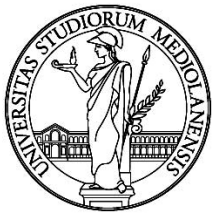


UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea Magistrale in Sicurezza Informatica

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

RELATORE

Prof. Claudio Agostino Ardagna

CORRELATORE

Dott. Marco Anisetti

SECONDO CORRELATORE

Prof. Ernesto Damiani

TESI DI LAUREA DI

Patrizio Tufarolo

Matr. 875041

Anno Accademico 2016/2017

Ai miei genitori e a mio fratello

Ringraziamenti

Ringrazio tutti coloro che mi sono stati vicini in questi cinque anni, credendo in me, supportandomi e spronandomi a fare sempre di meglio.

Ringrazio tutti i membri del SESAR Lab, che mi hanno dato la possibilità di apportare un contributo alle attività di ricerca, in particolar modo relative ai progetti CUMULUS e Moon Cloud. Ringrazio in particolare **Filippo Gaudenzi**, supervisore delle mie attività nel suddetto laboratorio con cui ho maturato un rapporto di amicizia e collaborazione.

Un ulteriore ringraziamento va alla prof. Sara Foresti, che ha accettato l'impegno di essere controrelatore di questo lavoro di tesi.

Patrizio Tufarolo

Indice

Elenco delle figure

Elenco delle tabelle

Introduzione

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 *on premises* tradizionali.

La centralizzazione degli aspetti di sicurezza nelle mani di un *cloud service provider* rappresenta infatti uno dei maggiori limiti 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, 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 il Dipartimento della Difesa americano.

Ci si è concentrati quindi da un lato sull'analisi e sullo studio dello standard FedRAMP, allo scopo di identificare i controlli di sicurezza di interesse per una valutazione di compliance (descritti nel documento NIST SP 800-53); 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 sotto-

messo 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 tenuto in considerazione i costi prestazionali dei controlli di sicurezza.

L'organizzazione dei capitoli è la seguente:

- **Capitolo 1 - Security assurance: lo stato dell'arte e la sfida** Nel primo capitolo sono analizzate le problematiche di sicurezza nella migrazione di infrastrutture tradizionali verso la *cloud* illustrando le soluzioni proposte dalla letteratura. Tra queste, vengono approfondite le tecnche di *assurance* mediante certificazione e controllo della *compliance* tramite la raccolta di evidenze.
- **Capitolo 2 - Moon Cloud, un framework per il monitoraggio e la security assurance** Nel secondo capitolo viene illustrato Moon Cloud, una soluzione software prodotta dal laboratorio SESAR dell'Università degli Studi di Milano, avente come obiettivo la security assurance.
- **Capitolo 3 - FedRAMP - Federal Risk and Authorization Management Program** Nel terzo capitolo viene analizzato FedRAMP, analizzando i punti chiave del programma, i ruoli e le responsabilità degli attori coinvolti, e identificando i possibili approcci per implementarne i controlli di sicurezza all'interno di Moon Cloud, al fine di fornire uno strumento a supporto delle attività di ciascun attore.
- **Capitolo 4 - Implementazione dei controlli di sicurezza FedRAMP in Moon Cloud** Nel quarto capitolo viene proposto un approccio ibrido orchestrato

tramite l'integrazione di attività di *security assessment* automatiche e ad interazione umana (per i controlli di sicurezza di carattere proceduale e l'analisi dei processi di business) e ne viene illustrata una possibile implementazione. Nel primo caso, viene presentato il framework OpenSCAP, un ecosistema realizzato da Red Hat per le attività di auditing, e ne viene proposta un'integrazione con Moon Cloud. Nel secondo caso, viene presentato un driver Moon Cloud ad interazione umana, che invia questionari personalizzabili tramite template agli utenti interessati, richiedendone la compilazione e creando un report in PDF.

- **Capitolo 5 - Validazione del framework** Nel quinto capitolo viene effettuata la validazione del lavoro svolto, in particolar modo per l'approccio automatico. Il driver OpenSCAP viene eseguito sul deployment in produzione dello stesso Moon Cloud, per effettuarne l'analisi della sicurezza. Come illustrato nel capitolo 2, Moon Cloud è organizzato in microservizi gestiti tramite *container*. In particolare, il deployment è effettuato su una IaaS OpenStack e una PaaS Docker: viene perciò analizzata l'infrastruttura OpenStack sottostante, mediante OpenSCAP e controlli di sicurezza specifici mappati sui requisiti FedRAMP; viene quindi eseguito l'*assessment* dei container dei vari componenti di Moon Cloud e dei canali di comunicazione. Infine, viene proposta una valutazione delle performance del lavoro svolto e saranno trattate alcune delle problematiche riscontrate.

- **Capitolo 6 - Conclusione e sviluppi futuri** Nel capitolo finale vengono mostrati alcuni sviluppi futuri del progetto in questione, che spaziano dall'integrazione dei driver sviluppati con altri standard, per arrivare all'utilizzo dell'approccio illustrato in casistiche analoghe al processo di auditing della compliance.

Capitolo 1

Security assurance: lo stato dell'arte e la sfida

1.1 Introduzione

In questo capitolo si approfondirà lo stato dell'arte in materia di **security assurance** e **controllo della compliance**, ovvero la verifica della conformità di un'infrastruttura informatica tradizionale, ibrida o cloud, rispetto a una politica, che può essere sviluppata internamente oppure derivata da un più complesso apparato normativo o da uno standard. In particolare verranno trattate le problematiche di sicurezza introdotte dall'adozione di un approccio *cloud*, all'interno dei processi *IT* di un'organizzazione strutturata sulla base di un'infrastruttura informatica tradizionale.

Spesso si fa coincidere il concetto di *cloud computing* con quello di *outsourcing*, di fatto presupponendo che l'adozione di tecnologie *cloud* corrisponda all'attitudine di concedere a terzi gli oneri di gestione di una parte dell'infrastruttura informatica. La definizione di *cloud computing* a cui si fa riferimento in questo elaborato di tesi è quella del NIST[1] nel documento *SP-800-145*[1] nel quale il cloud è presentato come un insieme di tecnologie aventi come obiettivo l'erogazione di servizi e risorse in modalità *on-demand* da un pool condiviso. La condizione di *outsourcing*, quindi, acquisisce una connotazione non strettamente necessaria all'adozione del servizio *cloud*, con cui tuttavia condivide alcuni vantaggi[2] soprattutto per realtà dove il *core business* non è il settore IT:

1. Contenimento dei costi
2. Velocità nel ciclo di sviluppo
3. Garanzia di prestazioni e di qualità
4. Servizio distribuito geograficamente
5. Contratti di affitto strutturati e dimensionati

[1] National Institute of Standards and Technology, *http://www.nist.org/*

1.2 Sicurezza nel cloud computing

Lo scopo finale dell'utilizzo di tecnologie *cloud* consiste nella possibilità per un'organizzazione di usufruire di un modello scalabile, elastico, standard, misurabile e orchestrabile al fine di poter garantire continuità di servizio e prestazioni elevate, demandando la gestione dei processi sistemistici a piattaforme centralizzate e intelligenti. A tal proposito il NIST[1] identifica tre modelli di servizio:

- **IaaS**, *Infrastructure as-a-Service*, nel quale è l'asset erogato è l'infrastruttura informatica, in termini di potenza di calcolo mediante sistemi di virtualizzazione, risorse di rete e storage. Essendo il modello più di difficile gestione, è spesso amministrato tramite un orchestratore. Esempi di tecnologie open-source in questo settore sono *OpenStack*[2], *oVirt*[3], *Apache CloudStack*

- **PaaS**, *Platform as-a-Service*, tramite il quale si fornisce all'utente la possibilità di eseguire servizi personalizzati offrendo meccanismi di contenimento nell'esecuzione, scalabilità e multi-tenancy. L'utente ha un controllo parziale sull'esecuzione del servizio: solitamente egli può interagire in modo limitato con il kernel. Una delle tecnologie più utilizzate è quella dei *container*, un evoluzione del concetto di *jail* proprio dei sistemi operativi BSD, il cui obiettivo è quello di utilizzare meccanismi di segregazione delle risorse basati sulle funzionalità del kernel. I servizi vengono eseguiti in un ambiente isolato, ed hanno un filesystem e uno stack di rete simulato in software dedicati. Una delle implementazioni più note della tecnologia *container* è *Docker*[4] che, nato inizialmente come evoluzione di LXC, è ora basato su una libreria proprietaria e costituisce la base per molte piattaforme PaaS (es. Kubernetes[5] e OpenShift[6]).

