

**Luisa Franchina, Marco Carbonelli, Laura Gratta**

Dipartimento della Protezione Civile

**Daniele Perucchini**

Fondazione Ugo Bordoni

## **LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE: IL RUOLO DELLA CERTIFICAZIONE DI SICUREZZA**

### **(CRITICAL INFRASTRUCTURES PROTECTION: THE ROLE OF SECURITY CERTIFICATION)**

**S**ommario: i paesi maggiormente industrializzati sono dotati di sempre più estesi e sofisticati sistemi infrastrutturali, le cosiddette *Infrastrutture Critiche Nazionali* (CNI - *Critical National Infrastructures*). Appartengono a tali sistemi le infrastrutture pubbliche o private il cui corretto funzionamento è essenziale per l'operatività e la sicurezza dell'intera nazione. La presenza di queste infrastrutture consente di garantire l'efficacia operativa di molti servizi vitali per la società come la distribuzione dell'energia, i trasporti, le telecomunicazioni, la tutela della salute dei cittadini, la difesa nazionale e, in generale, tutta la pubblica amministrazione. Le CNI possono essere soggette a vari tipi di malfunzionamento, legati a problemi tecnologici o a disastri naturali o ad attacchi intenzionali. Una caratteristica tipica delle moderne CNI è quella di utilizzare in modo sempre più massiccio servizi vitali forniti dalle infrastrutture che gestiscono il trasferimento delle informazioni e la comunicazione, denominate *Infrastrutture Informatiche Critiche* (CII - *Critical Information Infrastructures*). Da questo punto di vista, le CII debbono garantire nel loro funzionamento la regolare operatività delle CNI, sia in condizioni di funzionamento normale, sia in condizioni di emergenza quando eventi critici mettono in repentaglio la fornitura dei servizi fondamentali di una nazione.

In questo lavoro viene analizzato in dettaglio il ruolo che può giocare nel contesto delle *Infrastrutture Critiche Nazionali* la certificazione di sicurezza di sistema e di prodotto. Infatti, soprattutto l'adozione di sistemi ICT certificati

può garantire l'efficacia e la correttezza delle misure di sicurezza implementate nelle CII. In particolare, il lavoro proposto discute le scelte strategiche più opportune al fine di ottenere il massimo beneficio dal processo di certificazione di sistemi ICT in termini di sicurezza.

**A**bstract: the most industrialized countries are provided with more and more wide and sophisticated infrastructural systems, the so-called *Critical National Infrastructures* (CNI). Among these systems are public or private infrastructures whose correct operation is crucial for the functioning and security of the whole country. The presence of these infrastructures allows guaranteeing the effective operation of many services essential for the society, as power distribution, transportation, telecommunications, health care, national defence, and generally speaking, all public administration.

CNIs can undergo various types of malfunctioning, due to technological problems or natural disasters or terrorist attacks. A peculiarity of modern CNIs is that they utilize more and more intensively services provided information technology infrastructures (*Critical Information Infrastructures*, CII). From this point of view, CII must guarantee the regular operation of CNIs, both during routine and emergency conditions, when critical events endanger the provision of fundamental services.

In this paper the role of system/product security certification in the context of CNIs protection is analyzed. In fact, the use of certified ICT systems

## I. Le Infrastrutture Critiche e la sicurezza

Negli ultimi anni le CNI hanno sovente sperimentato, in aggiunta alle tradizionali minacce fisiche, anche minacce alle infrastrutture tecnologiche che trattano le informazioni. Questo fenomeno è certamente riconducibile sia alla diffusione straordinaria che i sistemi dell'Information and Communication Technology (ICT) hanno vissuto nell'ultimo decennio per finalità di gestione e controllo anche nell'ambito delle Infrastrutture Critiche, sia al fatto che le CII sono potenzialmente l'obiettivo privilegiato di molti attacchi e crimini informatici soprattutto per la risonanza che tali attacchi possono ingenerare, anche grazie alla amplificazione dovuta ai mezzi di comunicazione di massa, tra i cittadini direttamente o indirettamente colpiti dal disservizio.

Accanto a queste considerazioni va tenuto in debito conto il fatto che lo scenario architetturale delle CNI sta cambiando rapidamente e molto profondamente. Fino a una decina di anni fa, una caratteristica che accomunava tutte le infrastrutture critiche era la loro indipendenza reciproca: infatti, ciascuna infrastruttura critica di per sé rappresentava un sistema pressoché autosufficiente, gestito in modo verticale da un solo operatore o da un insieme di operatori omogenei. Questa caratteristica risultava molto positiva per gli ambiti della sicurezza e della disponibilità, proprio per la chiara possibilità di individuare i problemi in un unico contesto e di assicurare l'assenza di influenze reciproche tra le infrastrutture diverse.

La necessità di ottimizzare le infrastrutture e ridurre i costi di gestione, associata all'evoluzione della tecnologia informatica e dei sistemi ICT, ha di fatto ribaltato questo originale paradigma di indipendenza e ha condotto ad una sempre maggiore interdipendenza delle infrastrutture che oggi condividono, attraverso le CII, il cosiddetto *cyberspace*, cioè uno spazio virtuale costituito da computer, sistemi di telecomunicazione, dati e applicazioni informatiche. In considerazione di questa trasformazione molti dei malfunzionamenti (accidentali o causati in modo doloso) di una infrastruttura CII possono compromettere il funzionamento delle altre, innescando un effetto domino, con disservizi che rapidamente si estendono su tutto il territorio fino agli utenti anche geograficamente molto distanti dal punto fisico in cui il malfunzionamento ha avuto origine.

