TECNOLOGIE PER LA SICUREZZA E PRIVATEZZA – a.a. 2012/2013

GESTIONE DELLA SICUREZZA DI INFORMAZIONI

Salvatore Fresta

La sicurezza non comprende solo aspetti di tipo tecnologico ma anche **gestionale**. Dal punto di vista gestionale, la sicurezza racchiude in sé 6 caratteristiche principali note come le **sei P**:

1. PIANIFICAZIONE

Sono tutte quelle **attività necessarie per pianificare, creare e realizzare delle strategie** all'interno di un sistema. L'obiettivo primario è quello di realizzare diverse tipologie di piani da utilizzare a fronte di diversi eventi:

- Risposta agli incidenti (**incident response**)
- Recupero da disastri (**disaster recovery**)
- Gestione dei rischi (**risk management**)
- **Addestramento del personale** ecc..

2. POLITICHE

Sono delle **linee guida che stabiliscono i comportamenti** di un'organizzazione che possono avere un impatto sulla sicurezza.

3. PROGRAMMI

Programmazione di misure di sicurezza logiche e fisiche. Anche l'elemento umano è fondamentale e non può essere trascurato (programmi di addestramento).

4. PROTEZIONE

Le risorse non hanno tutte la stessa importanza e non sono sottoposte alle stesse minacce, per cui occorre un'**analisi per verificare il grado di sicurezza da adottare** in termini di tecnologie, meccanismi di protezione e dispositivi.

5. PERSONE

La sicurezza può essere minacciata anche dal personale che lavora dall'interno, per questo motivo occorre prestare attenzione al ruolo da assegnare ad ogni persona ed i rapporti che questi hanno con l'azienda, al fine da non creare i presupposti che spingono un impiegato a schierarsi contro la società.

6. PROJECT MANAGEMENT

È una disciplina del programma di sicurezza il cui obiettivo è **controllare le risorse utilizzate nel progetto, misurare i progressi ed aggiustare il processo** non appena si hanno progressi verso l'obiettivo del progetto stesso.

PIANIFICAZIONE DELLA SICUREZZA

La sicurezza di un sistema si ottiene applicando un processo i cui obiettivi principali sono:

- **identificare le risorse da proteggere** (**asset identification**): hardware, software, dati, persone, ecc..

- **determinare le minacce alla sicurezza** (**threat assessment**): violazione di confidenzialità/integrità/disponbilità

- **calcolare la probabilità che una minaccia si realizzi** (**risk assessment**): identificare le aree di rischio, valutare il rischio, sviluppare ed applicare un piano per la gestione del rischio e rivalutare nuovamente il rischio.

Dopo di che si stabiliscono delle **politiche di sicurezza** per diminuire il rischio di una minaccia, dei **piani di sicurezza** che le realizzano ed infine si avvia un **processo di audit** per constatare il livello corrente di sicurezza offerto dal sistema, testarlo ed eventualmente migliorarlo.

I **parametri fondamentali** della **fase di risk assessment** sono:

- **Risk likelihood**: calcola la **probabilità che una minaccia si concretizzi in un attacco**. Tale valore si può calcolare col **calcolo classico delle probabilità** (approccio teorico che richiede un modello che non sempre è possibile), con la **frequenza relativa** (quindi un approccio basato su **osservazioni** che possono essere già presenti nel sistema) o con la **probabilità soggettiva** (approccio sul **giudizio di un'analista esperto** che indica delle probabilità sulla base di un sistema simile)

- **Risk impact**: calcola il **costo dell'attacco** (costo di hardware, software, aspetti legali, immagine aziendale ecc..), anche in termini di perdite

- **Risk exposure**: Risk likelihood * Risk impact

- **Risk control**: indica il **grado di controllo atto ad eliminare o ridurre l'impatto** (ad esempio i meccanismi di sicurezza)

Il rischio può essere ridotto evitandolo (ad esempio cambiando i requisiti di sicurezza), **trasferendolo** (ad altre organizzazioni ad esempio) o **assumendolo** e quindi preparandosi ad affrontare i costi (anche in termini di perdite).

L'efficacia di una strategia per la riduzione del rischio si calcola con il **risk leverage**:

*(**risk exposure prima** della strategia - **risk exposure dopo** la strategia) / **costo risk exposure***

PIANO DI CONTINGENZA

Nonostante l'applicazione di misure di sicurezza **non si possono escludere eventi che possono bloccare il sistema**. Per far fronte a questa spiacevole possibilità si stipula un piano di contingenza per **minimizzare il pericolo e le conseguenti perdite** per l'organizzazione.