- **SaaS**, *Software-as-a-Service*, che permette all'utente di usufruire delle funzionalità di un singolo applicativo, riducendo al minimo l'effort computazionale sulla macchina dell'utente stesso. Tipicamente in questa categoria ricadono le applicazioni web, alcune applicazioni mobile e alcuni software per PC. Alcuni esempi di *SaaS* noti sono *Office 365 Online*[7] e *Google Docs*[8].

[2]Software open-source per la realizzazione di infrastrutture cloud pubbliche e private, https://www.openstack.org/

[3]Software open-source alla base della piattaforma

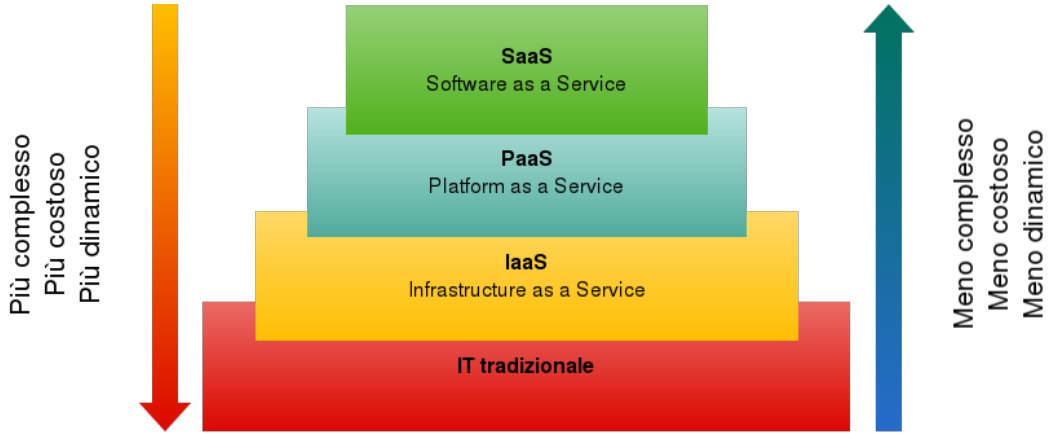
[4]Docker, *https://www.docker.com*

[5]Kubernetes, soluzione *PaaS* progettata da Google *https://kubernetes.io/*

[6]OpenShift, soluzione *PaaS* di Red Hat *https://www.openshift.com/*

[7]Office 365 è la versione cloud-based della nota suite per l'ufficio *Microsoft Office*, *https://www.office365.com*

[8]Google Docs è una suite per l'ufficio sviluppata da Google ed erogata esclusivamente come applicazione web, *https://docs.google.com*



:q!

Figura 1.1: Modelli di servizio

La parola chiave è quindi **"automazione"**. Questa, oltre a garantire una solidità del modello di distribuzione di un servizio grazie a schemi dichiarativi, apporta notevoli vantaggi anche dal punto di vista della sicurezza, facilitando la gestione degli aspetti di confidenzialità, integrità e disponibilità.
Il paradigma *as-a-service* ha infatti consentito la costituzione di una *baseline* robusta garantita dalla centralizzazione delle funzionalità di security le quali, essendo erogate come risorse *cloud*, sono interamente gestite dal *cloud service provider* - pubblico o privato - che può demandarne la gestione parziale all'utente mediante meccanismi di orchestrazione, interfacce grafiche ed API.
Se a primo impatto può apparire come un enorme vantaggio, di fatto ciò introduce un *single point of failure*, determinando livelli di rischio aggiuntivi rispetto alle infrastrutture tradizionali. Si pensi, ad esempio, alle funzionalità di *firewalling* offerte generalmente con la denominazione di *security groups* o *Firewall as-a-Service* (FWaaS): un'implementazione non idonea dal punto di vista funzionale nel substrato infrastrutturale del fornitore di servizi, potrebbe determinare la mancanza di sicurezza per i servizi che ne fanno affidamento. La stessa asserzione è valida per molte altre funzionalità comunemente offerte dal provider: cifratura dei volumi di storage, crittografia e controllo degli accessi nei servizi di block-storage e così via.

Ulteriori riflessioni possono essere fatte anche per quanto riguarda l'aspetto di integrità del dato: se da una parte il cloud service provider implementa già meccanismi di basso livello per la persistenza dello storage, ridondanza, sistemi di backup automatici, dall'altra non si ha la chiara evidenza di come questi aspetti siano effettivamente gestiti e di come la proprietà sia garantita.

Per quanto concerne la proprietà di disponibilità, la dicotomia va ricercata trattando i concetti di disponibilità del dato e disponibilità del servizio separatamente. Il *cloud computing* offre intrinsecamente solidità in quanto basato sui concetti di scalabilità, elasticità e ridondanza. Grazie ai meccanismi di orchestrazione tramite API è infatti possibile configurare le applicazioni per l'*auto-scaling*, al fine di mantenere una qualità adeguata nell'erogazione del servizio al crescere degli utenti. Ciò, dal punto di vista della sicurezza, ha portato a notevoli benefi-

ci per quanto riguarda la mitigazione di attacchi DoS[9], garantendo la continuità di servizio riducendo i costi. Tuttavia esistono dei prerequisiti per garantire la disponibilità: innanzitutto il *cloud service provider* deve assicurare la ridondanza dei dati e della rete, contemplando l'ipotesi di distribuire le risorse su più località geografiche, con l'obiettivo sia di prevenire guasti localizzati che di erogare la risorsa dalla località più vicina rispetto all'utente.

Nel momento in cui funzionalità comunemente demandate ad hardware specifico vengono implementano in software, si determinano sia benefici che svantaggi che devono sia essere contemplati in fase di valutazione del rischio che trattati nei contratti di service level agreement. Una compromissione dell'interfaccia di gestione della piattaforma cloud, sia che si tratti di una dashboard sia che si tratti di un'interfaccia API, può portare a un'interruzione di servizio.

Gli standard di sicurezza classici, così come l'assetto normativo e i contratti di *service level agreement*, necessitano di essere adeguati per supportare l'integrazione di tecnologie cloud all'interno degli stack tradizionali, tenendo conto delle problematiche di *shared responsability* presentate.

Il NIST [1] riconosce quattro diversi modelli di deployment:

- **Public Cloud**: modello in cui le risorse sono fornite per un utilizzo pubblico. È tipicamente erogato in outsourcing tramite la rete internet. L'hardware è in mano a un unico provider che eroga servizi in *outsourcing* e ne dispone le metriche e la tariffazione.

- **Private Cloud**: cloud dedicata a un'azienda o organizzazione, sfruttata per erogare servizi appartenenti al provider. L'hardware è generalmente nel datacenter dell'organizzazione.

- **Hybrid Cloud**: approccio ibrido dato dalla composizione di public cloud e private cloud, o di public cloud e infrastrutture tradizionali. Le infrastrutture coinvolte rimangono distinte e sono legate tra loro da un'unica tecnologia (standard o proprietaria) che facilita la migrazione e la portabilità delle risorse.

- **Community Cloud**: modello che fornisce una cloud per uso esclusivo di una comunità di utenti appartenenti ad organizzazioni con obiettivi funzionali comuni. Può essere di proprietà di una o più organizzazioni della community, o di terze parti.

Per ognuno di questi modelli è possibile esplicitare dei requisiti da soddisfare al fine di colmare il rapporto di sfiducia proprio di questo settore[3].