Il grave blackout che si è manifestato nella maggior parte dei territori della costa nord-est degli Stati Uniti nell'agosto 2003<sup>1</sup> è un esempio eclatante di come un banale malfunzionamento in alcuni moduli del sistema di controllo di una società che forniva servizi di distribuzione di energia, sommati con altri eventi accidentali, possa condurre alla pressoché completa paralisi di tutte le infrastrutture locali, provocando danni economici ingentissimi. L'esempio riportato conferma come l'interdipendenza delle Infrastrutture Critiche sia oggi grandemente evoluta e come questo aspetto, di per sé, costituisca un nuovo elemento di vulnerabilità: l'esistenza di questa interdipendenza attraverso i sistemi che costituiscono la CII impone quindi dei requisiti ancora più stringenti in termini di caratteristiche di sicurezza delle CII stesse.

A questo punto dell'analisi la domanda che sorge spontanea è la seguente:

*quale politica debbono intraprendere le nazioni per rendere più affidabili e sicure le infrastrutture CII?*

Non è semplice rispondere a questa domanda perché gli aspetti che sono connessi con la sicurezza delle reti sono molti e spesso abbracciano ambiti completamente diversi. In questo lavoro si concentra l'attenzione sugli aspetti più propriamente connessi con la sicurezza dei sistemi e dei prodotti, cercando di fornire strumenti adeguati per poter incrementare l'affidabilità, l'idoneità e la robustezza delle funzioni di sicurezza utilizzate a fronte di obiettivi di sicurezza da raggiungere.

Dopo una breve analisi delle esigenze di sicurezza peculiari delle CII (par.2), si introducono in modo dettagliato i concetti fondamentali che caratterizzano lo standard Common Criteria (par.3). Infine (par.4) vengono discusse le modalità più opportune di applicazione della certificazione di sicurezza Common Criteria al mondo delle infrastrutture critiche nazionali.

## 2. La gestione della sicurezza nelle CII

<sup>1</sup> Il blackout dell'agosto 2003 negli USA [5] ha colpito parti del Nord-Est degli Stati Uniti e dell'est del Canada il 14 agosto 2003. È stato il più grave blackout della storia del Nord-America. Si stima che abbia interessato 10 milioni di persone nella provincia canadese dell'Ontario (circa un terzo della popolazione del Canada), e 40 milioni di persone in otto Stati degli USA (circa un settimo della popolazione USA). Le perdite finanziarie legate al blackout sono state stimate

Dalle considerazioni finora svolte emergono alcuni aspetti peculiari delle CII, che dovrebbero guidare nella predisposizione di un sistema di gestione della sicurezza delle informazioni, e che possono essere così riassunti:

- dal corretto funzionamento delle CII dipende ormai la possibilità di condurre gran parte delle attività quotidiane;
- il ruolo fondamentale delle CII le rende particolarmente appetibili come bersaglio di possibili attacchi (terroristici e non);
- le CII sono caratterizzate da una elevata complessità e interdipendenza;
- l'accesso alle CII non può essere controllato mediante misure di protezione puramente fisiche;
- un attacco condotto ai danni di una CII potrebbe portare, indirettamente, a danni ingentissimi, anche in termini di vite umane.

La messa a punto di un Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management System, ISMS) è un tema da lungo dibattuto nella comunità di standardizzazione internazionale. Lo standard ISO 27001, che raccoglie i risultati di decenni di lavoro, costituisce il riferimento per "...establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System." In base allo standard, la gestione di un sistema informativo si basa sulla comprensione dei requisiti e dei rischi, sull'individuazione delle misure per gestire i rischi, sul continuo controllo e miglioramento del sistema stesso. La certificazione ISO 27001 può essere considerata una certificazione aziendale, analogamente alla ben nota certificazione ISO 9000, ma specializzata al campo della sicurezza ICT.

Appare quindi come sia fondamentale, nella progettazione dell'ISMS di una CII, prestare la dovuta attenzione alla gestione dei rischi. In primo luogo, come è previsto dallo standard ISO 27001, il processo di gestione del rischio prevede che vengano condotte *l'identificazione e l'analisi dei rischi*, ai fini di:

1. individuare i beni da proteggere
2. individuare le minacce informatiche che possono mettere a rischio i beni
3. individuare le possibili vulnerabilità che potrebbero essere sfruttate
4. valutare l'impatto nel caso in cui le minacce

si concretizzano

5. stabilire se il rischio che deriva dall'applicazione dei passi precedenti sia compatibile con le politiche dell'ente o dell'azienda.

Non è scopo di questo lavoro approfondire i singoli aspetti dell'analisi del rischio nelle CII; tuttavia, appare evidente come il particolare contesto in cui operano le CII renda critico il processo accennato sopra.