Lo scopo è dunque quello di **riprendere il normale funzionamento** con costi e disturbi minimi

Un piano di contingenza **comprende**:

- **Un piano di risposta agli incidenti**: insieme di **procedure** (incident response) **da effettuare immediatamente dopo il verificarsi del danno al fine di ridurre l'impatto**. Questo piano include procedure da sviluppare e documentare durante l'incidente, dopo l'incidente ed anche prima dell'incidente (ad esempio la **pianificazione del backup**)

- **Un piano di ripresa dai disastri**: insieme di **procedure per ripristinare le operazioni primarie** dopo il disastro. Un incidente diventa **disastro** se l'organizzazione non è capace di controllarlo o se i danni sono talmente gravi da non poter ripristinare il sistema velocemente.

- **Un piano di business continuity**: **procedure che facilitano la messa in opera di un sistema alternativo**. Assicura che le **funzioni critiche continuino a funzionare** in caso di disastro, talvolta presso una **sede alternativa** (ed esempio un altro server). Quando necessario viene avviato in contemporanea al piano di disaster recovery. Essendo i due piani strettamente correlati, molte organizzazioni li fondono in un unico piano.

Un aspetto principale di un piano di contingenza è **individuare se un evento dev'essere o meno considerato incidente** e lo si fa consultando report di utenti finali, IDS, anti virus ecc.. Dopo l'individuazione si passa alla fase di reazione. Ad incidente contenuto si passa alla verifica dei danni per poi avviare la fase di ripristino (determinare e risolvere le vulnerabilità, rivedere le contromisure che non hanno bloccato l'attacco, valutare le attività di monitoraggio ed eventualmente migliorarle, ripristinare dati e servizi)

COMMON CRITERIA E BS 7799

La **garanzia delle misure di sicurezza** adottate dev'essere ottenuta con metodi e valutazioni di criteri (standard) ben definiti ed internazionalemnte accettati. Tra gli standard ve ne sono due che necessitano di una particolare attenzione: i **Common Criteria** ed il **BS 7799**.

Gli antichi criteri di metodologia dei vari Paesi non riuscivano più a soddisfare una **comune metodologia di valutazione** e non fornivano risultati sempre confrontabili. Per ovviare a tale problema, nel 1993 furono realizzati i Common Criteria (CC), che nascono con lo scopo di sviluppare una comune metodologia per la valutazione della sicurezza nel mondo dell'informatica che fosse applicabile in campo internazionale.

Essi non sono altro che un **insieme di criteri** che applicano il tema della sicurezza per sistemi e prodotti informatici nelle loro tre componenti fondamentali:

- **funzionalità**: ciò che il sistema deve fare per la sicurezza
- **efficacia**: in che misura le contromisure annullano le minacce
- **correttezza**: come sono state implementate le contromisure

I requisiti supportati dai CC si suddividono fondamentalmente in due classi:

- **Requisiti funzionali**: definiscono i **comportamenti** in materia di sicurezza dei prodotti e dei sistemi informatici.

- **Requisiti di affidabilità**: stabiliscono la **fiducia che si può riporre nelle funzioni** di sicurezza, sia in termini di correttezza dell'implementazione sia in termini di efficacia.

I CC presentano **7 livelli di valutazione dell'affidabilità**, definiti con la sigla **EAL** (**Evaluation Assurance Levels**). Ognuno necessita un grado di affidabilità sempre maggiore, partendo dal primo, in cui le minacce non appaiono serie, fino al settimo, in cui i sistemi sono utilizzati in situazioni di estremo rischio.

Il **modello costruttivo** su cui si basano i CC fa riferimento a due oggetti che possono essere oggetto di descrizione e valutazione:

- **Protection Profile (PP)**: **insieme di obiettivi e requisiti di sicurezza** associabili a **generiche** categorie di prodotti o sistemi informatici che soddisfano le necessità di sicurezza degli utenti

- **Security Target (TG)**: **insieme di requisiti e specifiche di sicurezza** associati ad un prodotto o sistema informatico **specifico** che è oggetto di valutazione. L'oggetto di valutazione viene chiamato anche **TOE** (**Target Of Evaluation**)

Il TOE è il prodotto, o il sistema informatico, che è oggetto di valutazione. Ad esso sono associati due elementi:

- **TOE Security Policy (TSP)**: insieme di **regole** che governano le modalità secondo cui vengono gestiti, protetti e distribuiti i beni (asset) all'interno del TOE.

