/Ente erogatore
- Ente erogatore/Ente fruitore
- Ente erogatore/cittadino fruitore



Le tipologie di accesso al servizio

L'accesso alle informazioni può essere:

- **Libero:** qualsiasi entità può accedere a qualsiasi dato senza restrizioni alcune
- **Identificato:** qualsiasi entità, previa identificazione, può accedere a qualsiasi dato senza restrizioni alcune
- **Autenticato:** qualsiasi entità può accedere, previa autenticazione, a qualsiasi dato senza restrizioni alcune
- **Controllato:** qualsiasi entità precedentemente identificata ed autenticata può accedere a dati soggetti a restrizioni (lettura, scrittura, ...)
- **Non ripudiabile:** l'entità precedentemente autenticata, effettua delle operazioni sui dati che non può negare al completamento della transazione.
- **Segretato:** lo scambio di informazioni tra il richiedente ed il servizio è oggetto di crittografia.



Le operatività sui dati

Le azioni che si possono intraprendere sulle informazioni sono:

- inserimento
- aggiornamento
- cancellazione
- interrogazione



La sensibilità delle informazioni

Le informazioni possono essere classificate come:

- **Conoscibili da chiunque:** *l'informazione può essere fornita a chiunque*
- **A conoscenza circoscritta:** *l'informazione può essere fornita solo a chi è stato identificato/autenticato*
- **Ai sensi della legge 675/96 o altra norma:** *l'informazione può essere fornita solo a chi ne è stato autorizzato dal proprietario*
- **Proprietarie:** *dati proprietari visibili al massimo all'interno di una Intranet.*
- **Sensibili:** *dati proprietari visibili solo dal proprietario e dalle persone che svolgono un ruolo sociale particolare (medici, polizia, ...)*



Il modello

Risulta a questo punto naturale il seguente modello:

24-11-03 10:30 AM - 30-NA-07 - 30-NA-07 - 30-NA-07 - 30-NA-07

	Accesso libero	Identificato	Autenticato	Controllato	Non ripudiabile	Crittografato
Ente/azienda						
Cittadino						
Risorsa						
Ente erog.re/ente erog.re						
Ente erog.re/ente fruitore						
Ente erog.re/cittadino						
Inserimento						
Aggiornamento						
Cancellazione						
Interrogazione						
Conoscibile da chiunque						
Conoscenza circoscritta						
Ai sensi L. 675 o altra norma						
Proprietarie						
Sensibili						



Il fattore umano

**UNA MACCHINA, DI PER SE', E' INNOCUA:
E' L'UOMO CHE LA RENDE PERICOLOSA.
UNA MACCHINA, DI PER SE', NON FUNZIONA:
E' L'UOMO CHE LA FA FUNZIONARE.**

Perciò vale il detto: se conosci il nemico e conosci te stesso, non devi temere il risultato di cento battaglie. Se conosci te stesso ma non il nemico, per ogni vittoria ottenuta potrai subire anche una sconfitta. Se non conosci nè il nemico nè te stesso, soccomberai in ogni battaglia.

(Sun Zi Bing Fa)



Sviluppo del modello

- ◆ analisi del contesto
- ◆ piano di attuazione (pianificazione)
- ◆ valutazione aspetti organizzativi
- ◆ valutazione aspetti tecnologici
- ◆ modalità di revisione



Analisi del progetto

■ Compilazione del modello

- ➔ Individuazione degli attori
- ➔ Individuazione della tipologia di interazione
- ➔ Individuazione delle operatività sui dati
- ➔ Individuazione della tipologia dei dati



Piano di attuazione

- ◆ priorità di protezione
- ◆ tempi di attuazione
- ◆ ricaduta sugli aspetti organizzativi
- ◆ ricaduta sugli strumenti
- ◆ ricaduta sugli aspetti tecnologici



Aspetti organizzativi

Il concetto base che deve guidare l'individuazione della struttura organizzativa della sicurezza è la suddivisione delle responsabilità: ogni funzione deve essere ben definita e non possono esistere sovrapposizioni (principio della delega).

Ogni attività comportante rischio, inoltre, deve essere suddivisa tra più figure, in tal modo per effettuare malversazioni si rende necessaria la collaborazione di almeno due persone.