A titolo di esempio, si consideri la seguente tabella esemplificativa dei possibili impatti per aziende ed amministrazioni pubbliche derivanti dalla riuscita di un attacco portato, ad esempio, alla integrità dei dati trattati da una CII.

Una volta acquisiti gli elementi conoscitivi per il calcolo del rischio e la successiva gestione, nel caso in cui si identifichino aree di rischio di livello non accettabile è necessario procedere alla messa in campo di protezioni e contromisure di natura sia tecnica sia organizzativa per mitigare il rischio. Utilizzando i concetti e l'impostazione proposta dallo Standard ISO 27001 per i processi, una delle opzioni per trattare il rischio è quella di realizzare dei controlli sulle protezioni adottate, sia per l'ambito tecnico sia per quello organizzativo. Tali controlli dovranno essere selezionati tra quelli previsti dallo standard al fine di soddisfare i requisiti di sicurezza identificati in fase di analisi del rischio. Ovviamente, quanto maggiore è il numero e il rigore dei controlli implementati, tanto maggiore è il costo del sistema di gestione. Quindi, la selezione dei controlli deve essere svolta bilanciando le esigenze economiche con la necessità di ridurre il rischio ad un livello accettabile specialmente in ambiti particolarmente critici.

Tra i controlli di natura tecnica, lo stesso standard ISO 27001 prevede che sistemi ICT dedicati al trattamento di informazioni critiche siano sottoposti a certificazione di sicurezza, e in particolare alla certificazione secondo lo standard Common Criteria. La presenza di tale certificazione, infatti, non solo fornisce al proprietario del sistema una importante garanzia sostanziale sull'efficacia e la corretta implementazione delle misure di sicurezza ICT, ma permette di dimostrare, laddove richiesto ad esempio per adempiere ad obblighi di legge, di aver adottato tutte le misure utili a garantire la rispondenza dei dispositivi ai requisiti dati.

Nel seguito sono fornite alcune informazioni

Impatti fisici	perdita di vite umane, o danni alle persone
	incendi, esplosioni e rilascio di sostanze nocive nell'ambiente
	danni alle infrastrutture produttive
Impatti sulla capacità produttiva(aziende)	perdita di fatturato
	perdita della customer base
	perdita della competitività commerciale
	perdita di credibilità rispetto alla capacità commerciale ed alla solvibilità finanziaria
Impatti sulla capacità di esercizio dell'attività amministrativa (PA)	perdita della fiducia degli azionisti
	disagi alla cittadinanza nell'erogazione dei servizi essenziali
Impatti legali e sulla reputazione dell'azienda o dell'amministrazione	conseguenze socio economiche della mancata o ridotta (in termini di quantità/qualità) azione amministrativa
	violazione a norme, leggi , regolamenti o impegni contrattuali precedentemente sottoscritti
	perdita dell'immagine acquisita nella società e negli stakeholder per le aziende
	perdita di credibilità del 'Sistema Paese' per le amministrazioni pubbliche

Tab. 1 – Esempi di impatto sulla sicurezza di un attacco ai dati di una CII

utili a comprendere la filosofia in base alla quale operano i Common Criteria, e su come tali criteri possano essere efficacemente impiegati nel campo delle CII.

### 3. Valutazione e certificazione della sicurezza ICT

L'espressione "certificazione della sicurezza" identifica la certificazione, fornita da una terza parte indipendente, qualificata e ufficialmente riconosciuta, della conformità di un sistema, prodotto, processo o servizio rispetto ai requisiti di sicurezza definiti da una standard o una norma di riferimento.

Gli aspetti fondamentali che rendono utile ed efficace un processo di valutazione e certificazione della sicurezza sono l'efficacia provata degli standard di riferimento e le garanzie di terza parte che gli organismi di certificazione offrono agli utenti finali, gli sviluppatori di sistemi e prodotti, i committenti delle certificazioni.

Nel caso specifico delle certificazioni di sicurezza, il primo aspetto si può considerare soddisfatto dal momento che vengono applicati standard internazionali, testati nel corso del tempo da soggetti indipendenti, e che sono definite modalità implementative che, da una parte, si sono dimostrate utili nell'aumentare il livello di sicurezza e,

d'altra parte, consentono una efficace integrazione delle misure di sicurezza con i processi di produzione e utilizzo impiegati.

Per quanto riguarda il secondo aspetto, una garanzia significativa sulla natura di terza parte del processo di certificazione può essere rappresentata dal fatto che gli organismi di certificazione sono ufficialmente incaricati di svolgere questo ruolo dai governi delle Nazioni in cui operano, e sono generalmente riconosciuti da organizzazioni internazionali indipendenti.

Il processo di valutazione e certificazione della sicurezza deve quindi possedere le seguenti caratteristiche:

- la ripetibilità: la valutazione dello stesso oggetto effettuata in tempi diversi in relazione agli stessi requisiti di sicurezza e dallo stesso Valutatore deve portare agli stessi risultati;
- la riproducibilità: la valutazione dello stesso oggetto effettuata con gli stessi requisiti di sicurezza da un diverso Valutatore deve portare agli stessi risultati;
- l'imparzialità: la valutazione deve essere condotta senza pregiudizi e, in particolare, deve essere possibile dimostrare che i valutatori coinvolti non abbiano interessi commerciali o finanziari dipendenti dall'esito della valutazione stessa;
- l'oggettività: le conclusioni del processo di

valutazione devono essere motivate da evidenze sperimentali ogni qual volta sia realizzabile, in modo da limitare il più possibile opinioni e valutazioni soggettive.