1.3 Valutazione del rischio: vulnerabilità, minacce e attacchi

In letteratura sono stati proposti molti lavori sulla valutazione del rischio su infrastrutture cloud. Nei paragrafi a seguire verranno discussi alcuni di questi approcci, sulla base della metodologia utilizzata da Ardagna et Al.[3]. Le vulnerabilità

[9] Denial of Service

possono essere categorizzate in tre macro aree, in base alla superficie di attacco considerata:

1. **Livello applicativo**: quando l'attacco è condotto da un qualsiasi attore nei confronti di una piattaforma SaaS
2. **Tenant su tenant**: quando l'attacco è condotto da attori appartenenti a un tenant nei confronti di un altro tenant
3. **Provider su tenant** e **Tenant su provider**: quando l'attacco è condotto dal provider nei confronti di un tenant (tipicamente malevolo) oppure da un tenant nei confronti del provider

1.3.1 Livello applicativo

Si tratta di vulnerabilità tradizionali che da anni tengono sotto scacco il panorama *web services*: si va da attacchi protocollari sulla comunicazione tra servizi fino alla compromissione di applicativi software specifici. Il target dell'attacco sono le piattaforme SaaS, spesso derivate dal porting di un'applicativo tradizionale sul cloud e non nativamente pensate per essere erogate online: per questo motivo sono caratterizzate da una superficie di attacco molto vasta.

Alcuni lavori significativi citati nel survey di rifermento [3] sono:

- **Gruschka and Iacono, 2009**[4], nel quale è stato presentato un *replay attack*, sfruttando una vulnerabilità del meccanismo di verifica della firma digitale sull'interfaccia SOAP di *Amazon EC2*, e sono state eseguiti comandi sulle API con i privilegi di un utente legittimo
- **Bugiel et Al., 2011**[5], che hanno analizzato le minacce sulla confidenzialità e la privacy estraendo con successo informazioni sensibili da immagini di macchine virtuali Amazon

1.3.2 Tenant su tenant

Le vulnerabilità *tenant su tenant* sono tipiche dei sistemi virtualizzati, quando tenant differenti condividono la stessa infrastruttura e, più specificatamente, lo stesso hardware fisico: gli attacchi possono avvenire per configurazioni erronee o vulnerabilità sull'infrastruttura di virtualizzazione. Si tratta quindi di attacchi che avvengono al livello più basso dello stack cloud[3].

Alcuni contributi interessanti per questa categoria di attacchi e vulnerabilità sono quelli di:

- **Ristenpart et al**, 2009[6], in cui è discusso un attacco alla confidenzialità delle informazioni relative a istanze di servizi in esecuzione. L'attacco dimostrato è basato sul fatto che i servizi sono ospitati sullo stesso hardware, per cui per un servizio è possibile generare traffico e monitorare le proprie performance per fare inferenza su quelle di un altro servizio.
- **Green**[7], che propone un ulteriore attacco di tipo *side-channel* che coinvolge, questa volta, due virtual machine ospitate sullo stesso hardware.

1.3.3 Provider su tenant, tenant su provider

Le vulnerabilità di questo tipo si verificano ogni qual volta un utente o un'organizzazione sposta le proprie risorse su un'infrastruttura cloud non fidata - nella quale il provider è malevolo oppure semplicemente curioso - oppure nel caso in cui l'utente inizia ad usare un servizio cloud con l'obiettivo di attaccare il provider (ad esempio creando botnet per lanciare attacchi denial of service, attaccando le API di orchestrazione e così via) [3].

Le tipologie di attacchi che sfruttano queste vulnerabilità, sono generalmente rivolte al livello IaaS[3], ma non è esclusa la possibilità di attacchi a livello PaaS e SaaS.

Il survey si sofferma sul lavoro Huan Liu[8], il quale illustra una attacco DDoS basato sulla saturazione della banda della rete virtuale: la virtualizzazione dello stack di rete a livello software (*software-defined network*) richiede, oltre a risorse di rete, anche un'elevata capacità di calcolo.

Le vulnerabilità provider su tenant sono invece trattate da Rocha e Correira[9] che propongono una panoramica dei possibili attacchi alla confidenzialità - che possono essere condotti anche dal fornitore di servizi - discutendone le contromisure, e da Bleikertz et al. [10] che si concentrano sulla problematica di proteggere i clienti da attacchi condotti da provider esterni, fornendo un'architettura *Cryptography as-a-Service client-driven*.

La problematica di confidenzialità nella casistica *provider-on-tenant* è anche l'oggetto di De Capitani di Vimercati et. al[11] in cui è descritta una tecnica per preservare la confidenzialità del dato riallocandolo in modo dinamico ad ogni accesso su tre nodi, risolvendo così anche i problemi di collusione tra i service provider coinvolti. Un ulteriore articolo di De Capitani di Vimercati et al[12]. affronta la problematica del provider *onesto ma curioso* con una soluzione per l'integrità dei risultati delle query di join, che discute la casistica di un server di storage di terze parti e di fornitori di potenza di calcolo esterni e malevoli i quali producono i risultati del join per basi di dati ospitate esternamente.

1.4 Tecniche di sicurezza per la cloud

Data l'etereogeneità delle problematiche e degli approcci adottati negli articoli citati, è possibile affermare che garantire proprietà di sicurezza in ambienti cloud è molto impegnativo: questi lavori presentano solamente soluzioni parziali al problema, affrontando di volta in volta problemi specifici e presentando tecniche sviluppate *ad-hoc*[3]. Saranno di seguito presentati alcuni approcci e tecniche per garantire la sicurezza su sistemi cloud.

1.4.1 Autenticazione e controllo degli accessi

I sistemi tradizionali per l'autenticazione e il controllo degli accessi si sono verificati inefficienti per la cloud, pertanto è stato necessario definire nuovi approcci. L'adozione di nuovi *pattern* di sviluppo orientati alla scalabilità - come ad esempio il pattern *micro-services*, naturale evoluzione delle architetture SOA - ha reso necessario sviluppare meccanismi di autenticazione decentralizzati e federati.

Almulia and Yeun [2010] offrono una panoramica sui protocolli di autenticazione e *identity management*, analizzandone la sicurezza, l'effort implementativo e i costi[13].

Costituendo parte critica per la maggior parte dei sistemi, i servizi di autenticazione, gestione dell'identità e gestione delle policy di accesso sono erogati *as-a-service*.

Takabi e Joshi hanno descritto un sistema di gestione delle policy *as-a-service* (PMaaS, *Policy Management as-a-service*) che fornisce un punto di controllo centralizzato indipendente dalla locazione della risorsa[14]. Prima di accedere a una risorsa è necessario contattare il server di autenticazione e autorizzazione centralizzato che rilascerà il *grant* dopo opportuna verifica. *Azure Active Directory*, il porting *SaaS* di *Microsoft Active Directory*, provvede sia a funzionalità di autenticazione che di policy management e fornisce alcuni driver di integrazione per la maggior parte dei protocolli noti.

Tuttavia, poiché molte realtà complesse dispongono già di meccanismi di autenticazione mediante *ticket granting* isolate dalla rete Internet, sono stati ideati anche modalità di autenticazione e controllo degli accessi completamente *stateless* (ad esempio OAuth). È il caso dei *JSON Web Token*, formalizzati nella RFC 7519: l'*authentication server*, dopo aver validato la richiesta di autenticazione, restituisce un token *JSON* firmato che contiene l'identità dell'utente e tutti i *grant* per le autorizzazioni ad esso relative. Non esiste il concetto di sessione, la validità del token è data esclusivamente da una marca temporale e da una durata. Il token può essere utilizzato quindi per autenticare le richieste verso i vari servizi, cui spetta l'onere di verificarne la validità del contenuto e della firma, decifrabile tramite segreto condiviso con il server di autenticazione che lo ha emesso. I vantaggi di un approccio simile sono molteplici, tuttavia è impossibile revocare il token una volta emesso. Eventuali blocchi sono effettuabili tramite sistemi di *blacklisting* che riporterebbero in auge la problematica della decentralizzazione che si voleva risolvere. La prassi è quindi quella di emettere token *one-time* o con durata breve, al fine di minimizzare la durata di una possibile finestra temporale di attacco.

1.4.2 Crittografia, firma digitale e trusted computing

La crittografia è essenzialmente utilizzata per proteggere la confidenzialità dei dati, delle comunicazioni e le attività sensibili da tutti quegli avversari che mirano a disturbare l'operatività della cloud. La maggior parte della letteratura utilizza tecniche di crittografia per preservare la confidenzialità: l'obiettivo di queste metodologie è di facilitare la migrazione dei dati gestiti da sistemi tradizionali verso la cloud. Tuttavia non sono assenti tecniche focalizzate su altre proprietà di sicurezza, come l'utilizzo della firma digitale per curare gli aspetti di integrità e privacy.

Trusted Computing

Il *trusting computing* è una tecnica utilizzata per effettuare computazioni sicure, basata sull'utilizzo della crittografia asimmetrica e di un dispositivo hardware

dedicato (TPM, Trusted Platform Module) tramite il quale è possibile *i)* identificare univocamente i dispositivi con un numero di serie e una chiave di cifratura implementata in hardware *ii)* cifrare informazioni con la chiave di cifratura *iii)* firmare informazioni con la chiave di cifratura. Queste funzionalità pongono le basi per una serie di utilizzi avanzati volti a preservare l'integrità e la confidenzialità di dati - sia in transito su una rete, che memorizzati su disco o sui firmware del dispositivo - codice e hardware, riducendo o annichilendo gli effetti di eventuali attacchi.

Boampong e Wahsheh nel 2012 hanno proposto un modello per utilizzare il TPM al fine di garantire la correttezza dei processi di autenticazione, l'integrità e la confidenzialità sulla cloud[15]. Portare il TPM sul cloud significa realizzarne una versione virtuale, così come illustrato da Krautheim[16] nel 2009, basandosi sul concetto di virtual-TPM (vTPM) già descritto da Berger et al. nel 2006[17]. Il vTPM è un componente software che implementa le stesse funzionalità del TPM hardware, garantendo la multi-tenancy mediante istanze multiple e multiplexing. I vantaggi dell'utilizzo di una tecnologia di *trusted computing* nel contesto cloud sono molteplici, come la possibilità per l'utente di fare enforcement di politiche di privacy togliendo la possibilità al cloud service provider di modificarle, fornendo una soluzione parziale problematiche di *shared responsability* discusse. Come illustrato da Velten and Stumpf[18] e più recentemente da Szefer e Lee[19] il TPM può essere utilizzato per garantire confidenzialità e integrità a tutti i livelli dello stack, prevenendo tampering da parte del fornitore di servizi e attacchi da parte di altri tenant o da malware.

1.5 Approcci per assurance, testing, monitoraggio e compliance

I progressi nella ricerca sulla sicurezza della cloud hanno portato la necessità di avere tecniche di *security assurance* per aumentare la confidenza degli utenti nei confronti del provider[20]. Per *assurance* si intende la modalità per ottenere, con un certo livello di precisione, la consapevolezza che l'infrastruttura e/o le applicazioni manterranno nel tempo una o più proprietà di sicurezza, e la loro operatività non sarà compromessa indipendentemente da malfunzionamenti o attacchi[21]. In accordo con Ardagna et Al.[3], è possibile affermare che quello di *assurance* è un concetto più esteso della mera nozione di *sicurezza informatica*, comunemente definita come *la protezione delle informazioni e dei sistemi informativi da accessi, utilizzi disclosure, interruzioni del funzionamento, modifiche e distruzioni non autorizzate*. Nella cloud è molto facile avere livelli di sicurezza elevati con livelli di assurance scarsi poiché le funzionalità di sicurezza realmente implementate sono difficilmente percepite.

Per la messa sicurezza delle realtà che decidono di trasferire degli *asset* sulla cloud è necessario considerare tre aspetti fondamentali:

- Necessità di una soluzione di analisi e gestione del rischio, in grado di valutare l'impatto dell'adozione di servizi cloud sul business

- Esigenze di *transparency*, ovvero la possibilità per l'utente di essere consapevole del modello di business del fornitore di servizi
- Soluzione di assessment, verifica delle policy e della compliance, che permetta sia di verificare lo stato istantaneo del livello di conformità, che di spiegare all'utente le metodologie attuate per mantenere livelli di compliance adeguati, secondo il principio "comply-or-exmplain" di MacNeil and Li[22]

L'obiettivo di questo lavoro di tesi è quello di fornire un framework per la security assurance i) insistendo sulla valutazione continuativa dello stato di sicurezza sulla cloud ii) offrendo un framework cloud-based per la security assurance insistendo su

- testing di proprietà non funzionali
- monitoraggio continuativo della sicurezza del sistema
- conformità del sistema a politiche di sicurezza, siano esse definite internamente ad un'organizzazione, siano esse provenienti da uno standard di settore
- ottemperare alle esigenze di transparency degli utenti della cloud, offrendo una dashboard panoramica sullo stato della cloud del provider

1.5.1 Testing di proprietà non funzionali

Il *testing* è definito come la fase del ciclo di vita del software composta da tutte le attività, statiche o dinamiche, atte a determinare che questo soddisfi i requisiti specificati e che sia conforme all'obiettivo proposto, nonché per rilevare eventuali difetti.

Nel contesto *cloud* possiamo riconoscere due tipologie di soluzioni di testing: quelle specifiche per il collaudo di infrastrutture cloud e quelle generiche per il testing del software, applicabili anche a servizi cloud.

Il lavoro di tesi si focalizzerà maggiormente sulla prima categoria insistendo sulla validazione delle proprietà a tutti i livelli dello stack (in accordo con Riungu et. Al[23]); nonostante ciò il framework proposto può essere adattato ad entrambe le tipologie.

1.5.2 Monitoraggio continuativo della sicurezza del sistema

La natura stessa dei sistemi cloud complica notevolmente l'analisi delle informazioni relative allo stato dei servizi: a causa dell'elevata complessità dei software impiegati nell'orchestrazione e nell'erogazione delle risorse è spesso difficile rilevare cambiamenti nello stato del sistema, il cui back-end è continuamente tempestato di eventi. È quindi necessario introdurre una componente di monitoraggio, collezionamento e correlazione di eventi.

Per valutare aspetti non funzionali come la sicurezza, è poi necessario che questi eventi vengano contestualizzati: possono essere necessarie pertanto analitiche *stateful*, effettuabili anche tramite strumenti più complessi o provenienti dal mondo *big-data*.

Proprio per facilitare scenari di *software integration* il framework proposto nei prossimi capitoli è stato strutturato esasperando la modularità, ed è stato basato principalmente su tecnologie *open-source*.

Come per il testing, anche per il monitoraggio è possibile individuare sia soluzioni generiche sia soluzioni specifiche per il mondo *cloud*. Software come *Nagios*[10] e *Ganglia*[11] rientrano nella prima categoria, ma vantano livelli di espandibilità tali da poter essere adeguati ai sistemi di collezionamento delle metriche dei maggiori software cloud. Ulteriori soluzioni come *Sensu*[12], *Sysdig*[13], *Weave*[14] contengono strumenti specifici per la cloud.

Per quanto riguarda gli aspetti di sicurezza, la disponibilità di potenza computazionale on-demand, ha garantito la possibilità di effettuare il deploy scalabile di sistemi IDS[15] e IPS[16]. L'utilizzo di questa tipologia di software è stato approfondito da Modi et al. [24], i quali hanno illustrato come utilizzarli sulla *cloud* al fine di mitigare le diverse tipologie di attacchi al paradigma CIA (attacchi provenienti dall'interno, dall'esterno, attacchi di flooding, *privilege escalation*, *port scanning*, attacchi agli *hypervisor* di virtualizzazione e attacchi tramite *backdoor*). Un lavoro di Ficco et Al. del 2013[25] ha presentato un'architettura multi-layer per il rilevamento delle intrusioni, che supporta l'aggregazione di eventi complessi.

