Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico (matricola 886667)

/02/2020

RELATORE
Prof. Valerio Bellandi

CORRELATORE
Prof. Claudio A. Ardagna

Il Cloud Computing solleva diverse problematiche legate alla mancanza di fiducia e trasparenza visto che i clienti necessitano di avere delle garanzie sui servizi Cloud ai quali si affidano; spesso i fornitori di questi servizi non fornisco ai clienti le specifiche riguardanti le misure di sicurezza messe in atto.
Per rendere il Cloud fidato e trasparente, per questo sono state introdotte tecniche di *Security Assurance*, delle garanzie che permettono di ottenere la fiducia necessaria nelle infrastrutture e/o nelle applicazioni di dimostrare il rispetto di certe proprietà di sicurezza; grazie alla raccolta e allo studio di evidence è possibile che venga accertata la validità e l'efficienza delle proprietà di sicurezza messe in atto.
Moon Cloud è un framework di *Security Assurance* il quale garantisce che un sistema ICT soddisfi certi requisiti prestabiliti da appropriate politiche e procedure precedentemente definite. Una *Security Compliance Evaluation* è un processo di verifica a cui un target è sottoposto e il cui risultato deve soddisfare i requisiti richiesti da standard e politiche. Per Evaluation si intende quel processo di verifica di uniformità di un certo target o asset, fornito dall'utente, a una o più politiche attraverso una serie di Controlli che a seconda delle caratteristiche e proprietà del target, può avere successo o meno. In altre parole, si può dire che un Evaluation è costituita da uno o più Controlli.
I sistemi di raccomandazione (*Recommendation System*) sono nati con lo scopo d'identificare quegli oggetti (detti generalmente *item*) all'interno di un vasto mondo d'informazioni che possono essere di nostro interesse.
Per poter rendere ancora più intuitivo e semplice da utilizzare un sistema di questa importanza, si è pensato d'introdurre un sistema che possa raccomandare agli utenti, in base agli asset che vogliono proteggere e monitorare, una serie di Evaluation o politiche da applicare in quei casi; questo permette anche a utenti meno esperti di poter configurare in modo rapido ed efficiente meccanismi di protezione da minacce.
Inizialmente lo sviluppo di questa soluzione ha affrontato una fase di studio del funzionamento della piattaforma Moon Cloud, in particolare vennero raccolte le Evaluation e i Controlli implementati; si analizzarono i diversi approcci per la creazione di tassonomie all'interno di un database relazionale unitamente a come costruire un sistema di raccomandazione. Vennero approfonditi diversi approcci, come ad esempio i *Content-based filter* e i *Collaborative filter*, utilizzati per filtrare i dati e determinare gli *item* più adatti ad essere raccomandati all'utente. Successivamente si è passati a integrare quanto fatto con la piattaforma già esistente. Per integrare questi due sistemi vennero predisposti dei servizi di API REST che permettessero a Moon Cloud di effettuare delle richieste al sistema di raccomandazione e di ricevere come risposta una lista di Evaluation da

proporre all'utente. Inoltre per fare in modo che il database utilizzato dalla piattaforma stessa e quello creato in questa soluzione avvessero dati consistenti vennero predisposte ulteriori API REST.
In conclusione, la soluzione sviluppata offre delle raccomandazioni di tipo basico, tuttavia è in grado di supportare gli utenti nell'utilizzo del framework Moon Cloud.