Attualmente i due standard di riferimento per la certificazione di sicurezza ICT sono lo standard ISO 15408 [1,2,3] (Common Criteria-CC) e lo standard ISO 27001 [4]. Questi standard mirano a certificare due cose ben distinte: nel caso dei Common Criteria, l'oggetto della valutazione (ODV) è un *sistema o prodotto* ICT<sup>2</sup>; nel caso dello standard ISO 27001 viene certificato un processo impiegato in un'organizzazione, sia questa una società privata o una struttura pubblica, per gestire internamente la sicurezza ICT. Specificare l'oggetto della certificazione è un elemento fondamentale, poiché alcune caratteristiche dello standard ISO 27001 potrebbero indurre in errore gli utenti facendo credere che la certificazione ISO 27001 renda la certificazione ISO 15408 praticamente superflua. In realtà, tra i requisiti che una organizzazione deve soddisfare per ottenere una certificazione ISO 27001 alcuni costituiscono requisiti funzionali di sicurezza dei prodotti/sistemi ICT dell'organizzazione. Tuttavia, ai fini della certificazione ISO 27001, è sufficiente verificare che i requisiti suddetti siano stati selezionati sulla base di un processo corretto di analisi e gestione del rischio, e che le corrispondenti funzionalità di sicurezza siano state implementate nelle infrastrutture ICT in base alle necessità. Ai fini della certificazione di sistema/prodotto Common Criteria, invece, è necessario verificare che le funzionalità implementate non abbiano difetti nella progettazione e realizzazione e siano in grado di resistere, fino ad una data soglia, ad un insieme di minacce definite nel loro ambiente operativo.

### 3.1 I Common Criteria

Nel 1999 l'ISO (International Standardization Organization) ha adottato una serie di criteri, noti come "Common Criteria", che consentono la valutazione e certificazione della sicurezza di prodotti

<sup>2</sup> Un sistema ICT, secondo la terminologia utilizzata nei CC, è una installazione IT utilizzata per uno scopo definito in un ambiente operativo completamente definito. Un prodotto ICT, invece, è un dispositivo hardware o un pacchetto software destinato per un uso generico in un'ampia gamma di

e sistemi ICT. Ciò ha dato luogo all'emissione dello standard ISO 15408. La versione dello standard attualmente utilizzata è la versione 2.3; la versione 3.0 è in corso di finalizzazione, e viene utilizzata come versione "trial" da alcuni organismi di certificazione.

In Italia le certificazioni di sicurezza di sistema/prodotto sono state condotte fin dal 1995 nel campo della sicurezza nazionale, relativamente a sistemi che trattano dati classificati. Al fine di consentire la certificazione di sistemi e prodotto ICT nel settore commerciale secondo gli standard ITSEC e CC, nel 2004 [6] è stato istituito l'Organismo di Certificazione della Sicurezza Informatica (OCSI) [7]. L'OCSI svolge il ruolo di Organismo di certificazione all'interno dello Schema Nazionale di Certificazione di prodotti/sistemi commerciali.

Lo Schema Nazionale definisce le procedure e le regole nazionali per la valutazione e certificazione di prodotti e sistemi ICT, in conformità ai criteri europei ITSEC e ai Common Criteria.

La filosofia che è alla base dei CC è stata ripresa dai precedenti criteri europei ITSEC (Information Technology Security Evaluation Criteria) che per primi l'hanno introdotta. In base a tale filosofia non ha senso verificare se un sistema/prodotto è sicuro se non si specifica:

- "sicuro" per fare cosa (obiettivi di sicurezza)
- "sicuro" in quale contesto (ambiente di sicurezza)
- "sicuro" a fronte di quali verifiche (requisiti di assurance).

Un *obiettivo* di sicurezza viene definito, secondo i CC, come l'intenzione di contrastare una minaccia o quella di rispettare leggi, regolamenti o politiche di sicurezza preesistenti. Il conseguimento degli obiettivi avviene attraverso l'adozione di misure di sicurezza tecniche (funzioni di sicurezza) e non tecniche (fisiche, procedurali e relative al personale).

L'ambiente di sicurezza viene descritto in termini di:

- uso ipotizzato del sistema/prodotto (applicazioni, utenti, informazioni trattate ed altri beni con specifica del relativo valore)
- ambiente di utilizzo (misure di sicurezza non tecniche, collegamento con altri apparati)

ICT)

- minacce da contrastare, specificando caratteristiche dell'attaccante (conoscenze, risorse disponibili e motivazione), metodi di attacco (citando, tra l'altro, lo sfruttamento di eventuali vulnerabilità note del sistema/prodotto ICT), beni colpiti
- politiche di sicurezza dell'Organizzazione.

