Valutazione automatica e continua della compliance in ambienti cloud: il caso di studio FedRAMP

Patrizio Tufarolo (matricola 875041)

18.05.2017

Relatore: Prof. Claudio A. Ardagna

Correlatore: Dott. Marco Anisetti
Prof. Ernesto Damiani

L'adozione del paradigma permette alle organizzazioni di usufruire di vantaggi prestazionali ed economici nell'erogazione dei servizi IT, grazie sia alle caratteristiche di scalabilità ed elasticità proprie del paradigma, che alla possibilità di allocare risorse in modalità *on-demand*. Tuttavia, la natura distribuita ed automatizzata della cloud introduce numerose problematiche di sicurezza e valutazione del rischio, soprattutto per tutte quelle realtà in procinto di effettuare migrazioni parziali o totali delle loro infrastrutture tradizionali. Infatti, per trarre effettivo vantaggio dalla centralizzazione degli aspetti di sicurezza nelle mani di un *cloud service provider*, è necessario stabilire un rapporto di fiducia reciproca tra il fornitore del servizio e il cliente, in modo da minimizzare il rischio e limitare il perimetro di attacco, e stabilire le responsabilità di ogni entità coinvolta.

Questo lavoro di tesi si pone sull'ambito della ricerca sulla *security assurance*, basata su attività di testing, monitoraggio e controllo della *compliance*; l'obiettivo è l'analisi di FedRAMP, il programma governativo americano per la valutazione del rischio e l'autorizzazione dell'utilizzo di servizi cloud nelle agenzie federali.

È stata quindi implementata un'integrazione tra i controlli di sicurezza descritti nel documento NIST SP 800-53, su cui FedRAMP è basato, e Moon Cloud, una piattaforma a micro-servizi per la trasparency, l'assessment e il monitoraggio continuativo di proprietà non funzionali.

Il lavoro di tesi vuole quindi assumere un ruolo di supporto per tutti gli attori coinvolti nel processo di autorizzazione di FedRAMP, in particolare i fornitori di servizi che vogliano attestarne la *readiness*.

Infine, il lavoro è stato validato mediante l'esecuzione dei controlli di sicurezza automatici sul deployment multi-layer della piattaforma Moon Cloud, fornendo una prospettiva sulle performance.

Nell'ambito del progetto è stato inoltre redatto un articolo dal titolo "A security benchmark for OpenStack" che, partendo dal benchmark CIS, identifica alcuni controlli di sicurezza specifici per il prodotto in oggetto. Questo è stato sottomesso ed accettato alla conferenza IEEE Cloud 2017 in programma dal 25 al 30 Giugno ad Honolulu (Hawaii, USA).

Il lavoro di tesi può essere riassunto come segue:

- *Analisi di FedRAMP*, individuazione dei punti chiave del programma e studio di metodologie a supporto delle attività e degli attori coinvolti nel processo di autorizzazione.
- *Design e implementazione di driver* per la valutazione automatica e continua dei controlli di sicurezza. Al fine di garantire la copertura delle specifiche del framework, sono stati utilizzati due diversi approcci per l'esecuzione dei controlli di sicurezza:
  - *Driver per i controlli automatici*, la cui esecuzione avviene in modo autonomo, per l'*assessment* delle proprietà non-funzionali effettivamente implementate nei sistemi informatici
  - *Driver per i controlli ad interazione umana*, effettuati tramite la somministrazione di questionari ad utenti, per l'analisi dei processi di business.
- *Valutazione* dell'implementazione della sicurezza della piattaforma Moon Cloud, mediante i controlli sviluppati; valutazione dei costi e dell'effort di deployment dei controlli.

Il progetto di tesi si presta a numerosi sviluppi futuri, che possono riguardare sia il perfezionamento dei driver Moon Cloud realizzati, sia la integrazione degli stessi con documenti relativi ad altri standard di settore (PCI-DSS, HIPAA, ISO27000).