***IN BASE ALLE PRECEDENTI CONSIDERAZIONI, È
INDISPENSABILE CHE I GESTORI DELLE FUNZIONI DI
SICUREZZA SIANO NETTAMENTE DISTINTI DAI GESTORI
DELLE APPLICAZIONI E DAI CONTROLLORI.***



Aspetti organizzativi

- ◆ minimo stravolgimento dell'esistente
- ◆ individuazione delle funzioni coinvolte
(operative e di controllo)
- ◆ variazione dell'operatività
- ◆ normativa operativa



Aspetti tecnologici

- ◆ minimo stravolgimento dell'esistente
- ◆ individuazione degli strumenti
(operativi e di controllo)
- ◆ variazione dell'operatività
- ◆ normativa tecnica



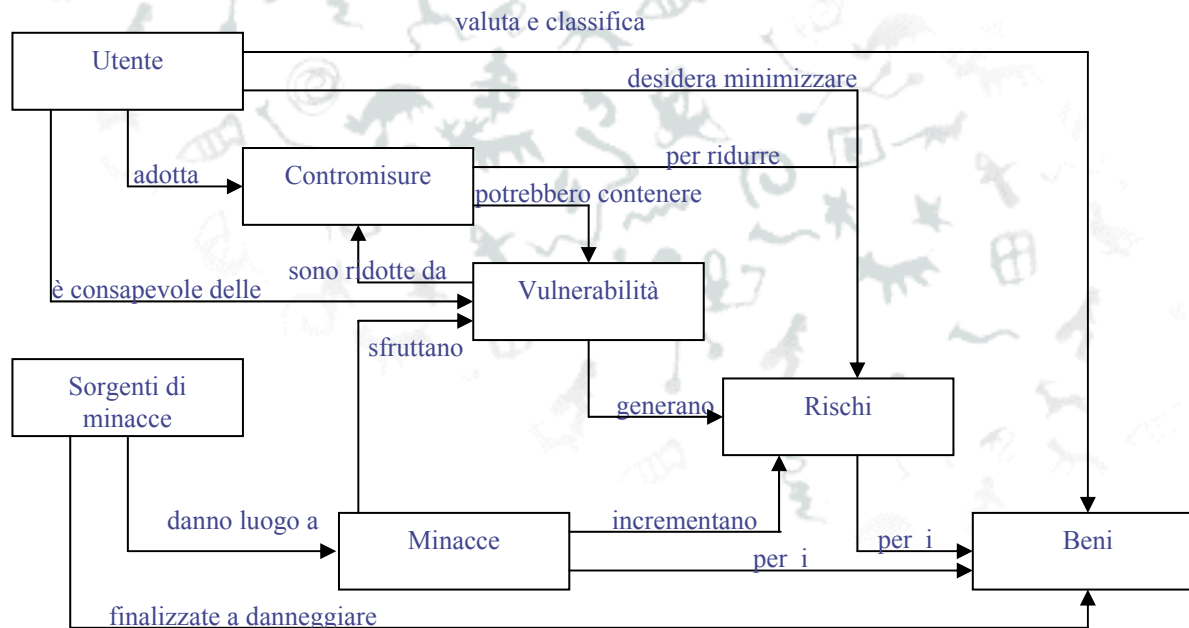
Revisione

- revisioni periodiche
- revisioni a seguito di modifiche
 - ◆ tecnologiche
 - ◆ organizzative
 - ◆ legali
 - ◆ contrattuali
 - ◆ assicurative



Lo scenario previsto

Il seguente schema rappresenta lo scenario tipico di un progetto di sicurezza:





Le attività

L'articolazione progettuale del piano di sicurezza prevede le seguenti fasi:

1. l'analisi del rischio,
2. la definizione della policy di sicurezza,
3. la gestione del rischio,
4. il piano operativo,
5. il controllo della sicurezza o audit,
6. la formazione delle risorse umane,
7. l'organizzazione a supporto



1- Attività: analisi del rischio

è la fase il cui obiettivo principale è quello di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio sistema informativo, nonché quello di avere una primissima stima delle contromisure da adottare. Essa prevede cinque sottofasi:

- ❑ il censimento del patrimonio informativo (asest),
- ❑ la classificazione dei beni,
- ❑ la valutazione della minacce,
- ❑ l'individuazione dell'esposizione al rischio,
- ❑ le contromisure da adottare.

