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 ha portato un rivoluzionario paradigma nella creazione di un nuovo business, virtuale e accessibile, in qualunque momento e luogo; esso sfrutta le tecnologie messe a disposizione dai sistemi ICT come le operazioni di virtualized computing, internet e distributed computing, provvedendo un sistema integrato molto potente. Si può definire il Cloud Computing come l'abilità di accedere a risorse (come database o applicazioni) in poco tempo e in tutto il mondo attraverso una rete.
Gli immensi benefici del Cloud in termini di flessibilità, consumo delle risorse e gestione semplificata, lo rendono la prima scelta per utenti e industrie per il deploy dei loro sistemi IT. Tuttavia il Cloud Computing solleva diverse problematiche legate alla mancanza di fiducia e trasparenza dove 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, e che operino normalmente anche se subiscono attacchi; 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 e tanto maggiore è il grado di conoscenza dell'individuo e tanto più vengono ritenuti affidabili.
Per poter rendere ancora più intuitivo e semplice da utilizzare un sistema di questa importanza come Moon Cloud, Il quale è costantemente a contatto con dati sensibili di utenti, si è pensato d'introdurre un sistema che possa raccomandare agli utenti, in base agli asset che vogliono proteggere e monitorare, una serie di Evalua-

tion 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. Un sistema di raccomandazione permette di selezionare all'interno di un ampio catalogo, un numero limitato di prodotti personalizzati sulla base delle preferenze dell'utente attivo. La ricerca in questo ambito si è sempre concentrata sulla qualità delle raccomandazioni di questi sistemi, tralasciando un aspetto fondamentale: la fiducia che un utente deve avere verso questi ultimi. E ciò è ottenibile se si è il più possibile trasparenti nei processi che portano alla nascita dei suggerimenti, partendo da questo si può ottenere l'ambita fiducia da parte degli utenti.