Organismo di Certificazione della Sicurezza Informatica

Possibilità di integrazione nello Schema di certificazione coordinato da OCSI

Giacinto Dammicco

(ISCOM)

Presidente del Consiglio Direttivo OCSI

Organismo di Certificazione della Sicurezza Informatica

Istituzione dello Schema

- Lo **Schema Nazionale** per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione **è stato istituito con un DPCM** del 30 ottobre 2003 (G. U. n. 98 del 27 aprile 2004)

- **L'Organismo di Certificazione della Sicurezza Informatica** (OCSI) **è l'ISCOM** (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) del Ministero delle Comunicazioni

- L'OCSI agisce in conformità agli standard internazionali ISO/IEC 15408 (Common Criteria) e ai criteri europei ITSEC e ITSEM.

Organismo di Certificazione della Sicurezza Informatica

Finalità dello Schema

- Insieme delle procedure e regole necessarie per la valutazione e certificazione in conformità ai criteri Common Criteria o, se richiesto, a ITSEC

- Possono essere valutati **sistemi**, **prodotti** o **Profili di Protezione**

Organismo di Certificazione della Sicurezza Informatica

Ruoli

- Organismo di Certificazione (OCSI)
- Committente
- Fornitore
- Laboratorio per la Valutazione della Sicurezza (LVS)
- Assistente

Organismo di Certificazione della Sicurezza Informatica

Organismo di Certificazione (1/3)

- OCSI è il **certificatore unico** in ambito commerciale

  (ANS ricopre lo stesso ruolo limitatamente a prodotti e sistemi che trattano informazioni classificate)

- OCSI fornisce garanzia quale **terza parte** tra Committente e LVS

Organismo di Certificazione della Sicurezza Informatica

Organismo di Certificazione (2/3)

- Predispone regole tecniche in materia di certificazione
- Coordina le attività nell'ambito dello Schema
- Accredita i laboratori di valutazione (LVS)
- Abilita gli assistenti
- Svolge attività di formazione e addestramento
- Ammette ed iscrive le valutazioni nello Schema

Organismo di Certificazione della Sicurezza Informatica

Organismo di Certificazione (3/3)

- Supervisiona la conduzione della valutazione
- Fornisce chiarimenti sull'applicazione delle metodologie
- Approva i Rapporti Finali di Valutazione
- Emette i Rapporti di Certificazione e i Certificati
- Revoca i Certificati inficiati dalla comparsa di nuove vulnerabilità

Organismo di Certificazione della Sicurezza Informatica

Linee Guida Provvisorie (LGP)

- LGP1: Descrizione generale dello Schema nazionale
- LGP2: Accreditamento LVS e abilitazione Assistenti
- LGP3: Procedure di valutazione
- LGP4: Attività di valutazione secondo i Common Criteria
- LGP5: Il Piano di Valutazione: indicazioni generali
- LGP6: Guida alla scrittura di PP e TDS
- LGP7: Glossario e terminologia di riferimento

Organismo di Certificazione della Sicurezza Informatica

Committente

- E’ il soggetto che paga la valutazione e sceglie l’LVS
- Può coincidere con il Fornitore
- Fa da punto di contatto tra LVS e Fornitore
- Fornisce all’LVS il materiale per la valutazione

Organismo di Certificazione della Sicurezza Informatica

Fornitore

- Fornisce l'ODV
- Fornisce la documentazione al Committente
- Dà supporto al Committente nel corso della valutazione
- Risolve eventuali problemi segnalati nei Rapporti di Osservazione

Organismo di Certificazione della Sicurezza Informatica

Laboratorio per la Valutazione della Sicurezza (LVS)

Un LVS è accreditato dall'OCSI

Il personale di un LVS può:

- Svolgere la valutazione di PP o ODV
- Fornire assistenza al Committente per:
  - Stesura di documentazione
  - Verifica della valutabilità di un PP/ODV
  - Mantenimento di un Certificato

Un Valutatore che svolge assistenza per un ODV non può partecipare alla valutazione dell'ODV stesso

Organismo di Certificazione della Sicurezza Informatica

La procedura di accreditamento

L' accreditamento di un LVS si svolge in tre fasi:

1. richiesta di accreditamento
2. test di competenza e verifiche di organizzazione
3. rilascio dell'accreditamento

L'LVS **deve rispondere** alle normative internazionali (ISO17025, parte organizzativa-procedurale)

Organismo di Certificazione della Sicurezza Informatica

Durata del processo di accreditamento

La durata del processo di accreditamento è stimata in circa **60 giorni** dalla ricezione della domanda di accreditamento, a condizione che:

- il Manuale di Qualità fornito e le procedure di attuazione siano essenzialmente corretti
- il laboratorio possieda all'atto della richiesta di accreditamento tutti i requisiti formali necessari
- gli impegni economici siano stati rispettati

