Organismo di Certificazione della Sicurezza Informatica

# La sicurezza delle reti: dall'analisi del rischio alle strategie di protezione

Seconda parte

*La certificazione di sistema/prodotto*

**Luisa Franchina**, *Direttore ISCOM*

**Marco Carbonelli**, *Responsabile sezione Pre-certificazione OCSI*



MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Cosa è l'OCSI?

## L'OCSI è l'Organismo per la Certificazione della Sicurezza Informatica

Nasce attraverso il decreto

"Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione", GU n. 98 del 27-4-2004

del Ministro per l'Innovazione e le Tecnologie di concerto con i Ministri delle Comunicazioni, delle Attività Produttive e dell'Economia e delle Finanze

**Luisa Franchina**, **Marco Carbonelli**
ISCOM


MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# ISCOM, OCSI e sicurezza informatica


**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Tra i compiti dell'OCSI…

1) Rendere operativo lo Schema nazionale per la Certificazione secondo CC e ITSEC
2) Accreditare i Laboratori per la Valutazione delle Sicurezza (LVS)
3) Abilitare gli Assistenti di Sicurezza
4) Promuovere la cultura della sicurezza informatica

**Luisa Franchina**, **Marco Carbonelli**
ISCOM


MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Da dove partire per una strategia efficace?

1) Fare tesoro delle esperienze non del tutto positive delle certificazioni eseguite negli schemi esteri
2) Tenere in grande considerazione gli interessi dell'utilizzatore finale dei sistemi ICT e non solo quelli dei fornitori di prodotti
3) Prevenire le critiche che i detrattori delle certificazioni possono fondatamente muovere osservando i limiti, spesso macroscopici, delle certificazioni già eseguite

**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# In quale direzione muoversi?

- Cercare un dialogo, invece che uno scontro, con i soggetti che gestiscono certificazioni di sicurezza complementari (BS7799 e competenza del personale)
- Valorizzare il più possibile i pregi principali della certificazione: garanzia fornita da una terza parte e applicazione di uno standard internazionale
- Favorire la diffusione delle certificazioni sia in ambito pubblico sia in ambito privato

Organismo di Certificazione della Sicurezza Informatica

# I passi principali

- Individuazione di una **strategia** di applicazione degli standard di certificazione che riesca a soddisfare gli obiettivi di
  - effettiva utilità della certificazione per gli utenti
  - veloce time to market
  - affinamento dell'applicazione dei criteri
- Ampia divulgazione dei vantaggi offerti dalla **strategia**
- Avvio di adeguate iniziative che consentano di cooperare con la Certificazione di Processo e di diffondere la certificazione OCSI nel pubblico e nel privato

Organismo di Certificazione della Sicurezza Informatica

# Come vanno le cose all'estero?

Sono quasi tutte certificazioni di **prodotto** (non di **sistema**) finanziate dai fornitori che le eseguono per migliorare l'immagine del proprio prodotto

- sono eseguite a livelli di *assurance* medi o alti (altrimenti l'immagine del prodotto non risulterrebbe migliorata)
- richiedono tempi e costi elevati
- spesso vengono eseguite in condizioni piuttosto distanti da quelle tipiche di utilizzo del prodotto
- non vengono generalmente mantenute valide nel tempo, tuttavia viene consentito che si continui a pubblicizzarle

Organismo di Certificazione della Sicurezza Informatica

# La situazione non è così incoraggiante …

- 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

Organismo di Certificazione della Sicurezza Informatica

# La certificazione, i PP e i sistemi

- 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

**Luisa Franchina**, **Marco Carbonelli**
ISCOM


MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# E la tutela dell'utilizzatore?

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 o dell'installazione di patch o dello sviluppo di nuove versioni del prodotto

Organismo di Certificazione della Sicurezza Informatica

# Ma è facile orientarsi?

- Spesso i prodotti vengono certificati in condizioni molto diverse dalle normali condizioni di utilizzo (es: sistema operativo con funzionalità di rete disattivate)
- A volte dai livelli di certificazione si può essere ingannati. 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)

Organismo di Certificazione della Sicurezza Informatica

# 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

Organismo di Certificazione della Sicurezza Informatica

# Ancora considerazioni a corredo

- 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

Tutti comprendono facilmente che il **livello di sicurezza del sistema** dipende dalla robustezza dell'**anello** più debole della catena

Organismo di Certificazione della Sicurezza Informatica

# Quindi cosa fare???

Promuovere la certificazione a **bassi livelli di assurance**, soprattutto per i **sistemi** (vulnerabilità note assenti anche al primo livello di certificazione EAL1)



MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Quindi cosa fare???

Promuovere a bassi livelli di assurance il **mantenimento** sistematico dei certificati

**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Quindi cosa fare???

Stimolare la domanda di sistemi certificati agendo anche (e soprattutto) sugli **utilizzatori**

**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Quindi cosa fare???

Diffondere la certificazione di **sistema** a **bassi livelli** di assurance nella PA per innescare un effetto “volano”

**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

# Ma quali vantaggi abbiamo ai 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) Si  potrebbero certificare molti sistemi ICT, alzando di gran lunga la soglia di sicurezza del Paese

Organismo di Certificazione della Sicurezza Informatica

# Cosa si aspetta l'OCSI da questa strategia?

Se si riuscirà ad avere numerose richieste di certificazioni ai bassi 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

# Cosa ha predisposto l'OCSI?

Per poter facilitare la graduale crescita quantitativa delle risorse interne allo Schema Nazionale si è deciso

1) di prevedere accreditamenti e abilitazioni differenziate per livello di assurance e per profilo di attività
2) di non rendere obbligatoria la frequenza di costosi corsi di formazione, in modo da rendere molto accessibili sotto il profilo economico l'accreditamento degli LVS e l'abilitazione degli Assitenti
3) di prevedere, al contempo, verifiche di competenza severe e periodiche

Organismo di Certificazione della Sicurezza Informatica

# Conclusioni

Quella dell'OCSI è una importante sfida che viene condotta per innalzare il livello di sicurezza dell'intero paese.

Certificare con l'OCSI deve poter significare "**proteggere veramente**"

**Luisa Franchina**, **Marco Carbonelli**
ISCOM
Verona 25-26 maggio 2006
XX Convegno Nazionale AIEA

MINISTERO DELLE COMUNICAZIONI

iscom Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione