

L'interpretazione dei Common Criteria relativamente alle aree di confine con lo standard BS7799

Daniele Perucchini

Obiettivi comuni CC-BS7799

- Aumentare la sicurezza globale dell'utilizzo dei sistemi ICT, tenendo in conto sia gli aspetti tecnici, sia gli aspetti procedurali, fisici e quelli relativi al personale
- Ottimizzare l'uso delle risorse nelle fasi di certificazione e controllo

Terminologia Common Criteria

- **Prodotto**: un insieme di elementi software, hardware e/o firmware che svolge una funzione che può essere utilizzata da molti sistemi
- **Sistema**: una specifica installazione IT (sw, fw o hw), caratterizzata da uno scopo e da un ambiente operativo ben definiti
- **Traguardo di Sicurezza (TdS)**: il documento, utilizzato come base per la Valutazione di un OdV, che contiene gli obiettivi di sicurezza, **la descrizione dell'ambiente in cui l'OdV è utilizzato** e le minacce alle quali è soggetto, i requisiti funzionali e di garanzia, la specifica delle funzioni di sicurezza
- **Oggetto della Valutazione (OdV)**

Valutazione e Certificazione CC

- Il processo di valutazione è effettuato da un Laboratorio (LVS) ed è finalizzato all'emissione di un rapporto in cui si dichiara se:
 - il Traguardo di Sicurezza è completo, congruente, tecnicamente corretto ed adatto ad essere usato come base per la valutazione del corrispondente ODV,
 - l'Oggetto della Valutazione soddisfa il Traguardo di Sicurezza al livello di garanzia richiesto
- l'Organismo di Certificazione esamina il rapporto e, se positivo, certifica l'OdV
- I livelli di garanzia sono denominati EALx (x=1...7), e prevedono dettagliate azioni del Valutatore descritte nei requisiti di garanzia

Aree di confine

- Analizzando le azioni dei Valutatori CC che potrebbero essere affini ad attività previste nella certificazione BS7799, è possibile individuare le seguenti aree di confine:

Ambiente
operativo
dell'OdV

Ambiente e
processo di
sviluppo
dell'OdV

Ambiente operativo dell'OdV

TdS: ambiente dell'OdV

- In generale, la descrizione dell'ambiente di sicurezza include **ipotesi** su:
 - Protezione fisica (locazione dell'OdV, aree riservate per gli amministratori, etc.);
 - Gestione del personale (la competenza, gestione amministrativa del personale, etc.).
 - Procedure (validazione degli aggiornamenti, aggiornamento periodico degli antivirus, etc.);
 - Aspetti di connettività (connessioni ad altri sistemi IT, etc.) ;
- Le ipotesi, insieme a politiche di sicurezza opportune e ben definite, **assumono il ruolo di misure di sicurezza** e concorrono a contrastare le minacce ai beni dell'OdV, individuate nel TdS.

TdS: ambiente operativo dell'OdV

- L'attività di valutazione dell'ambiente di sicurezza è finalizzata a consentire **all'utente finale** di verificare che le ipotesi fatte in sede di valutazione siano verificate nell'ambiente operativo dell'OdV
- Le attività del Valutatore per la certificazione di sicurezza di prodotti o sistemi IT non prevedono una **verifica** dell'attuazione delle misure di sicurezza non tecniche

Ambiente e processo di sviluppo dell'OdV

Ambiente di sviluppo: visite al sito

- Le visite del Valutatore al sito dello Sviluppatore sono **utili** al fine di determinare se le misure di sicurezza previste per lo sviluppo sono realizzate in modo congruente con quanto descritto nella documentazione
(CEM Annesso B)

Ambiente di sviluppo: visite al sito

- Attività di valutazione che prevedono la possibilità di una visita al sito dello Sviluppatore sono:
 - ACM_AUT: (*Automazione della Gestione della Configurazione*)
 - ACM_CAP.n (n>2): (*Potenzialità della gestione della configurazione*)
 - ADO_DEL: (*Consegna dell'OdV*)
 - ALC_DVS: (*Identificazione delle misure di sicurezza nell'ambiente di sviluppo*)
 - ADO_IGS (*Installazione, generazione e start-up*)

Ambiente di sviluppo ACM_AUT

Automazione della Gestione della Configurazione

- Si deve verificare che le operazioni di modifica dell'OdV avvengano in accordo a procedure ben definite e sotto il controllo di strumenti di tipo automatico (>EAL3)
- Possono essere effettuate visite al sito di sviluppo per verificare l'attuazione delle procedure previste

Ambiente di sviluppo ACM_CAPn ($n > 2$)

Potenzialità della gestione della configurazione

- I requisiti di garanzia introdotti dalla famiglia *ACM_CAP* hanno l'obiettivo di ridurre la probabilità che gli elementi che fanno parte della configurazione possano subire modifiche di tipo accidentale, o comunque non autorizzate ($>EAL2$)
- Sono possibili anche interviste al personale

Ambiente di sviluppo ADO_DEL

Consegna dell'OdV

- Si deve verificare che esistano (>EAL1):
 - procedure che descrivano in dettaglio le misure che sono necessarie per garantire che la sicurezza dell'OdV sia preservata durante la distribuzione dell'OdV agli utenti finali.
- Questa attività potrebbe richiedere anche visite al sito operativo dell'OdV

Ambiente di sviluppo ALC_DVS

Identificazione delle misure di sicurezza nell'ambiente di sviluppo

- Si deve verificare che i controlli di sicurezza esercitati dallo Sviluppatore sull'ambiente di sviluppo siano adeguati a preservare la confidenzialità e l'integrità del progetto e dell'implementazione dell'OdV. (>EAL2)
- Sono previsti, tra l'altro:
 - Esame delle misure di sicurezza fisiche
 - Verifica di prove documentali dall'applicazione delle procedure
 - Interviste con il personale

Ambiente di sviluppo ADO_IGS

Installazione, generazione e start-up

- Si deve verificare che esistano le procedure per installare, generare ed avviare per la prima volta l'OdV in modo sicuro (da EAL1)
- Questa attività potrebbe richiedere anche visite al sito operativo dell'OdV

Ambiente di sviluppo: visite al sito

- Le visite del Valutatore al sito dello Sviluppatore possono essere non necessarie quando (CEM Annesso B):
 - È stata recentemente effettuata una visita relativa a una valutazione di un altro OdV;
 - Sono state recentemente effettuate **particolari** procedure di verifica nell'ambito di certificazioni tipo "ISO 9000".
- Possono essere considerati approcci diversi dalla visita, a patto che forniscano lo stesso livello di garanzia (CEM Annesso B)
- La decisione se fare o meno una visita al sito di sviluppo deve essere presa in accordo con l'Ente Certificatore (OCSI)

Conclusioni 1/2

- I CC analizzano soprattutto le misure di sicurezza tecniche:
 - Non sono previste verifiche di misure di sicurezza non tecniche nell'ambiente operativo dell'ODV
 - Verifiche limitate sulle misure di sicurezza non tecniche all'ambiente di sviluppo dell'OdV (e in qualche caso eccedono lo spirito della norma CC)

Conclusioni 2/2

- Nel caso di certificazioni congiunte CC e BS7799, è abbastanza semplice trovare l'accordo sulle rispettive competenze
- Nel caso di certificazioni o solo CC o solo BS7799, l'obiettivo di aumentare la sicurezza globale (aspetti tecnici e non tecnici) è difficilmente raggiungibile