Organismo di Certificazione della Sicurezza Informatica

Richiesta di Accreditamento e Costi

Si può richiedere **l'accreditamento** a diversi **livelli di garanzia**:

l'OCSI consiglia l'accreditamento EAL4

Costo di accreditamento per LVS con 5 unità nel laboratorio: circa **€ 3000**

Organismo di Certificazione della Sicurezza Informatica

Competenze dell'LVS

LVS deve nel suo insieme:

- Conoscere le LG e le norme OCSI
- Conoscere i CC e ITSEC
- Saper operare secondo le unità di lavoro previste dalla CEM e in ITSEM
- Saper gestire test funzionali e di intrusione per l'identificazione delle vulnerabilità
- Saper predisporre la documentazione di valutazione

Organismo di Certificazione della Sicurezza Informatica

Competenze dei Valutatori

Nel Laboratorio devono essere presenti delle competenze per:

1. l'analisi e sintesi della documentazione
2. operare sugli oggetti da valutare (sicurezza informatica, test e vulnerabilità)

Due profili distinti di Valutatore:

documentale e operativo

Organismo di Certificazione della Sicurezza Informatica

I Valutatori

Viene riconosciuta la qualifica di “Valutatore” al personale tecnico la cui competenza sia stata verificata durante la procedura di accreditamento dell’LVS o durante una visita ispettiva periodica.

La qualifica di Valutatore è valida solo ed esclusivamente all’interno di un LVS.

Organismo di Certificazione della Sicurezza Informatica

LVS accreditati

RES	**www.consorzio-res.it**	(Pomezia)
IMQ CSQ	**www.imq.it**	(Milano)
progesoftware	**www.progesoftware.it**	(Roma)
BULL	**www.bull.it**	(Roma)

Organismo di Certificazione della Sicurezza Informatica

Assistente (1/2)

- L'Assistente deve garantire
  - L'imparzialità, l'indipendenza, la riservatezza e l'obiettività nello svolgimento del proprio ruolo
  - La capacità di mantenere nel tempo i requisiti in virtù dei quali è stato abilitato
- Requisiti
  - Competenze generali in materia di sicurezza IT
  - Conoscenza dei criteri (ITSEC/Common Criteria) di valutazione della sicurezza di sistemi o prodotti ICT e delle relative metodologie
  - Esperienza nelle metodologie di produzione della documentazione per la valutazione di un ODV

Organismo di Certificazione della Sicurezza Informatica

Assistente (2/2)

- Deve essere abilitato dall'OCSI
- Due diversi profili:
  - redazione e analisi della documentazione
  - operatività
- Può fornire consulenza tecnica ad un Committente per:
  - Stesura di documentazione
  - Verifica della valutabilità di un PP/ODV
  - Mantenimento di un Certificato

Organismo di Certificazione della Sicurezza Informatica

Profilo orientato alla *redazione e analisi della documentazione*

L'assistente con questo profilo ha la competenza per svolgere la redazione e l'analisi della documentazione inerente le attività di:

- Gestione della configurazione
- Fornitura e messa in opera
- Sviluppo
- Documentazione di utente e di amministratore
- Ciclo di vita dell'ODV
- Test

Organismo di Certificazione della Sicurezza Informatica

Profilo orientato all'*operatività*

L'assistente con questo profilo ha la competenza per:

- Progettare test
- Verificare la configurazione dell'ODV
- Condurre analisi di vulnerabilità
- Individuare vulnerabilità note
- Svolgere prove di intrusione

Organismo di Certificazione della Sicurezza Informatica

Abilitazione Assistenti

- Il candidato può decidere per uno o per tutti e due i profili previsti
- I costi relativi all'accreditamento sono pari a **€ 150** per ogni singolo profilo fino al livello di garanzia EAL4
- L'esame di abilitazione ha la durata di una giornata (prova scritta e esame orale)

Organismo di Certificazione della Sicurezza Informatica

Verifiche di competenza

- Non è necessario frequentare preliminarmente dei corsi per ottenere accreditamenti/abilitazioni
- OCSI esegue verifiche di competenza differenziate per
  - Ruolo (valutatore di un LVS o Assistente)
  - Profilo
    - Redazione e analisi della documentazione di valutazione
    - Operatività
  - Livello di valutazione
- LVS e Assistenti: validità **3 anni**

Organismo di Certificazione della Sicurezza Informatica

Strategia dell'OCSI

- Promuovere la certificazione ai **primi livelli di garanzia**, soprattutto per i **sistemi**
- Promuovere ai primi livelli di garanzia il **mantenimento** sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**
- Diffondere la certificazione di **sistema** ai **primi livelli** di garanzia nella PA, eventualmente utilizzando i Profili di Protezione, per innescare un effetto "volano"

Organismo di Certificazione della Sicurezza Informatica

Vantaggi dei primi livelli di garanzia (EAL1-2)

1) E’ comunque garantita l’assenza nell’ODV delle vulnerabilità più comuni
2) E’ abbastanza agevole **mantenere il certificato nel tempo**
3) La certificazione è **più economica e più rapida** rispetto ai livelli medio-alti di garanzia
4) Si può condurre in modo semplice **sull'intero sistema ICT**
5) I compiti di valutazione e mantenimento del certificato possono essere svolti da una ampia fascia di Assistenti di sicurezza

Organismo di Certificazione della Sicurezza Informatica

Cosa si aspetta l'OCSI da questa strategia?

