Valutazioni di sicurezza informatica
Metodologie ITSEC

Paolo PAVAN

Giugno 2002

Origini di ITSEC

- Nato per esigenze di sicurezza nazionale, le metodologie ITSEC si sono estese negli anni '90 a prodotti di carattere commerciale.
- Deriva dall'Orange Book (TCSC - Trusted Computer System Evaluation Criteria), che specifica i criteri di sicurezza per sistemi di tipo militare e governativo.
- E' una sua evoluzione ed un suo svecchiamento in ambito europeo.

Definizione di ITSEC

- ITSEC è l'acronimo di "**Information Technology Security Evaluation Criteria**", ovvero **Criteri per la Valutazione della Sicurezza nella Tecnologia dell'Informazione**, e costituisce la base normativa Europea, pubblicata la prima volta nel 1992 da parte della Commissione delle Comunità Europee (DGXIII), con cui gli organismi di Terza Parte che eseguono prove e certificazioni indipendenti nel settore della sicurezza informatica operano.

ITSEC in pratica

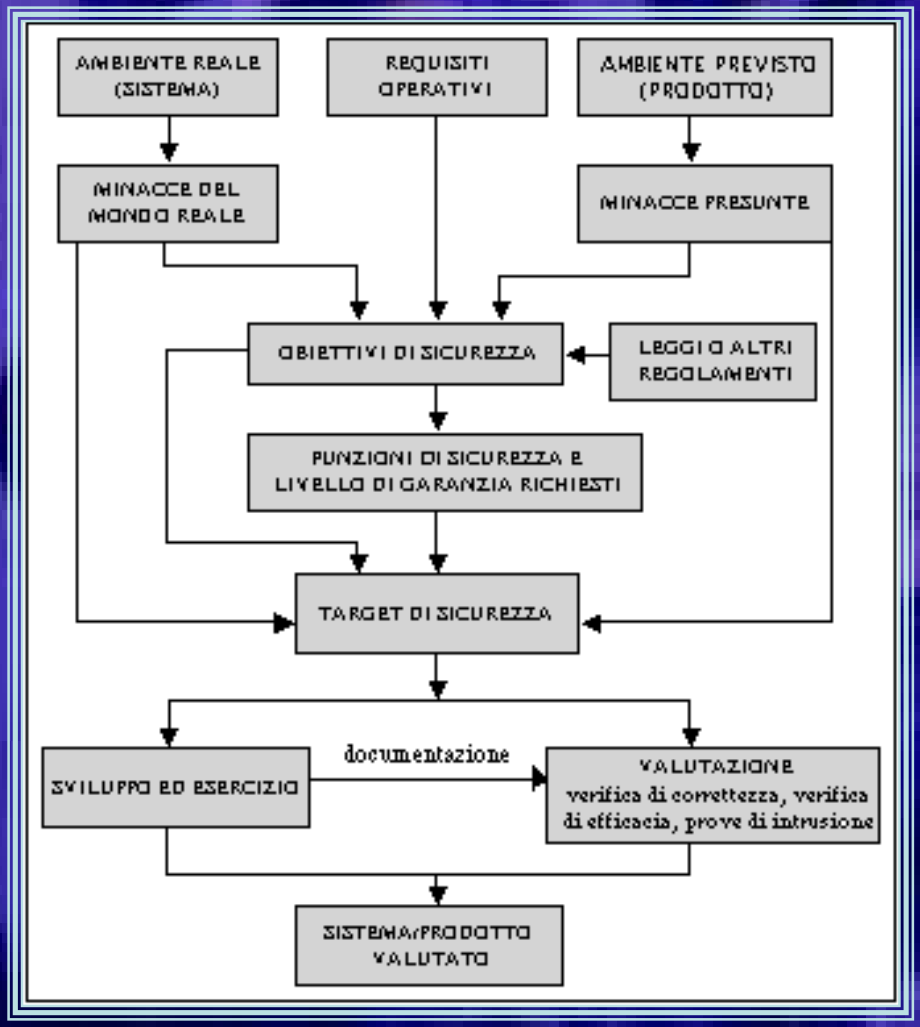
- ITSEC è in pratica **uno strumento di valutazione della sicurezza.**
- La sua metodologia di applicazione è l'**ITSEM** (Information Technology Security Evaluation Manual);
- l'oggetto (sistema o prodotto IT) della valutazione è detto **TOE** (Target Of Evaluation).
- Il soggetto (organizzazione, azienda, ecc.) che richiede una valutazione è detto sponsor.
  - http://www.itsec.gov.uk