Le verifiche previste durante il processo di valutazione mirano ad accertare che siano stati soddisfatti, da parte del sistema/prodotto, del suo sviluppatore e del valutatore, opportuni requisiti di assurance che diventano sempre più severi al crescere del livello di valutazione. I CC definiscono una scala di 7 livelli di valutazione (EAL1, EAL2,..., EAL7) o livelli di *assurance*, precisando, per ogni livello di tale scala uno specifico insieme di requisiti di assurance.

Le verifiche, eseguite in base ai requisiti di assurance del livello di valutazione considerato, hanno lo scopo di fornire garanzie circa:

- l'idoneità delle funzioni di sicurezza a soddisfare gli obiettivi di sicurezza del sistema/prodotto;
- l'assenza di errori nel processo che dalle specifiche iniziali di sicurezza (ambiente e obiettivi di sicurezza) porta alla pratica realizzazione delle funzioni di sicurezza (errori di interpretazione delle specifiche tecniche, errori di programmazione, ecc);

Nella tabella che segue sono brevemente riassunte le garanzie fornite dai sette livelli di assurance dei CC.

La parte 3 dei Common Criteria [3] definisce un catalogo dei requisiti di assurance, ovvero delle azioni di valutazione che devono essere svolte dai valutatori ai diversi livelli di assurance.

Al crescere del livello di assurance:

- vengono richieste specifiche realizzative più dettagliate (ad esempio progetto ad alto livello, progetto a basso livello, codice sorgente)
- il livello di rigore con il quale le specifiche devono essere descritte aumenta (descrizione informale, semiformale, formale)
- ai valutatori è richiesto di svolgere analisi più dettagliate e approfondite (test funzionali,

prove di intrusione).

La fig. 1 mostra, per ogni livello di assurance, il livello di rigore della descrizione delle specifiche (area in grigio) e le principali verifiche svolte nel corso della valutazione (area in bianco).

Le funzioni di sicurezza del sistema/prodotto sono descritte sulla base dei requisiti che devono essere soddisfatti. Questi requisiti, chiamati *requisiti funzionali*, devono essere descritti (salvo eccezioni che devono comunque essere motivate) usando il catalogo di componenti contenuto nella parte 2 dei CC [2].

I requisiti funzionali descritti nella parte 2 dei CC sono organizzati in 11 classi: *Audit, Comunicazione, Supporto crittografico, Protezione dei dati di utente, Identificazione e autenticazione, Gestione della sicurezza, Privacy, Protezione delle funzioni di sicurezza dell'ODV, Utilizzo delle risorse, Accesso all'ODV, Canali fidati*.

Il catalogo di componenti funzionali fornito dai CC è di fondamentale importanza, poiché permette di confrontare diversi prodotti sulla base delle funzionalità di sicurezza che offrono; in effetti, l'utilizzo di un catalogo universale di funzioni di base crea un linguaggio comune per la descrizione delle misure di sicurezza.

Le misure di sicurezza realizzate nell'ODV sono descritte, in termini dei componenti funzionali suddetti, in un documento chiamato Security Target. Questo documento, che costituisce un riferimento nel corso di tutto il processo di valutazione, deve descrivere gli obiettivi di sicurezza, l'ambiente di sicurezza, i requisiti funzionali e di assurance (e quindi il livello di assurance della valutazione), e deve fornire una descrizione ad alto livello delle funzioni di sicurezza.

Come emerge da questa introduzione sulle caratteristiche dei Common Criteria, l'impiego sistematico della certificazione di sicurezza secondo tali criteri può comportare molti vantaggi. I principali sono:

- la verifica, eseguita da una terza parte per la quale viene riconosciuto il possesso di conoscenze specialistiche, che le funzionalità di sicurezza del sistema/prodotto ICT, affiancate alle contromisure non tecniche previste, siano adeguate al soddisfacimento degli obiettivi di sicurezza
- lo svolgimento di un'azione di contrasto preventivo degli incidenti di sicurezza ICT;