Se si riuscirà ad avere numerose richieste di certificazioni ai primi livelli occorrerà:

- un numero piuttosto elevato di LVS e Assistenti
- un tipo di competenza più spostato nell'ambito delle vulnerabilità realizzative che in quello dell'analisi teorica dei documenti

Organismo di Certificazione della Sicurezza Informatica

Interazioni con lo Schema

- L'OCSI può svolgere al meglio i suoi compiti di indirizzamento tecnico, revisione tecnica e verifica delle competenze scambiando conoscenze con organizzazioni/professionisti altamente qualificati nell'area della sicurezza ICT (Associazioni, Università, Centri di ricerca, CERT, Forze di polizia, ecc.)
- La formalizzazione di queste interazioni può essere eseguita in modo da garantire un'adeguata visibilità

Organismo di Certificazione della Sicurezza Informatica

Integrazioni nello Schema

- La corretta applicazione degli standard di riferimento dipende sensibilmente dalla competenza dei valutatori e degli assistenti

- LVS e Assistenti dovrebbero quindi essere ricercati nell'ambito delle realtà che possono più facilmente avere al loro interno competenze operative nell'ambito della sicurezza ICT

Organismo di Certificazione della Sicurezza Informatica

Vantaggi dell'integrazione

- Per i fruitori del servizio di certificazione:
  - Maggiori capacità di soddisfacimento della domanda
  - Minori costi di certificazione e mantenimento in caso di uniforme distribuzione di LVS e assistenti sul territorio nazionale

Organismo di Certificazione della Sicurezza Informatica

Vantaggi dell'integrazione

- Per chi decidesse di entrare a far parte dello Schema:
  - allargamento dell'ambito della propria attività fornendo un contributo anche nell'ambito dei processi di valutazione e certificazione
  - negli altri contesti in cui opera potrebbe essere apprezzato dai possibili committenti l'accreditamento/abilitazione da parte di un organismo istituzionale che certifica la sicurezza di prodotti e sistemi ICT

Organismo di Certificazione della Sicurezza Informatica

Competenze richieste per l'integrazione (1)

- Sono dipendenti dalle modalità di applicazione degli standard di certificazione
- OCSI sta fornendo indicazioni che portano ad utilizzare gli standard nel modo che viene ritenuto più utile per l'utilizzatore finale
- In base a tali indicazioni risultano privilegiate le competenze di esperti di configurazioni di sicurezza sui sistemi ICT e quelle di coloro che eseguono test di intrusione

Organismo di Certificazione della Sicurezza Informatica

Competenze richieste per l'integrazione (2)

- Le indicazioni dell'OCSI portano infatti a certificare interi sistemi ai livelli di sicurezza iniziali (EAL1, EAL2) che prevedono produzione e analisi documentale molto limitate, ma che dovrebbero garantire l'eliminazione della causa più frequente di incidenti informatici (sfruttamento di vulnerabilità note)
- Viene inoltre raccomandato di eseguire sistematicamente il mantenimento nel tempo della certificazione, che di nuovo richiede competenze del tipo specificato

Organismo di Certificazione della Sicurezza Informatica

Competenze richieste per l'integrazione (3)

- Ai primi livelli di certificazione, quindi, potrebbe risultare piuttosto limitato lo sforzo per acquisire la conoscenza dello standard ed imparare ad applicarlo
- Inoltre OCSI potrebbe considerare, ai fini dell'accreditamento/abilitazione, titolo preferenziale il possesso di certificazioni di competenza aventi vasto riconoscimento internazionale

Organismo di Certificazione della Sicurezza Informatica

Conclusioni

- L'istituzione dello Schema nazionale offre un'opportunità per certi versi unica di sfruttare e valorizzare le migliori competenze esistenti in Italia nell'area della sicurezza ICT
- Se si riuscirà a cogliere questa opportunità si potrà offrire un servizio di certificazione realmente utile ed efficiente

Organismo di Certificazione della Sicurezza Informatica

Informazioni

www.ocsi.gov.it

MINISTERO DELLE COMUNICAZIONI

Giacinto Dammicco
ISCOM
Sessione di studio comune AIEA-ISCOM
Roma, 31 gennaio 2007

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione