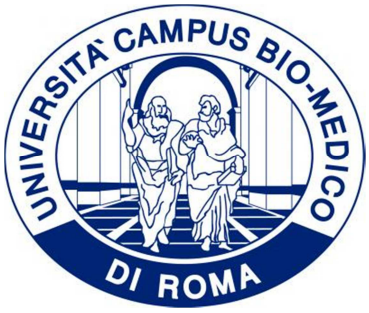

Master Universitario di II livello in
Homeland Security
Sistemi, metodi e strumenti per la security e il crisis management

VI edizione, a. a. 2013/2014

Gestione delle identità e degli accessi in ambiente Cloud Computing: modelli architetturali e conformità ai principali standard di sicurezza dell'informazione

Tutor: Prof. Roberto Setola

Candidato: Antonio Iossa

Abstract

Studi recenti hanno confermato che il Cloud Computing, oltre ad essersi ampiamente dimostrato all'altezza delle promesse più concrete in termini di riduzione del time-to-market e dei costi di manutenzione hardware e software, sta superando ogni previsione e diventerà il futuro modello di IT.

Tuttavia, uno dei maggiori motivi ostativi nell'adozione del Cloud Computing è rappresentato dalla sicurezza delle informazioni: con tale modello di elaborazione i dati e le applicazioni in possesso di un'organizzazione non vengono memorizzati all'interno dei confini fisici dell'organizzazione. Tale delocalizzazione dei dati assume particolare rilievo relativamente ai dati personali, sensibili e/o giudiziari caratteristici delle identità degli utenti che interagiscono con l'organizzazione.

In modelli di elaborazione tradizionali, soventemente vengono adottati ormai maturi sistemi di gestione delle identità e degli accessi (Identity and Access Management – IAM) che consentono una efficace ed integrata gestione delle identità e degli accessi, assicurando al contempo il soddisfacimento dei requisiti normativi applicabili e la conformità ai principali standard internazionali sulla sicurezza dell'informazione.

Un'organizzazione che ha adottato un sistema IAM tradizionale ed è pienamente conforme ai vincoli normativi applicabili e, al contempo, soddisfa i requisiti imposti dagli standard internazionali, quali problematiche si troverà ad affrontare volendo adottare un sistema IAM su piattaforma Cloud? Può l'organizzazione essere certa che, apportando le opportune modifiche, potrà continuare ad essere conforme a standard e normative applicabili?

In questo Project Work si cercherà di rispondere a tali quesiti. Per far ciò, si analizzeranno innanzitutto diversi modelli architetturali di Identity and Access Management che possono essere adottati in ambiente Cloud, evidenziandone le differenze ed individuandone i rischi caratteristici.

In seguito, si esamineranno i cambiamenti ed i rischi incombenti sui processi di Identity and Access Management nel passaggio dal modello di elaborazione tradizionale al modello di elaborazione Cloud.

Infine, allo scopo di valutare la capacità per l'organizzazione di essere conforme allo standard ISO/IEC27001:2013 in caso di adozione di un determinato modello IAM

su piattaforma Cloud, si provvederà a realizzare un'analisi volta a misurare la fattibilità del soddisfacimento dei requisiti imposti da predetto standard, per ognuno dei modelli architetturali considerati. L'analisi evidenzierà come le architetture IAM Cloud considerate consentano di coprire in maniera diversa le c.d. aree di controllo dello standard ISO/IEC27001:2013, e consentirà quindi di indirizzare l'organizzazione verso un determinato modello architetturale di IAM su piattaforma Cloud in funzione delle esigenze dell'organizzazione stessa.