Lavori successivi hanno successivamente presentato approcci più specifici e focalizzati su problemi singoli, come Ardagna et Al. 2014[20] che tramite un approccio introspettivo sulle virtual-machine ha prodotto un meccanismo di rilevazione dei *rootkit*.

1.5.3 Conformità del sistema a politiche di sicurezza e cloud transparency

Il presente lavoro di tesi trova le sue origini nel progetto europeo FP7 CUMULUS[26] (Certification infrastrUcture for MUlti-layer cloUd Services), nel quale sono stati proposti modelli, processi e strumenti a supporto di un processo di certificazione per proprietà di sicurezza e non-funzionali in ambito di cloud computing. L'obiettivo del processo di certificazione è quello di fornire quante più evidenze possibili per attestare che un sistema software garantisca determinate proprietà non funzionali e si comporti in modo corretto[3]; si tratta di un approccio alla sicurezza già sperimentato in altri ambiti che tuttavia rimane di difficile applicazione nel contesto dei *web-services*, in particolare nella cloud[27]. Infatti, le tecniche di certificazione usuali che considerano il software come blocco monolitico, vanno a scontrarsi con una struttura complessa e *multi-tier*[27] e necessitano

[10]Nagios, piattaforma di monitoraggio distribuita general purpose, *http://www.nagios.org/*

[11]Ganglia, soluzione per il monitoraggio delle performance dei cluster in ambito grid computing, *http://ganglia.sourceforge.net*

[12]Sensu, *https://www.sensuapp.org/*

[13]Sysdig, sistema per l'identificazione dei problemi nei sistemi basati su container*http://www.sysdig.org*

[14]Weave, piattaforma SaaS per il monitoraggio di architetture a micro-servizi *https://www.weave.works/*

[15]*Intrusion Detection System*, software per il rilevamento delle intrusioni

[16]*Intrusion Prevention System*, sistemi preventivi per la rilevazione di attività anomale usati per prevenire incidenti informatici

di essere integrate con i processi e caratteristiche tipiche del mondo cloud, come il deployment, la discovery degli asset, l'elasticità e il paradgima on-demand. Il problema è stato dapprima affrontato in Damiani et al. [2009b] [28], in cui è definita una soluzione di certificazione per i servizi basata su certificati di sicurezza basati su test-case firmati. Più recentemente Anisetti et. al [29][30][31] hanno proposto uno schema di certificazione sulla base di un processo di testing basato su un modello, esteso poi con un processo di certificazione incrementale al fine di coprire le esigenze evolutive del paradigma dei servizi.

L'obiettivo di questa tesi, tuttavia, non è quello di fornire un meccanismo di certificazione, bensì quello di offrire un framework per il controllo della conformità di un sistema rispetto alle proprietà non funzionali attese. La metodologia utilizzata è basata sul concetto di *auditing*, ovvero la possibilità di verificare il comportamento di un sistema per valutarne l'adeguatezza rispetto alle policy dell'utente piuttosto che ai regolamenti o alle legi vigenti.[3] Si vuole quindi rendere la cloud *auditable* - al fine di ottemperare alle esigenze di transparency dell'utente, incrementando così il livello di fiducia dell'utente nei confronti del provider e permettendo allo stesso di essere in grado di effettuare scelte ponderate delle varie soluzioni rispetto ai propri requisiti, funzionali e non.

La *transparency* consiste, per l'appunto, nel concedere all'utente una visione di alto livello a dati aggregati ed evidenze collezionati dal provider stesso a basso livello, ed è considerato alla base di ogni approccio efficace per la cloud assurance[20][32].

L'assenza di *transparency* infatti rende i problemi di sicurezza difficilmente percettibili per l'utente[3], in quanto i contratti di *service level agreement* non forniscono parametri tecnici per misurare il livello di sicurezza delle applicazioni e dei dati ospitati sulla cloud[33].

Essa, inoltre, è fondamentale per supportare sia una visione dei processi interni da parte del provider che una visione dei processi esterni per il cliente per fini di sicurezza, così da bilanciare entrambe le esigenze[3].

1.6 Conclusioni

Finora la *security assurance* è effettuata mediante tecniche perlopiù manuali e dall'effort elevato, con cadenze trimestrali o semestrali: il processo di verifica non è effettuato con continuità.

Nel prossimo capitolo verrà presentato Moon Cloud, un framework automatico e programmabile per documentare, valutare, osservare dei controlli tecnici (auditing su controllo degli accessi, configurazione del sistema, crittografia ecc.), controlli di processo (analisi delle vulnerabilità, analisi del rischio, acquisizione di evidenze sul funzionamento di sistemi e servizi) e controlli di sistema (gestione delle configurazioni, consapevolezza e training, gestione delle modifiche e dei cambiamenti)

Successivamente verrà illustrato ed analizzato FedRAMP, il programma governativo americano che fornisce un approccio standard per effettuare il *security assessment* e automatizzare il monitoraggio continuativo dei servizi cloud; verrà mostrata l'integrazione dello stesso nella soluzione Moon Cloud, illustrando gli

approcci per l'inclusione dei controlli di sicurezza di FedRAMP, per concludere con la valutazione e la validazione del lavoro mediante l'assessment del deployment di un'architettura software a microservizi (Moon Cloud stesso) in modalità multi-layer.

Capitolo 2

Moon Cloud: un framework per il monitoraggio e la security assurance

2.1 Introduzione

In questo capitolo verrà approfondito Moon Cloud[1], un framework per il monitoraggio e l'assurance di sistemi tradizionali, cloud e Internet of Things, sviluppato dai ricercatori del laboratorio SESAR Lab[2] dell'Università degli Studi di Milano.

L'obiettivo del progetto Moon Cloud è quello di implementare una metodologia automatica per la valutazione della sicurezza, delle performance e di altre proprietà non funzionali, offrendo un processo di assurance basato su attività di auditing e raccolta di evidenze.

Le caratteristiche di Moon Cloud sono le seguenti[34]:

- **Framework automatico e personalizzabile orientato a microservizi** basato su modelli per la raccolta di evidenze
- **Copertura di tutto lo stack cloud**, ai livelli *IaaS*, *PaaS*, *SaaS*
- **Possibilità di integrazione con tecnologie pre-esistenti e di terze parti**

L'orchestrazione avviene tramite una *dashboard* grafica erogata in modalità *Software as-a-Service*, la quale si interfaccia con diversi componenti che ne implementano la logica di funzionamento, l'esecuzione dei test, il collezionamento dei risultati e il reporting dello stato di compliance del sistema analizzato.

L'obiettivo di questo capitolo è quello di dare al lettore il *know-how* necessario a comprendere le motivazioni di alcune decisioni prese nella realizzazione della tesi ed alcune limitazioni del framework Moon Cloud. Di seguito sarà proposta una breve panoramica sulla terminologia utilizzata, sulle componenti principali, e sui principi di funzionamento dei processi di *assessment* e *compliance* all'interno della piattaforma.

[1] MOnitoring and assurance ON Cloud, *https://www.moon-cloud.eu/*
[2] SEcure Service-oriented Architectures Research Lab - *http://sesar.di.unimi.it*

2.2 Terminologia

- **Metriche**: insieme di proprietà non funzionali di cui si vogliono ottenere **misurazioni**.
- **Controllo**: rappresenta la modalità di raccolta ed elaborazione delle *misurazioni* di una *metrica*. Esso è descritto tramite un documento *JSON*[3], i cui attributi sono
  - **name**, nome del controllo
  - **description**, descrizione del controllo
  - **category**, categoria di appartenenza
  - **driver-name**, nome del driver che ne implementa il flusso di esecuzione
  - **inputs**, dati ricevuti in input
  - **outputs**, dati attesi in output (*misurazioni*)
- **Driver**: la porzione di codice che implementa il controllo
- **Test**: istanza di un controllo, che ne rappresenta l'esecuzione con gli input effettivi
- **Regola di valutazione astratta**, o *AER (abstract evaluation rule)*, regola logica che implementa un processo di valutazione. È data dall'aggregazione di controlli mediante operatori *booleani*. I suoi termini possono essere *controlli* e altre *AER*.
- **Regola di valutazione concreta**, o *ER (evaluation rule)*: istanza di una *AER*. I suoi termini possono essere *test* (mappati sui rispettivi *controlli* o altre *ER*.