EAL1	<p>Adeguato quando sia richiesta una qualche garanzia sulla corretta funzionalità, ma le minacce alla sicurezza non siano considerate gravi. Utile nei casi in cui sia richiesta una garanzia di terza parte per supportare la tesi del fornitore che sia stata dedicata la cura dovuta riguardo alla protezione dei dati e delle informazioni.</p> <p>EAL1 fornisce una valutazione dell'ODV così come reso disponibile al cliente, compresa un'attività di test indipendente svolta dai valutatori e un esame dei manuali d'uso. Questo livello di garanzia fornisce un aumento dell'assurance rispetto ad un prodotto/sistema ICT non valutato.</p>
EAL2	<p>Richiede una cooperazione da parte del fornitore dell'ODV in termini di messa a disposizione di informazioni di progetto e risultati di test, ma non dovrebbe richiedere da parte del fornitore un effort maggiore rispetto a ciò che deriva dall'applicazione di buone pratiche di sviluppo. Di conseguenza, non dovrebbe comportare un investimento sensibile in termini di costi o tempi.</p> <p>EAL2 è quindi applicabile nelle circostanze in cui il fornitore o gli utenti richiedano una garanzia di sicurezza indipendente ad un livello basso-moderato, in assenza della disponibilità di tutta la documentazione di sviluppo. Questa situazione si può verificare in presenza di sistemi pre-esistenti, che richiedano tuttavia la garanzia di una certificazione di terza parte con una disponibilità limitata da parte del fornitore. Questo livello rappresenta un incremento della sicurezza rispetto ad EAL1, poiché richiede lo svolgimento di test specifici da parte del fornitore, una analisi di vulnerabilità, e un'attività di test indipendente sulla base di specifiche più dettagliate.</p>
EAL3	<p>Permette al fornitore di ottenere la massima garanzia a partire da un buon processo di ingegnerizzazione in fase progettuale, senza richiedere modifiche sostanziali delle esistenti pratiche di sviluppo. EAL3 è applicabile nei casi in cui il fornitore o gli utenti richiedano una garanzia di sicurezza indipendente ad un livello moderato, e richiedano una approfondita analisi dell'ODV e del suo sviluppo senza una sostanziale reingegnerizzazione.</p> <p>Questo livello rappresenta un'incremento della sicurezza rispetto ad EAL2, poiché richiede un test più completo delle funzionalità di sicurezza, e alcune garanzie sul fatto che l'ODV non possa essere stato manomesso in fase di sviluppo.</p>
EAL4	<p>Permette al fornitore di ottenere la massima garanzia a partire da un buon processo di ingegnerizzazione in fase progettuale. EAL4 è il più alto livello di garanzia al quale è verosimile che sia economicamente praticabile certificare una linea di prodotti preesistente. EAL4 è quindi applicabile nei casi in cui il fornitore o gli utenti richiedano una garanzia di sicurezza indipendente ad un livello moderato-alto, e siano disposti ad incorrere in costi aggiuntivi di ingegnerizzazione specifici per la sicurezza.</p> <p>Questo livello rappresenta un incremento della sicurezza rispetto ad EAL3, poiché richiede che il fornitore metta a disposizione dei valutatori una descrizione progettuale più completa, un sottoinsieme della rappresentazione dell'implementazione, e maggiori garanzie sul fatto che l'ODV non possa essere stato manomesso in fase di sviluppo e consegna.</p>
EAL5	<p>Permette al fornitore di ottenere la massima garanzia a partire da un processo rigoroso di ingegnerizzazione in fase progettuale, supportato dall'applicazione di tecniche di ingegneria della sicurezza specialistiche. EAL5 è applicabile nei casi in cui il fornitore o gli utenti richiedano una garanzia di sicurezza indipendente ad un livello alto, pianificata a livello di sviluppo, e richiedano un'approccio di sviluppo molto rigoroso senza incorrere in costi irragionevoli.</p> <p>Questo livello rappresenta un'incremento della sicurezza rispetto ad EAL4, poiché richiede che il fornitore metta a disposizione dei valutatori una descrizione progettuale descritta in linguaggio semi-formale, l'intera rappresentazione dell'implementazione, un'architettura strutturata, un'analisi dei canali nascosti, e maggiori garanzie sul fatto che l'ODV non possa essere stato manomesso in fase di sviluppo e consegna.</p>
EAL6	<p>Permette al fornitore di ottenere la massima garanzia a partire da un processo rigoroso di ingegnerizzazione in fase progettuale, supportato dall'applicazione tecniche di ingegneria della sicurezza specialistiche, al fine di produrre un ODV con elevate prestazioni di sicurezza per proteggere beni di elevato valore contro rischi significativi. EAL6 è applicabile allo sviluppo di ODV che devono essere impiegati in situazioni di alto rischio, in cui il valore dei beni da proteggere giustifica i costi aggiuntivi.</p> <p>Questo livello rappresenta un incremento della sicurezza rispetto ad EAL5, poiché richiede che il fornitore dimostri la realizzazione di un'architettura maggiormente strutturata, un'analisi sistematica dei canali nascosti, l'utilizzo di sistemi sofisticati di controllo della configurazione, e richiede che il valutatore svolga un'analisi di vulnerabilità e prove di intrusione più rigorose.</p>
EAL7	<p>E' applicabile per lo sviluppo di ODV che devono essere impiegati in contesti soggetti ad altissimo rischio, e in cui l'elevato valore dei beni da proteggere giustifica i costi elevati. L'applicazione del livello EAL7 è attualmente limitata ad ODV con funzionalità di sicurezza molto ristrette, che però possono essere sottoposti ad un'analisi formale rigorosissima.</p> <p>Questo livello rappresenta un incremento della sicurezza rispetto ad EAL6, poiché richiede l'utilizzo di rappresentazioni formali per le analisi svolte, e lo svolgimento di campagne esaustive di prove di intrusione e test funzionali.</p>

Tab. 2 – Livelli di assurance dei Common Criteria

	Descrizione delle specifiche funzionali	Descrizione del progetto ad alto livello	Descrizione del progetto a basso livello	Rappresentazione dell'implementazione	Test funzionali	Prove di intrusione	Gestione della configurazione	Consegna e installazione	Sicurezza dell'ambiente di sviluppo	Strumenti di sviluppo
EAL0	-	-	-	-	-	-	-	-	-	-
EAL1	Informale	-	-	-	X	-	X	X	-	-
EAL2	Informale	Informale	-	-	X	X	X	X	-	-
EAL3	Informale	Informale	-	-	X	X	X	X	X	-
EAL4	Informale	Informale	Informale	Parziale	X	X	X	X	X	X
EAL5	Semi-formale	Semi-formale	Informale	Completa	X	X	X	X	X	X
EAL6	Semi-formale	Semi-formale	Semi-formale	Strutturata	X	X	X	X	X	X
EAL7	Formale	Formale	Semi-formale	Strutturata	X	X	X	X	X	X