1.1 censimento dei beni (assest)

Prevede l'identificazione delle risorse coinvolte nel piano di sicurezza. Si possono individuare le seguenti categorie di risorse (in accordo con la RFC 2196):

Tipo risorsa	descrizione	vulnerabilità e minacce possibili
hardware	CPU, terminali, PC, stampanti, dischi, dispositivi di rete, linee di comunicazione	malfunzionamenti <input type="checkbox"/> naturali, <input type="checkbox"/> dolosi.
software	di base e applicativi	malfunzionamenti <input type="checkbox"/> naturali, <input type="checkbox"/> dolosi (virus, cavalli di troia, ...), <input type="checkbox"/> <i>denial of service</i> per saturare la capacità di risposta di un servizio
dati	contenuto degli archivi, dati di transito, copie storiche, file di log	<input type="checkbox"/> visualizzazione non autorizzata, <input type="checkbox"/> modifica o cancellazione non autorizzata.
risorse professionali	operatori ed utenti del sistema informativo	<input type="checkbox"/> attacchi esterni e costringenti alle risorse, <input type="checkbox"/> ignoranza sull'utilizzo del sistema, <input type="checkbox"/> rivalse nei confronti dell'amministrazione
documenti cartacei	ogni sorta di documentazione afferente il sistema informativo	distruzione o alterazione: <input type="checkbox"/> naturale, <input type="checkbox"/> intenzionale.
supporti di memorizzazione	le copie di backup	distruzione o alterazione: <input type="checkbox"/> naturale, <input type="checkbox"/> intenzionale. evoluzione tecnologica e di mercato.



1.2 classificazione dei beni

Una volta individuato il contesto del progetto sicurezza, è bene classificare le risorse in funzione delle caratteristiche di:

- ❑ **riservatezza**, che si ottiene impedendo che le informazioni siano rivelate senza autorizzazione;
- ❑ **integrità**, che si ottiene impedendo che le informazioni siano modificate senza autorizzazione;
- ❑ **disponibilità**, che si ottiene impedendo che l'accesso alle informazioni o alle risorse sia negato senza autorizzazione.

Per soddisfare tali requisiti occorre implementare diverse misure tecniche di sicurezza riguardanti, ad esempio, settori quali il controllo di accesso, l'audit e il recupero da errore in base a principi **quantitativi** (essenzialmente costi, come per esempio costi di ripristino, costi di soluzioni alternative, ...) e **qualitativi**, come per esempio:

- ❑ rischio per la sicurezza dello Stato/cittadini,
- ❑ interruzione di pubblico servizio,
- ❑ alterazione di pubblico servizio,
- ❑ sottrazione o danneggiamento di patrimonio pubblico, perdita di immagine.



1.3 Valutazione delle minacce

Le minacce si possono categorizzare o in base alle tecniche utilizzate per condurre l'attacco, o in base alle caratteristiche architettoniche del sistema informativo.

1.3.1 Tecniche di attacco: a livello fisico



Il progetto di
sicurezza di
sistema di ser

In questa categoria rientrano attacchi **deliberati** o **intenzionali**:

- ❑ attacchi a livello **fisico**, rivolti a danneggiare o sottrarre risorse fisiche critiche per il sistema informativo. Rientrano in questa categoria il furto o danneggiamento come attacco alla disponibilità ed alla riservatezza;



1.3.2 Minacce a livello logico

- attacchi a livello **logico**, rivolti a sottrarre o danneggiare informazioni o a degradare le prestazioni del sistema; in questa categoria rientrano:
 - attacchi di **intercettazione** (attacco alla *riservatezza*) che sfruttano debolezze del sistema operativo o di configurazione di protocolli o di apparati di rete. Si possono menzionare:
 - **sniffing**: analisi del traffico di rete,
 - **spoofing**: server pirata che si spacciano per router,
 - **programmi di simulazione** per la fase di identificazione ed autenticazione dell'utente per carpirne l'identità;



1.3.3 Minacce a livello logico

- § attacchi di **deduzione** (attacco alla *riservatezza*), che si ottengono combinando delle informazioni ottenute in vario modo come per esempio analizzando componenti di sistema che singolarmente sono state configurate come poco riservate;
- § attacchi di **intrusione** (attacco alla *riservatezza ed integrità*), sono quelli che si ottengono attraverso programmi generatori di password o sfruttando buchi del sistema operativo della sua configurazione con particolare riferimento ai protocolli di rete. Tipico è il caso del meccanismo **backdoor**, che su sistemi Unix permette di avere dei privilegi di administrator anche quando la password di administrator viene cambiata. Un altro meccanismo è quello dei programmi **cavallo di Troia**, cioè di file eseguibili che si propongono all'utente con funzionalità innocue come cartoline di auguri o messaggi lusinghieri;
- § attacchi di **disturbo** o **worm** (attacco alla *disponibilità*), finalizzati a degradare le prestazioni del sistema, per esempio creando molte istanze di un certo processo fino a congestionare il sistema. Particolarmente usati su sistemi batch, in cui la rilevazione del danno si può prorarre nel tempo;
- § **virus** (attacco alla *riservatezza ed integrità*). Si tratta di programmi auto replicanti spesso inseriti come cavalli di Troia;
- § **denial of service** (attacco alla *disponibilità*), rivolti a negare l'accesso anche agli utenti che ne avrebbero diritto. Un tipico esempio è quello di paralizzare la rete con messaggi di errore o simulazioni di accesso.

1.3.4 Attacchi alla architettura del sistema

Disegno e architettura di sistema

Sono riconducibili a questa categoria minacce dovute al disegno o all'architettura del sistema:

Univocità: un sistema unico, come per esempio un sistema legacy, presenta forti criticità di sicurezza.

Singularità: come la possibilità di condurre un attacco a causa delle caratteristiche altamente specifiche del sistema (per esempio un sistema basato su comunicazione satellitare).

Centralizzazione: come la possibilità di condurre un attacco in un unico nodo o processo.

Separabilità: in relazione ad una strategia di attacco di tipo "dividi e conquista".

Omogeneità: se un sistema ha delle componenti omogenee, l'attacco condotto ad un suo modulo è potenzialmente riconducibile a tutti le sue componenti.

1.3.5 Attacchi al comportamento del sistema

Sensitività: come possibilità di condurre un attacco in procedure operative o strutturali dove il sistema è meno efficiente.

Prevedibilità: come la possibilità di condurre un attacco basato su un comportamento noto e prevedibile del sistema.

1.3.6 Attacchi al caratteristiche del sistema



Il progetto di sicurezza di un sistema di ser

Adattamento e alterazione

Sono riconducibili a questa categoria minacce dovute alla facilità di cambiare le caratteristiche del sistema:

Rigidità: come l'impossibilità a difendersi da un attacco.

Malleabilità: come la facilità di simulare una modifica del sistema.

Ingenuità: come la difficoltà, da parte del sistema, a distinguere un attacco da un utilizzo lecito.

1.3.7 Attacchi alla configurazione del sistema

Configurazione

Sono riconducibili a questa categoria minacce dovute alla modalità di configurazione o di gestione di un particolare processo del sistema.

Limiti di capacità: come l'impossibilità a difendersi da un attacco quando il sistema lavora vicino alle sue capacità limite (e quindi in condizioni di stress).

Impossibilità di ripristino: come inibizione delle modalità di ripristino del sistema.

Mancanza di auto-consapevolezza: come impossibilità di tenere traccia o di monitorare il sistema.

Difficoltà di gestione: aggiornamenti periodici o frequenti delle configurazioni del sistema offrono occasioni di attacco.

Facilità di utilizzo: l'uso eccessivo di interfacce semplici di dialogo introducono la possibilità che il sistema possa essere utilizzato da personale non competente.

1.3.8 Attacchi alla esposizione del sistema

Esposizione remota del sistema

Sono riconducibili a questa categoria minacce dovute alla possibilità di fruire in maniera remota del sistema.

Accessibilità: la possibilità di connettersi in maniera remota introduce elementi di probabile attacco.

Trasparenza: più un sistema è aperto a procedure pubbliche più è semplice da attaccare.

1.3.9 Attacchi alla esposizione del sistema

Esposizione fisica del sistema

Sono riconducibili a questa categoria minacce dovute alla possibilità di attaccare il sistema in maniera fisica o tramite interazioni dirette.

Accessibilità fisica: intesa come la possibilità di usare direttamente le risorse del sistema.