[3]JSON, JavaScript Object Notation, *http://www.json.org/*

2.3 Architettura e componenti

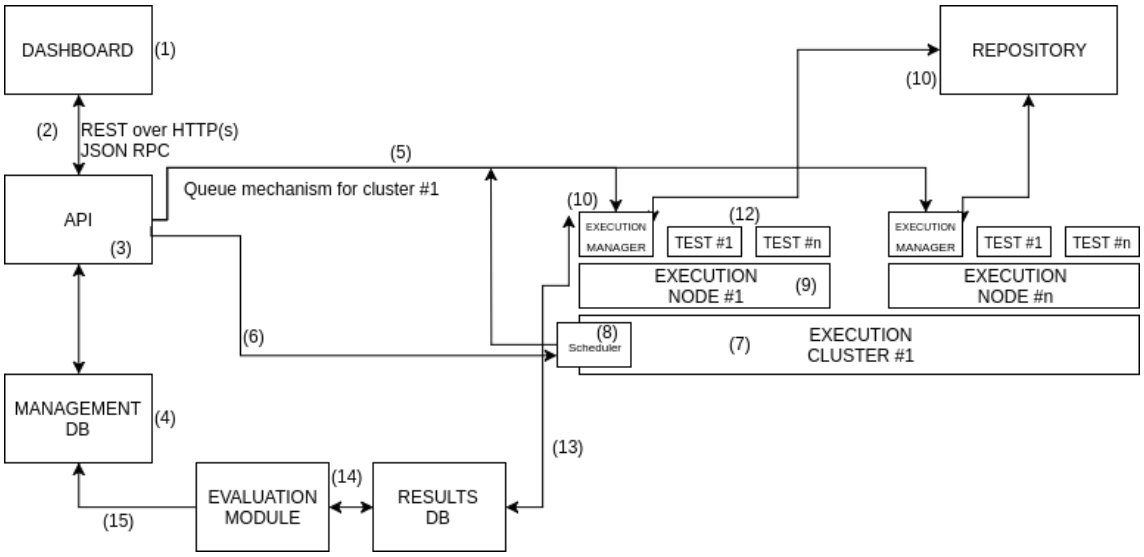


Figura 2.1: Architettura e componenti di Moon Cloud

In figura 2.1 sono illustrate l'architettura del framework Moon Cloud e l'interazione tra i vari microservizi che lo compongono. Questa può essere divisa in due aree. La prima, accessibile dagli utenti del sistema fornisce le funzionalità di gestione e comprende:

- **Dashboard** (1), sviluppata in Javascript, HTML5 e CSS mediante il framework Angular.JS. Rappresenta il punto di ingresso per l'utente, e fornisce un'interfaccia grafica per la fruizione delle funzionalità del prodotto. La *Dashboard* è supportata da API HTTP servite in modo sicuro tramite il protocollo TLS (2).
- **API** (3), costituiscono l'intefaccia con le principali funzionalità del sistema. Interagiscono con un database di management (4) seguendo il paradigma RESTful, e orchestrano l'esecuzione dei test. Il test può essere lanciato:
  - in modalità one-shot, inviando un messaggio agli *execution manager* (9) mediante un meccanismo di comunicazione basato su code(5).
  - inserendo un *task* periodico(6) nello *scheduler* (7)

  Successivamente alla conclusione del test di sicurezza, *one-shot* o *periodico* che sia, i risultati restituiti saranno disponibili sulla dashboard, con la possibilità di filtrarli e analizzarne le metriche.

La seconda invece, rappresenta il vero e proprio backend del framework, gestendo i meccanismi di esecuzione dei test, raccolta dei risultati e valutazione degli stessi. È composta da:

- **Execution Cluster** (8), ovvero l'insieme dei nodi - *execution node*, (9) - che eseguono materialmente il test. Gli execution cluster sono equipaggiati da

uno *scheduler* (7), che gestisce l'esecuzione temporizzata dei test periodici, per effettuare il monitoraggio in modo continuo, inviando i test in esso memorizzati a cadenze temporali scandite da un pattern *CRON*[4].

- **Execution Manager** (10), ovvero il servizio che gestisce il lavoro di ciascun nodo del cluster. Gli *execution manager* di uno stesso cluster sono connessi alla stessa coda: all'arrivo di un messaggio essi effettuano il download il driver relativo al controllo referenziato dal test dal repository (11), eseguono lo stesso con gli input contenuti nel messaggio, e collezionano gli output del test nel *results database*.

- **Evaluation Module** (13), rimane in ascolto sul database dei risultati (12) in attesa di eventi. Quando lo stato di uno specifico test cambia, avvia la procedura di valutazione di tutte le *ER* che fanno riferimento a tale test, e ne memorizza il risultato nel database di management (4).

- **Repository** (10), contiene i driver per i controlli di sicurezza. È realizzato tramite un ambiente Git[5], di cui condivide le funzionalità, e da un *registry* di *container*, che rappresentano il singolo driver. Il processo di sviluppo di un driver è ultimato da un motore di *continuous integration* che contestualmente al caricamento del codice dello stesso sul *repository* effettua la build del *container* associato e test automatici di validazione e sanitizzazione dello stesso, per poi pubblicare il *container* sul *registry*.

2.4 Moon Cloud come strumento di verifica delle raccomandazioni

Mediante i componenti software illustrati nel paragrafo precedente, Moon Cloud è in grado di effettuare un processo di *security assessment* basato sulla verifica di *recommendation*. Per verifica delle *recommendation* si intende il controllo della conformità di un sistema target rispetto ad una data raccomandazione.

Si tratta di un processo complesso, che richiede l'aggregazione delle valutazioni di diversi servizi. La tecnica adottata da Moon Cloud consiste nella raccolta di evidenze mediante il testing e il monitoraggio di uno specifico servizio, al fine di verificare se la raccomandazione sia effettivamente rispettata oppure no[35].

Definizione 2.4.1 (Recommendation verification[35]) *Sia R la recommendation da verificare, la reccomendation verification è una funzione $\widehat{R}$ definita sulla tupla $\langle EP, ER \rangle$ che restituisce un valore booleano {true, false} dove:*

- *EP è l'insieme di processi di valutazione $\{Eval\}$ da eseguire. L'output del processo di valutazione è un valore booleano che espreime se la valutazione abbia avuto successo o no, aggregato alle evidence collezionate a supporto del risultato.*

[4]http://man7.org/linux/man-pages/man5/crontab.5.html
[5]Git, *https://git-scm.com/*

- *ER è una evaluation rule espressa come formula di logica proposizionale, i cui termini sono i singoli processi di valutazione $Eval$. Essa combina il risultato di vari processi $Eval \in EP$ e restituisce true se la valutazione ha successo, altrimenti restituisce false.*

Definizione 2.4.2 (Eval{}) *Un processo di valutazione[35] $Eval\{\}$ è una tupla della forma $\langle t, C \rangle$, dove:*

- *t è il* ToE (Target of Evaluation)*, ovvero i servizi o i meccanismi, che costituiscono il perimetro entro cui la proprietà o la funzionalità di sicurezza deve essere valutata*
- *C è il* Control*, ovvero la funzione di valutazione su t che restituisce il risultato della valutazione insieme a un insieme di evidenze.*

Un controllo C specifica i dettagli su come collezionare le evidenze su un target t per valutare la *reccomendation*. È definito nel seguente modo[35]:

Definizione 2.4.3 (C) *C è definito su una tripla della forma $\langle \phi, \lambda, \pi \rangle$, dove:*

- *ϕ è il flusso di esecuzione del processo di raccolta delle evidenze. È composto da una sequenza di operazioni atomiche.*
- *λ è un insieme di parametri necessari a collegare il flusso ϕ al target t*
- *π è un insieme di Environmental Settings che descrivono le caratteristiche dell'ambiente in cui il controllo deve essere eseguito e le possibili dipendenze software dello stesso.*

Moon Cloud è in grado di eseguire molteplici processi di valutazione $Eval$ in parallelo, ciascuno dei quali si riferisce a un insieme di raccomandazioni R che devono essere valutati. I controlli C sono modellati utilizzando degli schemi, il flusso di esecuzione del codice (ϕ) è modellato come una catena formata da tutte le operazioni che un controllo necessita di effettuare per raccogliere le evidenze, ed è implementato sotto forma di script Python. I parametri (λ) e l'ambiente (π) sono rappresentati da metadati; ciascuna operazione del flusso ϕ è collegata agli specifici parametri necessari per la valutazione, mentre l'ambiente π rappresenta l'insieme di prerequisiti e dipendenze che devono persistere per l'esecuzione del controllo[35].

