Certificazione della sicurezza dei prodotti e sistemi informatici

La certificazione della sicurezza di prodotti e sistemi IT si effettua secondo le norme tecniche ITSEC (Information Technology Security Evaluation Criteria) e Common Criteria for Information Technology Security Evaluation (recepita dall'ISO come ISO 15048).

Ad esse sono associati i manuali ITSEM (nel primo caso, Information Technology Security Evaluation Manual) e CEM (nel secondo caso, Common Evaluation Manual).

Vale qui la pena ricordare che:

- I prodotti/sistemi da certificare sono detti in italiano Oggetto di Valutazione (OdV) e in inglese Target of Evaluation (TOE);
- i requisiti di sicurezza generali per una tipologia di prodotto o sistema sono descritti in *Classi di funzioni di sicurezza* nel caso di ITSEC o *Protection Profile (PP* o *Profilo di Protezione)* nel caso dei Common Criteria; queste "raccolte" possono essere anche loro oggetto di certificazione. A titolo di esempio sono state certificati Protection Profiles per firewall o per database;
- i documenti di maggior dettaglio relativi allo specifico OdV sono detti Security Target (o Target di sicurezza o Traguardo di Sicurezza sulle normative italiane);
- i due standard prevedono 6 o 7 livelli di sicurezza crescenti (nel caso di ITSEC E1... E6; nel caso dei Common Criteria EAL1... EAL7) dipendenti dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo. Ovviamente, più la documentazione è estesa e formale, più si ha la garanzia che il processo di sviluppo è stato rigoroso.

Il livello aggiuntivo dei Common Criteria rispetto a ITSEC rappresenta un livello minimo di certificazione, perché non richiede la valutazione della documentazione utilizzata e dell'ambiente di sviluppo. Gli altri livelli sì, e richiedono la collaborazione degli sviluppatori.

Gli schemi di certificazione italiani sono due: uno relativo ai prodotti e sistemi correlati alla sicurezza e l'altro relativo alla sicurezza "commerciale" (si pensi ai dispositivi utilizzati per la firma digitale).

Tutti e due gli schemi nominano uno specifico Oganismo di Certificazione (OdC), che accredita a sua volta dei laboratori per le attività di valutazione.

In particolare, gli OdC devono predisporre regole tecniche in materia, linee guida per la valutazione dei prodotti, divulgare principi e procedure, diffondere la lista dei prodotti e Protection Profile certificati, aggiornare l'elenco dei laboratori accreditati.

In questi casi, gli Enti di Certificazione *accreditano* i laboratori secondo le norme UNI CEI EN ISO/IEC 17025:2000 sui laboratori di prova e taratura e la UNI CEI EN 45011 sugli organismi di certificazione dei prodotti (le stesse del SINAL).

In tutti e due i casi, i laboratori possono fornire consulenza.

Le attività sono così sintetizzabili:

- il *committente* contatta un laboratorio e l'OdC per l'inizio delle attività e garantisce le comunicazioni tra laboratorio e sviluppatori;
- i laboratori inviano all'OdC dei *rapporti di attività*;
- Laboratori e OdC inviano eventuali *rapporti di osservazione* se necessitano chiarimenti da parte degli sviluppatori
- alla fine delle attività, il laboratorio invia all'OdC il *rapporto finale di valutazione* come base per la certificazione del OdV;
- l'OdC emette un *rapporto di certificazione* che conferma i risultati della valutazione e la corretta applicazione dei criteri e della relativa metodologia.

In tutti i casi, la certificazione è riferibile esclusivamente ad una specifica e determinata configurazione dell'ODV. Questo vuol dire che a fronte di patches o fixes o altri cambiamenti del software certificato, deve essere fatta un'ulteriore verifica. Questo implica una forte spesa di mantenimento della certificazione e il conseguente basso numero di certificati rilasciati.

Va anche detto che le normative non pongono limiti allo scopo di certificazione. In questo modo, la Microsoft ha certificato Windows NT (sistema operativo di rete) specificando che lo scopo di certificazione riguarda sistemi non collegati in rete.

Per quanto riguarda il riconoscimento tra i diversi OdC, è stato sottoscritto a Baltimora un accordo di mutuo riconoscimento tra 16 Paesi dei certificati Common Criteria (Common Criteria Recognition Arrangement, CCRA) sottoscritto il 23 maggio 2000, che nell'articolo 5 richiede che ciascun Paese aderente stabilisca lo schema di certificazione. L'Italia, in tale occasione è stata rappresentata dall'ANS-UCSi.

DPCM del 30 ottobre 2003: sicurezza commerciale

Ha titolo "Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del D.Lgs. 23 gennaio 2002, n. 10."

Lo schema si applica ai sistemi e prodotti IT, ma non si applica a sistemi e prodotti che trattino informazioni classificate (art. 2.2) perché di pertinenza del DPCM 11 aprile 2002 trattato in seguito.