Come opera ITSEC

- La prassi vuole la richiesta di prove di evidenza sulla sicurezza di un prodotto al fornitore del prodotto medesimo.(safety)
- Valutazioni di terza parte
  - Servizi di prova o valutazione: servizio tecnico, con prove di laboratorio produce dati reali misurabili. Il resoconto è una relazione tecnica destinata a tecnici con esperienze nel campo della sicurezza e dei sistemi
  - Servizi di certificazione: approva la sicurezza del prodotto, il documento è di tipo tecnico-legale destinato ad un pubblico più vasto e meno esperto.
- Criteri di valutazione: rappresentano lo strumento attraverso cui è possibile esprimere un giudizio su quanto sia sicuro un sistema informatico o un prodotto software.

NETLINK S.a.s.

Fondamenti dei criteri ITSEC
Schema



Il flusso logico di sviluppo e valutazione.

Si parte dall'**ambiente** elaborato per poter identificare degli **obiettivi di scurezza** che si concretizzano nel **target di sicurezza**.

Come avviene la valutazione

- Idealmente è scomponibile in 6 fasi principali
  1. Definizione dell'ambiente e dei requisiti operativi
  2. Identificazione di politiche di sicurezza e degli obiettivi che la mia sicurezza deve raggiungere
  3. Identificazione dei requisiti per il Target di sicurezza
  4. Sviluppo della valutazione
  5. Verifica della valutazione
  6. Sistema o prodotto certificato

Fondamenti dei criteri ITSEC
Requisiti e Obiettivi di Sicurezza

- Si presuppone che il sistema sia realizzato per un modello di business noto, che determini dei requisiti operativi noti, sia collocato in un determinato ambiente fisico, siano identificabili delle *politiche* di sicurezza e degli **obiettivi di sicurezza** in termini di *riservatezza*, *integrità* e *disponibilità*. ed uno scenario di *minacce a* cui il sistema è sottoposto.
- Se formalizziamo la definizione delle funzionalità ritenute necessarie, otteniamo una serie di requisiti, come presenti in una ipotetica norma, applicabile per quel sistema (quell'ambiente di esercizio, quello scenario delle minacce, quell'insieme di funzionalità). Tale ipotetica norma prende il nome di **Target di Sicurezza.**
- **semplificando i criteri** ITSEC sono definibili come **i criteri pubblici per valutare la conformità di un sistema o un prodotto qualsiasi al proprio Target di Sicurezza.** Ciò che è stato detto per un sistema vale anche nel caso di un prodotto informatico.

Sviluppo della Valutazione
Target di Sicurezza: livelli

- Il Target di sicurezza ovvero quella serie di requisiti necessari a raggiungere il livello di sicurezza indicato come nostro obiettivo può essere accompagnato da indicazioni che specificano quanto voglio essere protetto. Queste indicazioni sono dei "**livelli di sicurezza**" :
  - ITSEC riconosce **7 livelli di sicurezza** per garanzie crescenti da *E0* (nessuna garanzia) a *E6* (massima garanzia).
  - Il livello di sicurezza va scelto in base al tipo ed al valore del dato da proteggere.
  - Più alto è il livello più alto sarà il costo per raggiungere in termini di tempo e risorse umane.

Come si realizza il Target di Sicurezza
Robustezza dei meccanismi

- Le singole funzionalità di sicurezza in pratica sono realizzate con algoritmi software o con logica hardware, chiamati in termini generali **meccanismi** da ITSEC.
- Questo meccanismi devono essere più robusti quanto maggiore è i livello di sicurezza (ed il rischio di attacco) che vogliamo raggiungere
- Si distinguono tre livelli di robustezza dei meccanismi
  - **Basic**
  - **Medium**
  - **High**

- **Hardening dei sistemi**
- **Crittografia**
- **Sicurezza della rete**
- **Firewall/IDS**

Valutazione del Target di Sicurezza

- I criteri ITSEC si fondano sulla sistematica suddivisione dell'argomento sicurezza nei tre aspetti:
  - **funzionalità** *(ciò* che il prodotto/sistema deve fare per la sicurezza),
  - **efficacia** *(in che misura* le funzionalità di sicurezza annullano le *minacce)*
  - **correttezza** *(come* il sistema è stato implementato, quanto fedelmente rispetto all'idea del progettista).
- Da quanto esposto finora appare che la funzionalità è di definizione libera e diversa da caso a caso, dipendendo pesantemente dalla tipologia di prodotto/sistema che la realizza, dagli obiettivi alla base delle sua realizzazione, dallo scenario di minacce che si propone di contrastare.
- Il Target di Sicurezza contiene la formalizzazione di tutto questo. L'insieme dei due aspetti di *efficacia* e *correttezza* costituisce quella che in ITSEC è la ***garanzia***.

Verifica della Valutazione
Analisi di correttezza

- ITSEC parte dal presupposto che un processo ben strutturato e ben realizzato stia alla base di un progetto e di un esercizio di qualità.
- La verifica dei tre aspetti (funzionalità, efficacia e correttezza) che definiscono il target di sicurezza avviene attraverso l'analisi di correttezza:
  - sono oggetto di questa analisi i seguenti argomenti: il processo di sviluppo, l'ambiente di sviluppo, la documentazione di esercizio, l'ambiente di esercizio.

Verifica della Valutazione
Analisi di efficacia

- ITSEC considera **sei analisi di efficacia**, che devono essere prodotte dallo sponsor, cioè colui che richiede la valutazione, e, in maniera indipendente, dal valutatore utilizzando la documentazione consegnata per l'aspetto della correttezza. In aggiunta a ciò il valutatore è chiamato ad effettuare una serie di test di intrusione, per verificare la sfruttabilità delle eventuali *vulnerabilità* riscontrate.
- ITSEC considera efficaci le funzionalità presenti in un prodotto/sistema se:
  - Le contromisure implementate contrastano le minacce messe in opera attraverso attacchi diretti (*analisi di adeguatezza*);
  - Le contromisure implementate contrastano le minacce realizzate attraverso *attacchi indiretti (analisi di integrazione*);
  - Il prodotto/sistema è esente da vulnerabilità intrinseche sfruttabili (a*nalisi di vulnerabilità in costruzione*);
  - Il prodotto/sistema è esente da vulnerabilità di esercizio sfruttabili (*analisi di vulnerabilità in esercizio*);
  - Il prodotto/sistema non è passibile di utilizzo *insicuro*, pensando invece che sia sicuro (*analisi di facilità d'uso*);
  - I singoli meccanismi resistono ad attacchi diretti portati a termine con risorse determinate (*analisi di robustezza dei meccanismi*), in accordo con quanto specificato nel Target di Sicurezza, alla voce robustezza dei meccanismi

La situazione Europea ed Italiana per le valutazioni e certificazioni ITSEC

- Alla fine degli anni '80 erano presenti in Europa, Schemi Nazionali per le valutazioni e certificazioni di sicurezza informatica.
- La motivazione della nascita di tali Schemi è stata ovunque la **Sicurezza Nazionale**.
- Dall'inizio degli anni '90 gli Schemi hanno adottato i criteri e le metodologie descritte in ITSEC e sono iniziate le valutazioni di **prodotti a carattere commerciale**, cioè non legate alla tutela della Sicurezza Nazionale.

Schemi e paesi Europei

- **Regno Unito** - Esiste uno schema, che vede come Organismo di Certificazione un Organismo di Stato (UKITSEC CB) e come valutatori alcune strutture private, da esso controllate. Lo schema opera sia per prodotti commerciali, sia per prodotti e sistemi legati alla Sicurezza Nazionale.
- **Germania** - Situazione simile a quella descritta per il Regno Unito, con l'aggiunta di due Organismi di Certificazione privati, che svolgono anche attività di valutazione.
- **Francia** - L'organismo di certificazione è di Stato (SCSSI), che di fatto governa due Schemi separati. Per la Sicurezza Nazionale esiste un unico valutatore (CELAR), mentre per il settore commerciale esiste qualche struttura privata (CESTI).
- **Italia -** Lo Schema è nato nel 1995 per gli aspetti legati alla Sicurezza Nazionale, con la. pubblicazione di alcune direttive da parte dell'Autorità Nazionale per la Sicurezza. che ne è l'Organismo di Certificazione. Attualmente sono omologate due strutture di valutazione, entrambe private.