- **TOE Security Function (TSF)**: tutte quelle **funzioni** del TOE dalle quali dipende la garanzia della corretta esecuzione delle politiche di sicurezza TSP.

Vi sono **due modalità di utilizzo** dei CC:

1. una **modalità standardizzata** che viene utilizzata per **descrivere i requisiti di sicurezza** di un prodotto o di un sistema

2. una **struttura tecnica corretta** per la **valutazione delle caratteristiche di sicurezza** dei prodotti o dei sistemi

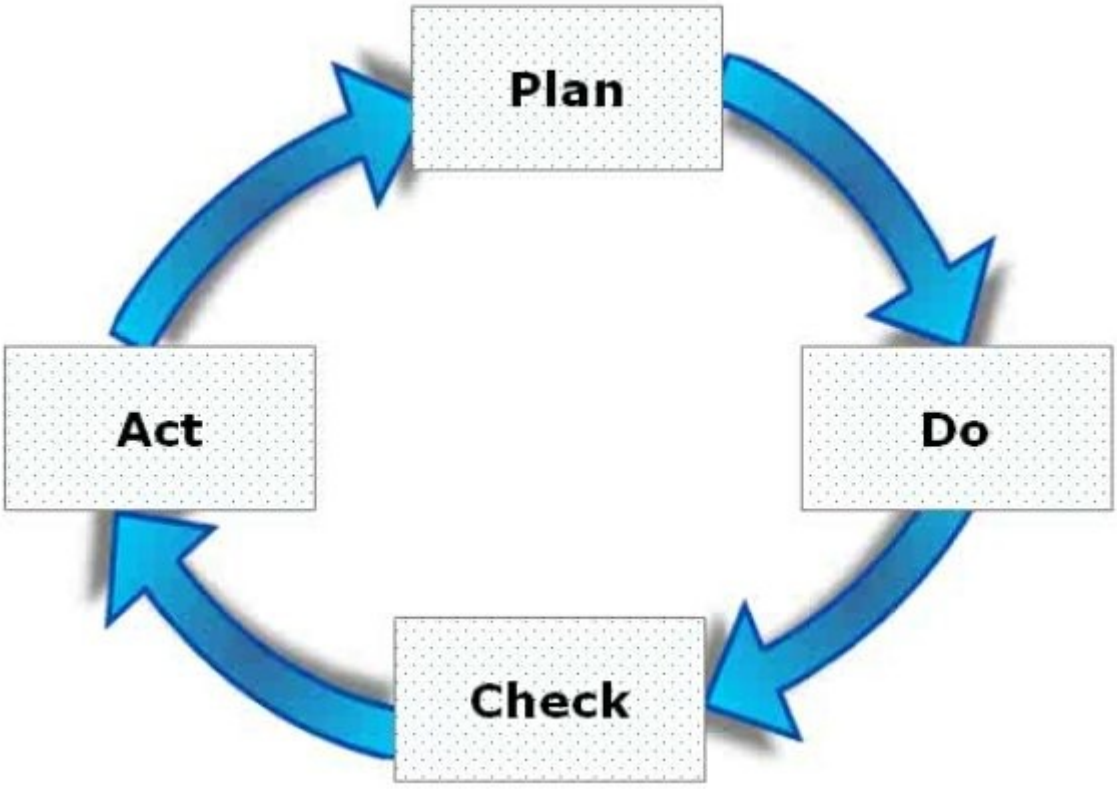
Un altro standard internazionale di sicurezza è il **BS 7799**. Lo scopo principale è quello di **identificare i controlli più appropriati** al fine di garantire la sicurezza di un sistema informatico.

Tale standard è suddiviso in **due parti**:

1. **Parte 1**: analoga al vecchio code of practice (regole di buon comportamento).

2. **Parte 2**: contiene i requisiti oggetto di possibile verifica da terze parti (requisiti normativi)

Il ciclo di vita del processo è suddiviso in **quattro fasi** (**modello PDCA**):



1. Plan: **pianificazione** del sistema di gestione
2. Do: **implementazione** del sistema di gestione
3. Check: **verifica** del sistema di gestione
4. Act: **manutenzione e miglioramento** del sistema

Riassumendo: la garanzia che il sistema o il prodotto soddisfi i suoi obiettivi di sicurezza deve essere frutto di osservazioni effettuate in base a criteri definiti. In altre parole, occorre effettuare delle valutazioni secondo degli standard noti per avere una certa garanzia in termini di sicurezza.