L'art. 4.1 stabilisce che è l'ISCTI (Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione) l'OdC della sicurezza informatica nel settore della tecnologia dell'informazione (cfr Dlgs 10/2002 art 10 e 1999/93/CE art. 3). Il tutto a titolo oneroso.

Attualmente l'ISCTI è stato rinominato ISCOM (www.iscom.gov.it) e si fa anche riconoscere come OCSI (Organismo di Certificazione della Sicurezza Informatica, www.ocsi.it).

I laboratori sono denominati Laboratori di Valutazione della Sicurezza (LVS) e il loro elenco è disponibile sul sito dell'ISCOM

Tra l'altro, l'articolo 13 indica che l'OdC ha 2 mesi per la predisposizione di Linee Guida provvisorie e 12 per quelle definitive, che devono essere approvate dal Ministero dell'Innovazione e le tecnologie in concerto con il Ministro delle comunicazioni. Va detto che le Linee Guida provvisorie sono state approvate il 17 febbraio 2005 e sono reperibili sul sito dell'OCSI.

Secondo questo DPCM, i certificatori di firma elettronica hanno 9 mesi di tempo per certificare i prodotti e dispositivi di firma elettronica. Attualmente forniscono autodichiarazioni ai sensi dei DPCM 7 dicembre 2000, DPCM 20 aprile 2001, DPCM 6 ottobre 2001 (ci si pone la domanda su come debbano muoversi a questo punto, dato che le linee guida provvisorie per l'attività di certificazione sono state emesse con 14 mesi di ritardo).

DPCM del 11 aprile 2002: sicurezza nazionale

Ha titolo "Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato".

Riguarda la Sicurezza dello stato e riguarda le informazioni classificate (art. 1)

E' del tutto simile al DPCM 30 ottobre 2003, ma:

- Stabilisce che l'OdC è l'ANS (Autorità Nazionale per la Sicurezza), che si avvale dell'Ufficio Centrale per la Sicurezza (UCSi), che a sua volta è un'articolazione della Segreteria Generale del Comitato esecutivo per i servizi di informazione e sicurezza (CESIS).
- I laboratori sono indicati con la sigla Ce.Va.

I laboratori accreditati sono 5: 3 privati e 2 pubblici (tra cui l'ISCOM, a sua volta ente di certificazione "commerciale").

A livello di norme italiane, attualmente non rintracciate:

- **Direttiva PCM-A.N.S. 1/R/A** edita nel 1985 a firma del Presidente del Consiglio dei Ministri e successivamente completamente revisionata nel 1993.
- **PCM-ANS TI-001, Procedura nazionale per l'omologazione di sistemi/reti EAD militari.** Vengono individuati i requisiti di sicurezza, il ruolo che questi svolgono ai fini dello studio di fattibilità dei sistemi/reti dell'approvazione di sicurezza, dell'omologazione, della determinazione del ciclo di vita operativo dei sistemi EAD. Qui si intende con omologazione: l'autorizzazione all'impiego operativo del sistema EAD, sulla base dei risultati della certificazione e delle condizioni operative ambientali (requisiti operativi e valutazione della minaccia e del rischio).
- **PCM-ANS TI-002 Standard di sicurezza per sistemi/reti EAD militari.** Procedure per l'accertamento del rischio e della vulnerabilità residua dei sistemi informatici, espressa in forma numerica, mediante l'applicazione di formule matematiche. Viene così determinato il valore di garanzia del sistema da valutare in relazione al tipo di classifica delle informazioni trattate (SS, S, RR, R), del grado di rischio e della modalità operativa del sistema (" dedicato", " al più alto livello di classifica", "multilivello"). In questa direttiva vengono pertanto individuate le risorse da proteggere, le minacce, la capacità offensiva dei potenziali aggressori, il grado di esposizione dei sistemi, la sensibilità e l'appetibilità dei dati, per la individuazione delle vulnerabilità e la scelta delle misure di sicurezza da adottare.
- **Linee guida per l'applicazione dello schema nazionale per la valutazione della sicurezza delle tecnologie dell'informazione (approvata il 24 marzo 1998)** - definiscono, nel dettaglio, le interazioni tra i soggetti di valutazione/certificazione; tengono conto anche delle esigenze relative ai sistemi misti nazionale/NATO, che fanno riferimento anche a norme NATO**;**
- **Procedura per la condotta di valutazioni ai fini della sicurezza informatica di prodotti/sistemi EAD (approvata il 24 marzo 1998)** - definisce le responsabilità dell'EC, del CEVA, dell'Organismo richiedente, del Fornitore**.**

- **Manuale di valutazione di sicurezza informatica - Tecniche e Strumenti di Valutazione (TSV)** contiene le linee guida di carattere tecnico su come espletare le azioni del valutatore specificate da ITSEC. Tale documento è consistente con ITSEM.
- **Piano di valutazione della sicurezza di un sistema informatico** - contiene la descrizione di tutte le attività che i valutatori di un CEVA devono eseguire. Attualmente sono state redatte sino al livello E3.