Centro di Valutazione della Difesa

II Reparto – Informazioni e Sicurezza

Ce.Va. Difesa: dipendenza ed ubicazione.

Il Ce.Va Difesa è un'articolazione del II Reparto (Informazioni e Sicurezza) dello Stato Maggiore della Difesa. Il Capo Reparto è il rappresentante legale ed esercita le sue funzioni tramite il Vice Capo Reparto per le Rappresentanze Militari e la Sicurezza, dal quale il Ce.Va. dipende direttamente. La sede legale è ubicata presso lo SMD – RIS di Roma, mentre la sede operativa è a San Piero a Grado (PI), nello stesso comprensorio del Centro Interforze Studi e Applicazioni Militari (CISAM).

La sicurezza nel settore della tecnologia della comunicazione e dell'informazione – *Information Communication Technology* (ICT) – consiste nella protezione della riservatezza, integrità e disponibilità delle informazioni, contrastando le minacce originate dall'uomo o dall'ambiente. Il fine è quello di impedire l'accesso, l'utilizzo, la divulgazione, e la modifica delle informazioni stesse a chi non è stato autorizzato, e di garantirne l'accesso e l'utilizzo a chi, invece può legittimamente accedervi.

Si riferisce quindi a molteplici aspetti tecnici, organizzativi, procedurali per proteggere l'hardware, il software, i servizi.

La certificazione di sicurezza è un processo a cui partecipano vari soggetti come il gestore dello schema, il garante dello schema, il certificatore, il valutatore e l'ente di accreditamento ed in cui sono definite delle regole, cioè delle norme di riferimento costituenti lo schema di certificazione.

Il principale standard di riferimento in uso presso il Ce.Va. Difesa è lo standard internazionale ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation*).

Il Laboratorio è anche in grado di condurre valutazioni secondo i criteri europei della metodologia ITSEC (*Information Technology Security Evaluation Criteria*).

I criteri ITSEC, tuttavia, stanno perdendo via via di interesse, a vantaggio dei Common Criteria. Ciò, anche grazie all'accordo di mutuo riconoscimento "*Common Criteria Recognition Arrangement*" (CCRA) che prevede che siano riconosciuti automaticamente i certificati emessi dagli Enti di Certificazione di nazioni denominate "*Certificate Authorizing*", mentre sono riconosciuti in base ad accordi bilaterali i certificati emessi a seguito di valutazioni dei Centri di Valutazione (Ce.Va.) delle nazioni definite "*Certificate Consuming*".

Perché non vi sia un
11 settembre informatico

Schema di certificazione.

In Italia sono attivi due schemi di certificazione: il primo, gestito dall'Autorità Nazionale per la Sicurezza (ANS) è impiegato nella valutazione di prodotti e sistemi destinati alla protezione di informazioni che trattano il segreto di Stato. Il secondo, gestito dall'Organismo di Certificazione della Sicurezza Informatica (OCSI), si occupa di prodotti e sistemi ricadenti al di fuori di tale contesto.

Nell'ambito del primo schema operano vari laboratori accreditati, tra i quali il Ce.Va Difesa.

Per rilasciare una certificazione basata su standard di riferimento comunemente accettati, occorre che la valutazione sia effettuata da laboratori di comprovata competenza ed avvenga nell'ambito di uno schema di certificazione.

Il valutatore deve sempre essere guidato dai seguenti quattro principi generali:

- **imparzialità**: la valutazione deve essere condotta senza pregiudizi e, in particolare, deve essere possibile dimostrare che il Ce.Va. e i Valutatori coinvolti non abbiano interessi commerciali o finanziari dipendenti dall'esito della valutazione stessa;
- **obiettività**: le conclusioni del processo di valutazione devono essere motivate da evidenze sperimentali ogni qual volta sia possibile;
- **ripetibilità** e **riproducibilità**: la valutazione dello stesso prodotto o sistema, effettuata con gli stessi requisiti di sicurezza dallo stesso Centro o, rispettivamente, da un diverso Centro di Valutazione, deve portare agli stessi risultati.