- = assente  
x = presente

Fig 1 - Aumento della complessità della valutazione ai diversi livelli di assurance dei CC

- la disponibilità di vasti cataloghi relativamente alle funzionalità di sicurezza ICT e ai requisiti di assurance adottabili;
- la possibilità di esprimere in forma standardizzata requisiti di sicurezza per sistemi e prodotti ICT.

Ovviamente, la certificazione CC è uno strumento che deve essere utilizzato correttamente per risultare efficace. Nel capitolo successivo sono evidenziati alcune problematiche che devono essere affrontate al fine di massimizzare i benefici della certificazione nel contesto nazionale e per la sua applicazione nell'ambito della CII.

#### 4. La certificazione Common Criteria dal punto di vista delle CII

Come è stato evidenziato, la certificazione Common Criteria è uno strumento molto com-

plesso, i cui numerosi parametri debbono essere opportunamente regolati per ottenere il massimo beneficio in termini di sicurezza. Nella messa a punto di una strategia di certificazione per le CII devono essere presi in considerazione gli aspetti fondamentali legati all'adozione sistematica della certificazione di sistema, alla sinergia con la certificazione ISO 27001, alla politica di gestione delle patch e al mantenimento nel tempo del certificato. Tali fattori sono approfonditi nel seguito.

#### **Ambito delle certificazioni: adozione della certificazione di sistema**

Il principio dell'anello più debole in una catena suggerisce che l'impiego di prodotti certificati (eventualmente a livelli di garanzia molto alti) in un contesto non sicuro non fornisce alcun vantaggio complessivo. Di conseguenza, una certificazione di sicurezza limitata ad una specifica parte di un siste-

ma complesso non ha molto senso se non si riesce a garantire un livello minimo omogeneo di sicurezza. Purtroppo, in molti casi è invece invalso l'uso di acquisire prodotti ICT certificati, eventualmente a livelli di assurance medio-alti, senza porre attenzione alla sicurezza complessiva del sistema integrato. Dall'analisi dei dati sulle certificazioni CC commerciali emesse in tutto il mondo (Fig. 2) emerge che quasi tutte le certificazioni emesse da schemi commerciali riguardano prodotti; inoltre, le certificazioni EAL4 superano in numero quelle di qualsiasi altro livello di garanzia.

In casi quali le CII, in cui i servizi sono forniti mediante l'integrazione di un complesso insieme di sistemi e prodotti, la certificazione di sicurezza potrebbe fornire garanzie consistenti se fosse sottoposto a valutazione l'intero sistema ICT di gestione dell'infrastruttura, anche se ad un basso livello di garanzia. Questo garantirebbe che le caratteristiche di sicurezza dell'intero sistema, compresi gli aspetti operativi quali la configurazione, siano state sottoposte a test. Va sottolineato che proprio gli aspetti operativi hanno un impatto notevole sulla sicurezza, in quanto nella fase operativa del ciclo di vita di un sistema ICT molti problemi di sicurezza derivano da una scarsa attenzione alla messa in sicurezza della configurazione del sistema stesso.

Un ulteriore aumento della sicurezza complessiva del sistema potrebbe essere ottenuta se il processo di certificazione CC fosse svolto in sinergia con la certificazione di processo ISO 27001, il che porterebbe ad una gestione comple-

ta di tutti gli aspetti di sicurezza del ciclo di vita del sistema.

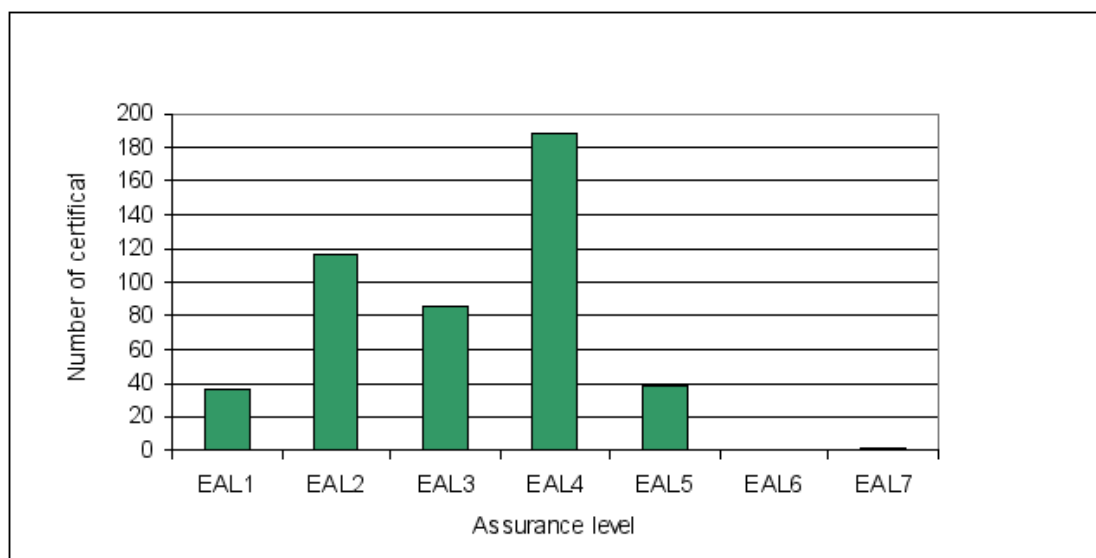
#### ***Natura degli incidenti di sicurezza: la gestione delle patch***

L'esperienza e i bollettini di sicurezza pubblicamente disponibili mostrano che la maggior parte degli incidenti di sicurezza sono dovuti allo sfruttamento di vulnerabilità note, per le quali esistono già le patch. Quindi, una politica di sicurezza che presti la dovuta attenzione al monitoraggio, al test e all'installazione delle patch potrebbe prevenire lo sfruttamento di molte potenziali vulnerabilità.

#### ***Efficacia della certificazione: il mantenimento***

L'efficacia della certificazione di sistema/prodotto è intrinsecamente limitata dalla rapida evoluzione dello scenario degli attacchi e delle vulnerabilità. In linea di principio, l'analisi di vulnerabilità e le prove di intrusione condotte dai valutatori sull'ODV potrebbero portare a risultati differenti se fossero condotti il giorno successivo all'emissione del certificato, a causa della messa a punto di nuovi metodi di attacco. Ovviamente, questo sarebbe un caso limite; nei casi reali, se l'insieme delle misure ICT e delle ipotesi ambientali implementate nell'ODV sono state realizzate e valutate attentamente, l'ODV stesso sarà almeno in grado di mitigare i danni di un attacco.

D'altro canto, la certificazione emessa ha valore unicamente se l'ODV è configurato e usato



nelle stesse condizioni nelle quali è stato valutato e, quindi, senza l'aggiunta di patch di sicurezza. Questo mette il proprietario di un sistema ICT di fronte ad un dilemma:

*mantenere il sistema in sicurezza, installando le patch necessarie, o lasciare il sistema nella configurazione certificata, sebbene esposto a potenziali vulnerabilità?*

Su questa domanda si gioca il reale contributo che la certificazione può dare al livello di sicurezza dei sistemi ICT. La sfida consiste nel fornire un framework all'interno del quale possano essere apportate ai sistemi certificati alcune modifiche (tipicamente patch di sicurezza) volte ad allineare l'assetto di sicurezza con il panorama corrente delle minacce. Soprattutto per sistemi basati su prodotti COTS (*Commercial Off The Shelf*) di largo consumo, il rapido insorgere di nuove vulnerabilità rende indispensabile il continuo aggiornamento del software, il che è incompatibile con la conduzione di un nuovo processo di certificazione ad ogni aggiornamento.

Tenendo conto delle considerazioni svolte, i requisiti individuati per una efficace applicazione della certificazione alle CII possono essere così riassunti:

- applicare la certificazione all'intero sistema CII, integrata con la certificazione di processo;
- utilizzare la certificazione a bassi livelli di assurance, riducendo drasticamente i tempi e i costi di certificazione, al fine di estendere il grado di penetrazione della certificazione e ottenere un livello base comune di sicurezza in tutte le CNI;
- applicare una sorta di mantenimento della certificazione, al fine di proteggere le CNI dall'insorgere di nuove vulnerabilità nello scenario in evoluzione della sicurezza ICT.

## 5. Conclusioni

La necessità di proteggere le infrastrutture critiche di una nazione impone l'individuazione di nuove politiche che aumentino la sicurezza delle CNI, innescando un processo virtuoso per la sicurezza di tutta la nazione. Dopo aver introdotto i concetti fondamentali di CNI e CII, si è condotta un'analisi per dimostrare come si renda sempre

più necessario un miglioramento delle funzionalità di sicurezza impiegate nelle infrastrutture che costituiscono il cyberspace, cioè lo spazio virtuale dove viaggiano e vengono elaborate e conservate le informazioni. L'applicazione degli standard ISO di sicurezza sia a livello di processo sia a livello di sistema possono consentire di migliorare la sicurezza complessiva delle infrastrutture. In particolare, l'analisi si è soffermata sulla certificazione di sistema e sui vantaggi che l'applicazione dello standard Common Criteria ai bassi livelli di certificazione potrebbe comportare nelle infrastrutture critiche nazionali.

## 6. Riferimenti Bibliografici

[1] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", version 2.3, part 1, august 2005.

[2] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part 2 – Introduction and general model", version 2.3, part 2, august 2005.

[3] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation, Part 3 – Introduction and general model", version 2.3, part 3, august 2005.

[4] ISO 27001, "Information Security Management - Specification With Guidance for Use" October 2005

[5] US-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Black out in the United States and Canada: Causes and Recommendations", April 2004, available together with further information at <http://www.ksg.harvard.edu/hepg/Blackout.htm>

[6] DPCM 30 ottobre 2003, "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

[7] <http://www.ocsi.isticom.it/>