Sensibilità elettromagnetica: come la possibilità di essere attaccati attraverso l'uso di radiazioni o fenomeni elettromagnetici.

Dipendenza: intesa come la diretta dipendenza del sistema da infrastrutture fisiche facilmente attaccabili.



1.4 Esposizione al rischio

Si tratta di misurare il rischio a cui è sottoposto il sistema informativo in funzione della combinazione tra:

- ❑ valore del bene,
- ❑ livello della minaccia,
- ❑ livello di vulnerabilità alla minaccia.



1.5 Contromisure

Si intendono contromisure tutte quelle azioni rivolte a minimizzare la possibilità di un attacco deliberato o accidentale o comunque a minimizzare i danni causati da un possibile attacco. Una delle tecniche più efficaci per individuare le contromisure, consiste nell'affiancare ad ogni tipologia di attacco, la sua specifica azione di contrattacco. Le contromisure si possono distinguere in:

- ❑ **preventive**, tese a rendere improbabile l'attacco;
- ❑ **correttive**, finalizzate a limitare i danni di un attacco avvenuto in barba alle contromisure preventive;
- ❑ **informatiche** o **organizzative**, se coinvolgono aspetti prettamente informatici o di tipo organizzativo - procedurale. Tra le principali contromisure di carattere informatico si possono annoverare quelle a carattere applicativo, molto cogenti, ma che riguardano un sottoinsieme specifico di utenti che è quello che utilizza l'applicazione, e quelle a carattere generale introdotte attraverso la configurazione dei file di sistema preposti alla funzioni di sicurezza. Tra le principali azioni di carattere organizzativo sono da annoverare i corsi di addestramento ovvero i processi di sensibilizzazione del personale. Sicuramente rientrano in questo tipo di contromisure la definizione di una struttura della sicurezza con la relativa definizione di ruoli, responsabilità e competenze, con particolare riferimento a chi individua la policy di sicurezza e chi deve controllarne la sua applicazione.
- ❑ a livello **fisico** o **logico**, se rivolte a contrastare attacchi di tipo fisico o logico.



2 Definizione policy di sicurezza

È la fase in cui si definiscono gli obiettivi di sicurezza dell'amministrazione: si tratta di tradurre l'analisi dei rischi in contromisure informatiche ed organizzative atte a garantire i livelli di sicurezza ritenuti validi in funzione dei costi necessari ad adottare una certa policy e dei risultati di sicurezza che questa policy garantisce.

2.1 Aspetti minimali della policy di sicurezza



- la **classificazione** della documentazione, per individuare quali informazioni si devono ritenere segrete, riservate, ristrette o di dominio pubblico;
 - la **protezione fisica** delle risorse, con la relativa
 - .. classificazione delle aree aziendali, delle modalità di accesso alle stesse,
 - .. definizione delle misure di sicurezza e di vigilanza degli impianti
 - .. definizione degli strumenti e delle modalità di rilevazione degli incidenti;
 - la **protezione logica** delle risorse, in termini di:
 - .. tecniche di **identificazione**, **autenticazione** e di **autorizzazione** ai dati ed ai servizi,
 - .. modalità di **crittografia** delle informazioni che lo richiedono,
 - .. **protezione** e **personalizzazione** del sw di base e dei file di configurazione,
 - .. modalità di registrazione, consultazione e conservazione dei file di **log**,
 - .. strumenti di individuazione **intrusioni**;
 - l'**organizzazione** a supporto con la netta separazione tra chi detta le regole per la sicurezza e chi ne deve controllare la corretta applicazione. Devono essere specificati ruoli, responsabilità e compiti di ogni figura professionale coinvolta;
 - le norme **comportamentali** del personale, in termini di utilizzo ed aggiornamento delle risorse del sistema, nonché le procedure di sensibilizzazione e formazione del personale
 - il piano di **ripristino** del sistema, in caso di malfunzionamenti
- lo **sviluppo** e l'aggiornamento delle risorse, in termini di procedure da utilizzare per lo sviluppo del sw, la messa in produzione, l'aggiornamento delle versioni, la distribuzione della patch e le modalità di sostituzione o riparazione degli apparati.