Certificazione e livelli di garanzia.

L'ANS, in qualità di Ente di Accreditamento, per lo schema per la tutela delle informazioni classificate, rilascia i certificati quando completata positivamente la valutazione tecnica condotta dal Ce.Va..

Per ottenere un certificato, un fornitore di un prodotto o sistema deve produrre idonea documentazione. Di fondamentale importanza è il documento detto Target di Sicurezza (TS), in cui si dichiara quali sono gli obiettivi di sicurezza del sistema o prodotto in esame, quali sono le minacce che possono ostacolare tali obiettivi e quali sono le funzioni di sicurezza realizzate per contrastare queste minacce.

Altra documentazione descriverà lo sviluppo del progetto, e quindi le scelte progettuali adottate dal fornitore, i manuali di supporto, il ciclo di vita, le fasi di test e le vulnerabilità.

La quantità di tale documentazione cresce al crescere del livello di garanzia richiesto per la valutazione del prodotto o sistema.

Nei Common Criteria, i livelli di *assurance* sono sette: da EAL1, che è il livello base, ad EAL7, che è il livello massimo.

Per la metodologia ITSEC, i livelli di assurance sono sette: da E0, che è il livello base, ad E6, che è il livello massimo.

Il laboratorio di valutazione (Ce.Va. Difesa) verifica, anche attraverso test di penetrazione, l'efficacia, cioè che le funzioni di sicurezza indicate siano idonee nel contrastare le minacce dichiarate e la correttezza, cioè che le stesse siano state realizzate senza commettere errori.

“Conosci il nemico come conosci te stesso. Se farai così, anche in mezzo a cento battaglie non ti troverai mai in pericolo.”

(Sun Tzu, stratega cinese, VI-V Secolo A.C.)

Differenze tra CC e ITSEC.

I CC costituiscono uno standard che fornisce un’univoca e concordata metodologia di valutazione (almeno fino ad EAL4), valida a livello internazionale, mentre ITSEC solo a livello europeo.

I CC obbligano lo sviluppatore a scegliere i requisiti funzionali e di garanzia dai cataloghi descritti dai CC, che diventano una sorta di dizionario, rendendo la completezza del ST molto più formale e ripetibile.

Nei CC si valutano anche i Protection Profile (PP), ossia documentazione che descrive una tipologia omogenea di prodotti in modo indipendente dalla realizzazione. Per questo i Security Target hanno la possibilità di essere sviluppati sulla base di PP scelti.

Il Ce.Va Difesa può valutare.

- applicazioni SW
- sistemi operativi
- varie combinazioni di applicazioni software con un sistema operativo e/o workstation
- circuiti integrati di smart card o i loro coprocessori crittografici
- LAN che includano terminali, server, apparati di rete e software
- applicazioni di database

Utilità della certificazione.

La certificazione della sicurezza serve ad offrire garanzie sulla corrispondenza tra le caratteristiche di sicurezza effettive di un sistema o di un prodotto ICT e quelle dichiarate dal costruttore.

Da un lato la certificazione risponde ad esigenze di garanzia sempre più sentita dagli utilizzatori di tali sistemi e prodotti, dall’altro però può essere utilizzata dagli sviluppatori come leva di marketing allo scopo di:

- accedere a quei mercati per cui l’uso di prodotti o sistemi certificati è un requisito del committente o un obbligo di legge, come la tutela del segreto di Stato;
- inserirsi nel mercato con prodotti affidabili, sottoposti a verifica da parte di laboratori accreditati;
- accrescere la propria immagine sul mercato dei prodotti per la sicurezza.

Il personale del Ce.Va. Difesa.

Il Ce.Va. Difesa dispone di **5 valutatori** (a maggio 2008 previsto inizio corso per ulteriori due valutatori):

- “*on-the-job training*” di 6 mesi presso i laboratori IBM in Canada
- abilitati come «Valutatori della sicurezza di sistemi/prodotti informatici fino a livello EAL4 “Common Criteria” ISO/IEC 15408» a cura CSE canadese
- accreditati valutatori, anche ITSEC, dall’A.N.S.

