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

Negli ultimi anni, l'adozione del paradigma cloud ha permesso alle organizzazioni di usufruire di vantaggi prestazionali ed economici nell'erogazione dei servizi IT, grazie sia alle caratteristiche di scalabilità ed elasticità proprie dello stesso, 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 quelle realtà in procinto di effettuare migrazioni parziali o totali delle loro infrastrutture tradizionali *on premises*. La centralizzazione degli aspetti di sicurezza nelle mani di un *cloud service provider* rappresenta infatti uno dei limiti maggiori dell'approccio, e richiede un rapporto di fiducia reciproca tra il fornitore del servizio e il cliente. Questo rapporto di fiducia, attualmente basato sulla reputazione del provider, rappresenta la base per minimizzare il rischio e limitare il perimetro di attacco, e per stabilire le responsabilità di ogni entità coinvolta nella gestione degli incidenti.

Questo lavoro di tesi si pone all'interno della filiera di ricerca sulla *security assurance*. La security assurance mira ad incrementare il livello di attendibilità di un sistema verificandone i comportamenti attesi in caso di fallimento o attacchi. Una delle tecniche che possono essere utilizzate consiste nella produzione di evidenze fidate e replicabili, basate su attività di testing e monitoraggio.

In particolare, il lavoro di tesi ha come obiettivo la verifica continua e automatica della compliance allo standard FedRAMP. FedRAMP è il programma governativo americano per la valutazione del rischio e l'autorizzazione all'utilizzo di servizi cloud nelle agenzie federali, che è stato adottato in diversi domini ad alta criticità come ad esempio Amazon AWS e US DoD.

Questa tesi si è concentrata da un lato sull'analisi e sullo studio dello standard FedRAMP allo scopo di identificare i controlli di sicurezza (descritti nel documento NIST SP 800-53) di interesse per una valutazione di compliance; dall'altro nell'implementazione dei controlli di sicurezza identificati e nella loro integrazione all'interno di 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 fornire un'ambiente per la valutazione di compliance continua e automatica allo standard FedRAMP e assumere un ruolo di supporto per tutti gli attori coinvolti nel processo di autorizzazione, in particolare i fornitori di servizi che vogliano attestarne la *readiness*.

Nell'ambito della tesi 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 online di questionari, per l'analisi dei processi di business.
- *Integrazione dei controlli di sicurezza automatici* all'interno della piattaforma multi-layer Moon Cloud.

- *Validazione* della soluzione proposta e dei corrispondenti controlli di sicurezza nell'ambito della verifica della compliance della piattaforma Moon Cloud allo standard FedRAMP. La fase di validazione ha anche considerato i costi e l'effort di deployment dei controlli di sicurezza.

Questa tesi si presta a numerosi sviluppi futuri, che possono riguardare sia il perfezionamento dei driver Moon Cloud realizzati, sia l'integrazione degli stessi per la valutazione di compluance ad altri standard di settore come ad esempio PCI-DSS, HIPAA e ISO27000. Inoltre, la tecnica presentata può essere utilizzata e adattata a contesti alternativi alla valutazione di compliance, come ad esempio la valutazione del grado di accettabilità delle politiche di sicurezza applicate all'interno di un sistema oppure la valutazione del grado di consapevolezza degli utenti sulle best-practices di sicurezza informatica.