3 Gestione del rischio

La fase, detta anche Risk management, consiste nella valutazione dei rischi da abbattere e in quella dei rischi da ritenersi accettabili. La ponderazione tra i **costi della sicurezza** e quelli della **non sicurezza** e quindi la valutazione del rapporto costo/benefici, è alla base della gestione del rischio, i cui obiettivi sono a completa responsabilità del direttivo dell'amministrazione. Il costo individuato per ogni tipo di contromisura ad un probabile attacco, deve tenere presenti sia i costi iniziali di implementazione, che dei costi di esercizio e di manutenzione annuale. Un probabile schema di gestione del rischio potrebbe essere il seguente:

Rischio o attacco	soluzione o contromisura	% di efficacia	costo iniziale	costo di esercizio	impatto organizzativo
-------------------	--------------------------	----------------	----------------	--------------------	-----------------------

4 Piano operativo

Individuate le risorse da proteggere, la natura dei possibili attacchi (fase di **analisi del rischio**), le contromisure da adottare (fase di definizione della **policy di sicurezza**), ed il livello di rischio ritenuto accettabile (fase di **gestione del rischio**), è necessario redigere il piano operativo della sicurezza che descrive:

- ❑ le **funzioni** di sicurezza da implementare in funzione dei diversi beni,
- ❑ i **meccanismi** e gli strumenti utilizzati all'interno delle diverse soluzioni,
- ❑ la collocazione della soluzione all'interno **dell'architettura** del sistema informativo,
- ❑ il **piano temporale** di realizzazione,
- ❑ le correlazioni e le **dipendenze** tra le soluzioni,
- ❑ le **alternative** alle soluzioni individuate,
- ❑ le **risorse** e la struttura organizzativa di supporto.



4.1 Piano operativo: operazioni

Le **funzioni** minime da prevedere sono (a norma ISO):

- ❑ autenticazione,
- ❑ controllo degli accessi,
- ❑ riservatezza,
- ❑ integrità,
- ❑ non ripudio.



4.2 Piano operativo: strumenti

Gli strumenti da utilizzare (sempre a norma ISO) sono:

- ❑ cifratura,
- ❑ firma digitale,
- ❑ meccanismi per il controllo degli accessi,
- ❑ funzioni di hash,
- ❑ saturazione del traffico,
- ❑ controllo degli instradamenti,
- ❑ notarizzazione.



5 Verifica della sicurezza

Questa fase prevede la verifica del raggiungimento degli obiettivi di sicurezza (e dei relativi livelli di qualità) definiti nella policy, nei tempi previsti, con l'organizzazione costituita e con i costi stimati durante le fasi di analisi.

Due sono le azioni previste:

- **monitoraggio**: effettuato da chi ha definito le policy di sicurezza e finalizzato al controllo dell'efficacia delle soluzioni adottate e all'aggiornamento delle policy in funzione dell'evoluzione del panorama delle minacce possibili. È una attività continua basata sull'analisi e le statistiche dei file di log;
- **audit**: è una funzione ispettiva, saltuaria, non programmata, effettuata da una struttura esterna a quella del monitoraggio e finalizzata a verificare la robustezza delle policy di sicurezza. Test di penetrabilità, simulazioni di attacco, consulenza da parte di ethical hackers sono alcuni strumenti da utilizzare per le attività di auditing che producono sia una documentazione di quanto riscontrato (report) che documentazione sulle azioni da intraprendere per risolvere i problemi riscontrati.



6 Formazione e sensibilizzazione

Il problema della sicurezza è anche un problema sociale e culturale!

Seminari, coinvolgimento a tutti i diversi livelli sulle tematiche della sicurezza sono alla base della buona riuscita del piano della sicurezza adottato. Un generico piano di formazione dovrebbe tenere presente almeno i seguenti aspetti:

- 1) il contesto normativo,
- 2) la definizione delle responsabilità,
- 3) la descrizione di tutte le possibili minacce e delle principali contromisure adottate,
- 4) la descrizione delle soluzioni di identificazione, autenticazione e di autorizzazione,
- 5) la descrizione di particolari strumenti adottati quali la firma digitale, la sensibilizzazione alle tecniche di auditing.



7 Organizzazione a supporto

Dal punto di vista organizzativo, tre sono i momenti da prevedere:

- la definizione della politica di sicurezza, attività di pertinenza del direttivo dell'amministrazione,
- la progettazione, l'implementazione e la manutenzione del piano di sicurezza,
- il controllo dell'efficacia delle scelte individuate.