I servizi offerti dal Ce.Va Difesa.

Il Ce.Va. Difesa è stato abilitato come Centro di valutazione dall’ANS nel 2004.

Utilizzando procedure amministrative che vedono l’accensione di convenzioni economiche tra le Direzioni Generali ed il fornitore, sempre avendo come riferimento per le valutazioni lo standard internazionale dei CC e o criteri ITSEC, il Ce.Va. Difesa offre servizi che includono:

- valutazioni di prodotti e sistemi ICT;
- valutazione di Security Target;
- assistenza sui Common Criteria;
- consulenza sulla stesura della documentazione necessaria ad una valutazione.

Valutazioni condotte dal Ce.Va Difesa.

Il Ce.Va Difesa ha condotto fino ad oggi tre valutazioni, tutte relative al programma italo-francese Cosmo-Skymed.

Tutte le valutazioni richieste sono state effettuate a livello EAL4.

Livelli di "garanzia" EAL e CAP

Evaluation Assurance Level – EAL –		
EAL1	Functionally Tested	Consente di avere una fiducia minima dell'ODV con verifica correttezza SF senza coinvolgimento sviluppatori. Minacce poco rilevanti.
EAL2	Structurally Tested	Come sopra con attenzione spedizione, test e sviluppo con la cooperazione degli sviluppatori. Ricerca vulnerabilità note. Minacce medio-basse.
EAL3	Methodically Tested & Checked	Massimo di affidabilità SF senza apportare modifiche sostanziali al processo di sviluppo esistente o re-engineering del TOE. Minaccia media.
EAL4	Methodically Designed, Tested & Reviewed	Per sistemi sviluppati correttamente anche senza specialisti in sicurezza. Massima affidabilità con eventuali piccole modifiche ai processi di sviluppo. Minaccia medio-alta. Ricerca delle vulnerabilità più evidenti. E' il livello più richiesto dai Committenti.
EAL5	Semiformally Designed & Tested	Security Policy a supporto ST descritto con un linguaggio formale. FS, progetto architetturale e progetto di dettaglio con un linguaggio semi-formale. Impiego progettisti adeguatamente esperti in sicurezza ed un maggior uso di risorse. Per minaccia elevata.
EAL6	Semiformally Verified Designed & Tested	Stretta corrispondenza tra progetto di dettaglio, source coding e schemi HW. Assurance elevato con alti costi per minacce gravi. Spedizione, testing e progetto di alta qualità. Assurance elevato per beni di valore sottoposti a gravi minacce.
EAL7	Formally Verified Designed & Tested	FS e progetto architetturale descritti con linguaggio formale consistente con il modello formale della Security Policy. Dimostrazioni formali fin dalla fase progettuale. Dimostrazione di assenza brecce per accesso ai dati. Per situazioni ad altissimo rischio.

Composed Assurance Packages – CAP –		
CAP-A	Structurally composed	CAP-A è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello basso o moderato di sicurezza garantita indipendentemente in assenza della pronta disponibilità di una completa documentazione di sviluppo.
CAP-B	Methodically composed	CAP-B è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello moderato di sicurezza garantita indipendentemente, e una accurata investigazione del TOE composto e del suo sviluppo senza una sostanziale re-ingegnerizzazione.
CAP-C	Methodically composed,	CAP-C è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello da moderato a elevato di sicurezza garantita indipendentemente e sono preparate a ricorrere a costi addizionali di re-ingegnerizzazione specifici per la sicurezza.

Via della Bigattiera lato monte, n.10 - 56122, San Piero a Grado (PI)
Tel / Fax 050 964 313 ris.ceva@smd.difesa.it

STATO MAGGIORE DELLA DIFESA

II REPARTO – INFORMAZIONI E SICUREZZA

CENTRO DI VALUTAZIONE DELLA DIFESA

Via della Bigattiera lato monte, n.10 - 56122, San Piero a Grado (PI)

Tel / Fax 050 964 313 ris.ceva@smd.difesa.it