Spiegare come deve variare la modalità descrittiva delle funzionalità di sicurezza al crescere del livello di garanzia a cui viene eseguita una certificazione ISO/IEC 15408 (Common Criteria).

Autore: Guzzo Antonio
In: Diritto civile e commerciale

Prima di passare ad esaminare come deve variare la modalità descrittiva delle funzionalità di sicurezza al crescere del livello di garanzia a cui viene eseguita una certificazione ISO/IEC 15408 è necessario definire dapprima i concetti di livelli di garanzia e di funzioni di sicurezza. In un sistema ict sicuro reale non possono essere fornite delle garanzie assolute circa la sicurezza del sistema ict. Quello che si deve fare è fornire una garanzia non completa e graduata secondo certi livelli (livelli di garanzia o assurance level). Questi livelli sono sostanzialmente le modalità con cui si misura quanto si ci può fidare della sicurezza di questo sistema ICT reale. Il concetto centrale che interviene è questo dell'assurance cioè della garanzia che può essere graduata. In realtà questi criteri prevedono un'altra gradazione che concerne specificatamente funzioni di sicurezza, basate su analisi di tipo probabilistico (ad es. funzioni hash o funzioni che utilizzano password). Per questi specifici tipi di funzioni di sicurezza è prevista che venga adottata una scala di valori che serve a misurare la robustezza di queste funzioni di sicurezza. Per quanto concerne i livelli di garanzia dobbiamo distinguere nell'ambito dell'approccio generale due principali tipi di verifica:

Livelli di garanzia

Diritto & Diritti ISSN 1127-8579

Verifiche di tipo 1

di progettazione della sicurezza del sistema ict. Ci troviamo nello specifico nella fase in cui utilizzando il processo di analisi dei rischi si vanno a selezionare delle contromisure tecniche (in particolare le funzioni di sicurezza) per contrastare minacce che potrebbero violare gli obiettivi di sicurezza).Le verifiche di tipo 1 controllano che vi siano tutte le funzioni di sicurezza necessarie, che siano in grado di cooperare efficacemente e che la robustezza dichiarata sia confermabile teoricamente.

Verifiche di tipo 2

incominciare a preoccuparci di quanto possiamo fidarci di queste funzioni). Qui intervengono le verifiche di tipo 2 dove si va a controllare, con una severità dipendente dal livello di garanzia, che il software/hardware con cui le funzioni sono realizzate esibisca nelle effettive condizioni di utilizzo il comportamento teorico previsto a fronte di eventi accidentali o di attacchi.
A tal proposito le verifiche di tipo 1 hanno lo scopo di controllare che non vi siano errori già nella fase di impostazione della progettazione delle funzionalità di sicurezza del sistema ICT. Un esempio ci viene dato dall'assenza di una funzione di sicurezza. A tal proposito le verifiche di tipo 2 vengono definite graduandole in funzione del livello di garanzia e tenendo conto del fatto che la sicurezza del sistema ICT può essere assimilata alla resistenza di una catena che dipende dalla resistenza del suo anello più debole. Passiamo ora ad esaminare le tipologie relative alle verifiche di tipo 2 precedentemente accennate. In particolare viene previsto che colui che chiede la certificazione debba documentare il modo in cui le funzionalità di sicurezza sono state progettate e

realizzate. Questa documentazione che è richiesto che lui fornisca, deve essere sviluppata secondo certi criteri che fanno si che possano esistere vari tipi di descrizioni di queste funzionalità di sicurezza a vari livelli di generalità cioè da un livello di generalità più elevato, via via con dettagli sempre più spinti si passa a modalità di descrizione più precise fino ad arrivare a quella ultima che corrisponde all'implementazione delle funzionalità di sicurezza. Per cui partendo dall'alto e cioè dalle descrizioni a più alto livello di queste funzioni di sicurezza (utilizzando una terminologia classica dei COMMON CRITERIA) avremo una descrizione delle funzioni di sicurezza che prende il nome di specifica delle funzioni di sicurezza (cioè una descrizione ad alto livello (ciò che un utente può osservare dall'esterno) del comportamento e dell'interfaccia delle funzioni di sicurezza). Quando si passa al successivo livello descrittivo definito progetto ad alto livello, già è necessario fornire delle informazioni più precise e cioè descrivere l'insieme delle funzioni di sicurezza in termini di sottosistemi, ossia di unità strutturali macroscopiche che a seconda dei casi possono realizzare una funzione di sicurezza, parte di essa o più funzioni di sicurezza. Il terzo livello, procedendo quindi ad un analisi maggiormente dettagliato, è quello relativo al progetto a basso livello che descrive il modo di operare interno delle funzioni di sicurezza in termini di piccoli moduli per i quali vengono specificate le operazioni svolte, le interfacce ed i modi di interazione. L'ultimo livello è quello della vera e propria implementazione (ad esempio il codice sorgente di un prodotto software) che descrive l'implementazione in termini di codice sorgente, firmware, disegni hardware fornendo quindi il massimo livello di dettaglio circa il funzionamento interno delle funzioni di sicurezza del TOE (Target of Evaluation Obiettivo di Valutazione). In questo caso arriviamo al livello di dettaglio massimo quello in cui è possibile avere tutte le informazioni relative

alle modalità secondo cui la funzionalità di sicurezza è stata realizzata. Avendo parlato sino ad ora di livelli di garanzia non è previsto che sempre sia necessario fornire delle indicazioni descrittive delle funzionalità di sicurezza al livello massimo fino all'implementazione. Inoltre l'altra modalità secondo la quale si può differenziare queste descrizioni delle funzioni di sicurezza in funzione del livello di garanzia al quale è stata richiesta la certificazione è quello della modalità descrittiva utilizzata ad uno di questi livelli già accennati. Per ciascuna di queste descrizioni delle funzioni di sicurezza è prevista dalle norme di riferimento che si possa adottare uno stile diverso cioè è previsto uno stile che può essere descritto in modo informale (indicato con i termini informal o descriptive), semiformale e formale. **Man mano che il livello di garanzia cresce non viene più accettato che le** cose si descrivano in modo ambiguo (cioè con il linguaggio naturale) ma è richiesto che si adottino linguaggi formali o semi-formali che consentano di ridurre al minimo la possibilità di non indicare con precisione ciò che fanno le funzionalità di sicurezza. Il primo concetto è che si ricorrerà alle descrizioni più accurate solo quando i livelli di garanzia sono elevati, il secondo che le descrizioni delle funzioni di sicurezza possono essere fatte tramite diversi stili (formale-semiformale). Quindi riassumendo al crescere del livello di valutazione vengono richieste specifiche realizzative più dettagliate (ad esempio il progetto a basso livello in luogo di quello ad alto livello) ed il livello di rigore con il quale le specifiche devono essere descritte aumenta (ad esempio descrizione formale invece che semiformale).

a cura del Dottor Antonio Guzzo – Responsabile CED – Sistemi Informativi del Comune di Praia a Mare

Diritto & Diritti ISSN 1127-8579

(una volta che queste verifiche siano state previste nel sistema ict ha senso(ad alto livello che servono ad evidenziare le eventuale presenza di errori in fase

https://www.diritto.it/spiegare-come-deve-variare-la-modalita-descrittiva-delle-funzionalita-di-sicurezza-al-crescere-del-livello-di-garanzia-a-cui-viene-eseguita-una-certificazione-isoiec-15408-common-criteria/

Diritto & Diritti ISSN 1127-8579