



Organismo di Certificazione della Sicurezza Informatica

# L'innovativa interpretazione del ruolo di Organismo di certificazione nell'ambito dello Schema Nazionale per la certificazione della sicurezza dei sistemi/prodotti ICT (DPCM 30/10/2003)

Luisa Franchina

Infosecurity 2005 – Fiera di Milano – 11 febbraio 2005

Luisa Franchina

Direttore ISCOM

Direttore dell'Organismo di Certificazione della Sicurezza Informatica (OCSI)



Ministero delle Comunicazioni

# Lo Schema Nazionale

## (DPCM 30/10/2003)

- OCSI (Certificatore/Accreditatore unico)
- Laboratori per la Valutazione della Sicurezza (LVS)
- Assistente
- Fornitore
- Committente
- Utilizzatore

# Concetti chiave

- Prodotto
- Sistema
- Protection Profile
- Security Target
- Livello di assurance (EALx)
- Mantenimento della certificazione

# Situazione estera attuale (1)

- Vengono eseguite relativamente poche certificazioni (quasi esclusivamente di prodotto) molto costose e lunghe
- Sono i grandi produttori di sw, per lo più, a certificare i propri prodotti a livelli medi i quali, pur essendo già molto onerosi, sono però i livelli minimi che consentono lo sfruttamento a fini pubblicitari della certificazione
- L'utilizzatore finale del prodotto è spesso vittima di una pubblicità ingannevole, anche a causa dell'atteggiamento non sempre chiaro degli Organismi di certificazione

Luisa Franchina

Direttore ISCOM

Direttore dell'Organismo di Certificazione della  
Sicurezza Informatica (OCIS)

# Situazione estera attuale (2)

- E' utilizzata la certificazione dei *Protection Profile* principalmente per l'uso nella PA USA. Tali certificazioni vengono intese soprattutto come “capitolati” per la fornitura
- Sono poco diffuse le certificazioni di sistema, ad eccezione del contesto relativo alla sicurezza nazionale

# Tutela dell'utilizzatore (1)

Il mantenimento nel tempo delle certificazioni, pur essendo essenziale per l'utilizzatore, non viene attualmente eseguito perché:

- le certificazioni risulterebbero ancor più costose
- l'atteggiamento non chiaro degli Organismi di certificazione esteri consente di farne a meno in quanto
  - ci si limita a precisare che le certificazioni valgono solo nel momento in cui vengono emesse
  - non si revocano né si impedisce l'uso pubblicitario di certificazioni che non hanno più valore a seguito:
    - della scoperta di nuove vulnerabilità
    - dell'installazione di patch
    - dello sviluppo di nuove versioni del prodotto

Luisa Franchina

Direttore ISCOM

Direttore dell'Organismo di Certificazione della  
Sicurezza Informatica (OC SI)

# Tutela dell'utilizzatore (2)

- Spesso i prodotti vengono certificati in condizioni molto diverse dalle normali condizioni di utilizzo (es: sistema operativo con funzionalità di rete disattivate)
  - Anche in questo caso l'utilizzatore può essere vittima di una pubblicità ingannevole fino ad oggi consentita da una scarsa vigilanza degli Organismi di certificazione esteri
- Spesso è più importante verificare le modalità di utilizzo delle funzioni di sicurezza (configurazioni: es. firewall) nel sistema IT dell'utilizzatore, piuttosto che studiarne a fondo la struttura interna (livelli medi e alti di certificazione) sperando di trovare nuove vulnerabilità che non siano già emerse con i test funzionali e l'eventuale *penetration testing*

# Scenario italiano

- Non vi sono i grandi produttori di sw come all'estero
- Vi sono invece molti integratori di sistema
- Seguire lo stesso approccio estero comporterebbe:
  - una diffusione ancor più limitata delle certificazioni (di prodotto)
  - Una scarsa tutela dell'utilizzatore finale

# Proposta italiana: considerazioni iniziali

- Il maggior numero di incidenti informatici deriva da vulnerabilità note per le quali spesso esistono le patch
- Non ha molto senso utilizzare prodotti “molto sicuri” in sistemi complessivamente molto vulnerabili
  - Il livello di sicurezza del sistema dipende dalla robustezza dell'anello più debole della catena

# Proposta italiana: priorità

- Promuovere la certificazione a bassi livelli di assurance, soprattutto per i sistemi (vulnerabilità note assenti anche al primo livello di certificazione EAL1)
- Promuovere a bassi livelli di assurance il mantenimento sistematico dei certificati
- Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli utilizzatori
- Diffondere la certificazione di sistema a bassi livelli di assurance nella PA per innescare un effetto “volano”, similmente a quanto si sta facendo negli USA

# Vantaggi della certificazione a bassi livelli di assurance (EAL1-2)

- 1) Risulta sufficientemente agevole mantenere il certificato nel tempo
- 2) Risulta più economica e più rapida rispetto ai livelli medio-alti di assurance
- 3) Si può condurre in modo semplice sull'intero sistema ICT
- 4) E' possibile individuare una ampia fascia di potenziali Assistenti di sicurezza con le competenze necessarie per svolgere compiti di valutazione e mantenimento del certificato ai bassi livelli
- 5) Come conseguenza dei punti 3 e 4 potrebbero essere certificati molti sistemi ICT

- Riferimenti

Sito web dell'OCISI: [www.ocsi.it](http://www.ocsi.it)