2.4.1 Regole di valutazione

Nel contesto implementativo le regole di valutazione sono modellate attraverso le classi *AbstractEvaluationRule* e *EvaluationRule*, rispettivamente per le regole astratte e per le regole concrete. Di seguito verranno approfondite entrambe le classi.

Regole di valutazione astratte

Per la classe *AbstractEvaluationRule* è definita una proprietà *formula* che contiene la formula in logica proposizionale che rappresenta il processo di valutazione.

La formula è espressa in un linguaggio libero dal contesto la cui grammatica è definita tramite la seguente BNF[6]:

```
expressions
    : expr $
    ;

expr
    : TOKEN_VAR
    | expr TOKEN_AND expr
    | expr TOKEN_OR expr
    | expr TOKEN_IMPLIES expr
    | expr TOKEN_IFF expr
    | TOKEN_NOT expr
    | TOKEN_LPAREN expr TOKEN_RPAREN
    ;
```

I token di questa grammatica sono *variabili* gestite dall'espressione regolare

- TOKEN_VAR → *[cf]"#"\d+*

e *operatori* (distinguibili in operatori unari e binari a seconda dell'arietà), implementati nel seguente modo:

- TOKEN_NOT → not(expr), operatore unario che effettua la negazione del termine: $return \sim expr$
- TOKEN_AND → and(expr1, expr2), operatore binario che effettua l'*and* logico dei termini: $return\ expr1 \wedge expr2$
- TOKEN_OR → or(expr1, expr2), operatore binario che effettua l'*or* logico dei termini: $return\ expr1 \vee expr2$
- TOKEN_IMPLIES → implies(term1, term2), operatore binario che implementa l'operatore di implicazione: $return \sim expr1 \vee expr2$
- TOKEN_IFF → iff(term1, term2), operatore binario che implementa l'operatore "se e solo se": $return\ (\sim term1 \vee term2) \wedge (\sim term2 \vee term1)$

TOKEN_LPAREN e *TOKEN_RPAREN* sono rispettivamente la parentesi tonda aperta e chiusa.

Tramite questo linguaggio è possibile generare tutte le formule ben formate della logica proposizionale.

[6]BNF, Backus-Naur Form

Le variabili possono essere quindi *Controlli* (rappresentati dalla classe *Control*, e indicati nella formula con la sintassi "c#<id>", dove <id> è l'identificativo del controllo) ed altre *AER* (indicate nella formula, in modo analogo ai controlli, con la sintassi "f#<id>"). Ciò permette di organizzare le regole di valutazione astratte secondo una gerarchia, concedendo all'utente una maggiore capacità espressiva nel processo di traduzione da politica a regola logica.

Regole di valutazione concrete

Le regole di valutazione concrete rappresentano le istanze delle *AER* sopra descritte. In questo caso la proprietà *formula* è derivata mediante l'applicazione della funzione di mapping $m(\chi)$, (2.1) dove χ è la regola di valutazione astratta di partenza, c_i è un controllo, t_i è un test ed e è una regola di valutazione concreta.

$$m(\chi) : c \rightarrow t \; \forall c_i \in \chi \mid t \text{ refers } c \text{ , } f \rightarrow e \; \forall \chi_i \in \chi \mid e \text{ refers } \chi_i \tag{2.1}$$

Tutte le regole di valutazione astratte incluse nella regola di partenza sono quindi sostituite da una o più regole di valutazione concrete che le referenziano, analogamente tutti i controlli inclusi nella regola di partenza sono sostituiti da uno o più test. Il mapping avviene sulla base di un oggetto JSON *chiave-valore*, in cui la chiave rappresenta l'identificativo dell'elemento di partenza e il valore rappresenta l'identificativo dell'elemento di arrivo.

La grammatica utilizzata per la validazione della formula così derivata, è ovviamente analoga alla precedente, ad eccezione del token *TOKEN_VAR* che assume valori rappresentabili dalla seguente espressione regolare:

$$\text{TOKEN\_VAR} \rightarrow \textit{[et]"\#"\textbackslash d+}$$

supportando il carattere '*e*' per indicare le Evaluation Rule, e il carattere '*t*' per indicare i test. In fase di esecuzione del processo di valutazione sarà questa la formula effettivamente utilizzata, sostituendo a ciascun termine il valore booleano del test o dell'evaluation rule referenziata.

2.4.2 Driver per i controlli di sicurezza

Di seguito verrà illustrata la struttura di un driver Moon Cloud, utilizzato per l'implementazione effettiva dei controlli di sicurezza e per l'esecuzione dei test.

I driver sono costituiti da container *Docker* basati sull'immagine *python:2-onbuild*[7] e possono essere eseguiti sia all'interno del framework Moon Cloud che in modalità completamente standalone. Il container è gestito da un *entrypoint* che riceve gli input per l'esecuzione del test, colleziona eventuali log di diagnostica e restituisce gli output all'*Execution Manager*. Sia l'input che l'output di un driver sono costituiti da documenti JSON le cui chiavi devono corrispondere a quelle dichiarate negli attributi *inputs* e *outputs*, del *Controllo* corrispondente, precedentemente trattati nella sezione 2.2

Struttura di un driver

All'interno del container sono presenti due componenti:

- *entrypoint.py*, il cui ruolo è quello di leggere ed effettuare la deserializzazione degli *input*, leggere i metadati del driver, e precaricare la classe del driver. Il discovery della classe viene fatto in modo automatico da una directory chiamata *test/* che andremo a dettagliare tra poco.
- *driver.py*, che fornisce un'*interfaccia* mediante la classe *Driver* che ciascun payload dovrà implementare. Una peculiarità della classe *Driver* è la presenza della sottoclasse *__metaclass__* che fornisce un meccanismo di *subscription* per tutte le classi che ereditano da Driver. Questo permette di far funzionare il meccanismo di *autodiscovery*, permettendo a chi scrive il payload di lavorare in modo agnostico rispetto alle funzionalità del framework. L'esecuzione effettiva del codice avviene per mezzo del metodo *run* e un meccanismo di gestione delle operazioni atomiche in due flussi (forward e rollback) dettagliatamente illustrati nella sezione successiva. Un'altra classe molto importante è la classe *DriverResult* che fornisce la possibilità di restituire le misurazioni effettuate dal controllo in forma *chiave-valore*.

Altri due file molto importanti sono:

- *Dockerfile*, che costituisce la definizione di ogni container Docker. Questo permette di installare o compilare eventuali dipendenze software utili all'esecuzione del driver
- *requirements.txt*, che, in Python, contiene tutte le librerie del database PyPI[8] da cui il codice del driver dipende.

Payload del driver

Il payload del driver è contenuto nella directory *test*, ed è costituito da una classe che eredita la classe *Driver* illustrata in 2.4.2 e ne implementa il metodo di interfaccia *appendAtomics*.

Esso è definito da:

[7] https://hub.docker.com/_/python/
[8] https://pypi.python.org/

- una sequenza A di n operazioni atomiche o_n, con corrispondenza biunivoca con le chiavi specificate nel documento JSON di input

$$A = \{o_0, o_1, o_2, ..., o_n\}$$

- una sequenza di n operazioni di rollback - una per ogni operazione atomica - che svolgono azioni di *undo*

$$R = \neg A = \{r_0, r_1, r_2, ..., r_n\}$$

aggregati in coppie ordinate.

$$P = \{(o_0, r_0), (o_1, r_1), (o_2, r_2), ..., (o_n, r_n)\}$$

Ogni operazione atomica $o_x \in A$ riceve in input gli output dell'operazione o_{x-1}; analogamente ogni operazione r_x di rollback $r \in R$ riceve in input gli output di r_{x+1}.

$$R_1 \subseteq R = \{r_{x-1}, r_(x-2), ..., r_{x-n}\}$$

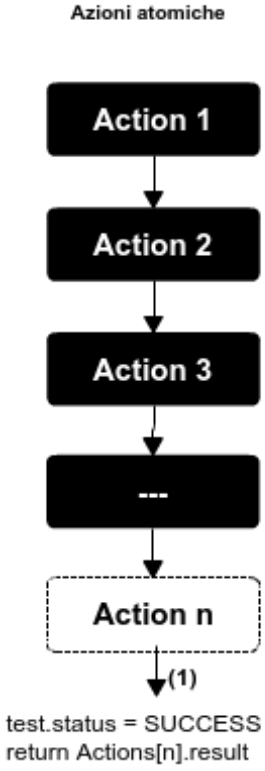


Figura 2.2: Esecuzione corretta di un test

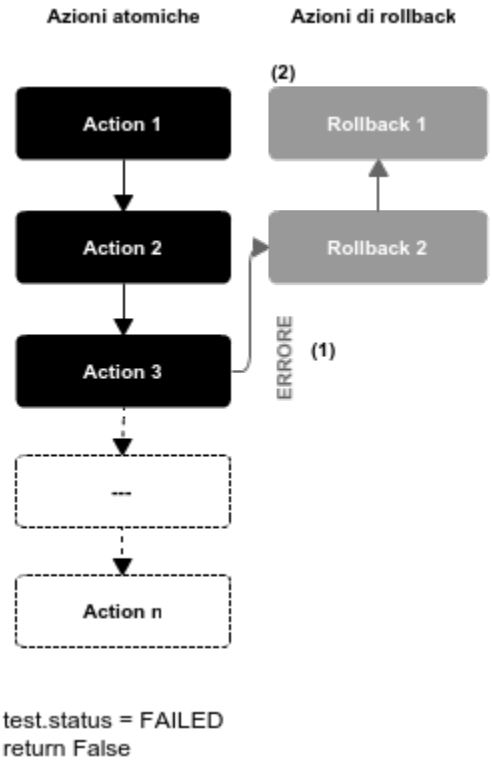


Figura 2.3: Esecuzione di un test con operazioni di rollback

Nella figura 2.2 è mostrata l'esecuzione di un driver di sonda il cui test viene eseguito correttamente. Il risultato dell'ultima operazione atomica deve essere un valore *boolean* e viene utilizzato come risultato finale (1).

In caso di fallimento di un'operazione $o_x \in P$, $x \leq n$ (figura 2.3) (1) l'interfaccia della classe *Driver* si occupa di lasciare il sistema target in uno stato sicuro provvedendo ad eseguire in sequenza le operazioni di rollback e restituendo come risultato *False*.

Gli input globali del test sono disponibili interrogando la proprietà "*testinstances*", un dizionario a due livelli che contiene nella chiave di primo livello il nome della fase a cui l'input è riferito, nella chiave di secondo livello il nome della chiave del valore di input.

```
1
2  from driver import Driver
3  from time import sleep
4
5  class MyDriver(Driver):
6      def step1(self, inputs):
7          self.logger.info("Sto eseguendo lo step 1")
8          sleep(10)
9          self.logger.info("Ho eseguito lo step 1")
10         return True
11
12     def rollback1(self, inputs):
13         self.logger.info("Sto eseguendo il rollback dello step 1")
14         sleep(10)
15         self.logger.info("Ho eseguito il rollback per lo step 1")
16
17     def step2(self, inputs):
18         self.logger.info("Sto eseguendo lo step 2")
19         self.logger.info("Stampo gli input del test")
20         self.logger.info(json.dumps(self.testinstances))
21         sleep(10)
22         self.logger.info("Ho eseguito lo step 2")
23
24     def rollback2(self, inputs):
25         self.logger.info("Sto eseguendo il rollback per lo step 2")
26         sleep(10)
27         self.logger.info("Ho eseguito il rollback per lo step 2")
28
29     def appendAtomics(self):
30         self.appendAtomic(self.step1, self.rollback1)
31         self.appendAtomic(self.step2, self.rollback2)
```

Nella directory "test", oltre al payload del driver, è contenuto un file *metadata.json* con le seguenti chiavi:

- driver-name, nome del driver
- inputs, oggetto di cui le chiavi costituiscono il nome simbolico da associare all'input e i valori costituiscono il tipo di dato atteso (stringa, intero ed eventuali tipi di dato personalizzati, anche complessi, come indirizzo ip, account Amazon, account OpenStack)
- outputs, oggetto analogo ad inputs, ma per la gestione degli output
- schema, oggetto contenente lo JSON schema utilizzato per effettuare il rendering del form di input nella dashboard

2.5 Esempio

Verrà di seguito proposto un esempio per illustrare la definizione completa di un processo di valutazione all'interno della piattaforma Moon Cloud. La proprietà

analizzata da questo esempio è la *confidenzialità del dato* ottenuta dall'aggregazione in *and* logico di due diversi controlli:

1. Confidenzialità dello storage (*c#1*)
2. Confidenzialità del canale di comunicazione (*c#2*)

2.5.1 Abstract Evaluation Rule

`c#1 and c#2`

```
{
    "id":1,
    "name":"Data Confidentiality",
    "description":"It allows to execute a set of tests against a given service to ensure
         that information are provided over a secure channel and stored over a secure
        storage.",
    "category":[],
    "formula":"c#1 and c#2",
    "enforced_control":null,
    "enforced_operator":null,
    "cardinality":null,
    "related_controls":[1, 2],
    "related_aers":[],
    "metadata":null
}
```

2.5.2 Controllo

Confidenzialità dello storage

```
{
  "category" : [  ],
  "driver" : "storage-confidentiality",
  "id" : 1,
  "metadata" : {
      "description" : "Evaluates storage confidentiality for a given target",
      "schema" : {
          "config" : {
              "properties" : {
                  "ssh_string" : {
                      "title" : "SSH Connection String",
                      "type" : "string"
                    },
                  "ssh_key" : {
                      "title" : "SSH Key",
                      "type" : "string"
                    },
                    "device_to_check": {
                        "title": "Device to check",
                        "type":"string",
                        "default": "/dev/sda"
                    }
                },
              "title" : "Target",
              "type" : "object"
          }
      },
      "inputs": {
          "config": {
              "ssh_string": "string",
              "ssh_key": "string",
              "device_to_check": "string",
          }
      },
```

```
35          "outputs": {
36              "result": "boolean"
37          }
38      },
39    "name" : "Checks luks is enabled on target"
40  }
```

Confidenzialità del canale

```
1   {
2     "category" : [  ],
3     "driver" : "channel-confidentiality",
4     "id" : 1,
5     "metadata" : {
6         "description" : "Evaluates SSL configuration for a given target",
7         "schema" : {
8             "config" : {
9                 "properties" : {
10                    "host" : {
11                        "title" : "Host",
12                        "type" : "string"
13                    },
14                    "port" : {
15                        "default" : 80,
16                        "title" : "port",
17                        "type" : "number"
18                    }
19                },
20                "title" : "Target",
21                "type" : "object"
22            }
23        },
24        "inputs": {
25            "config": {
26                "host": "hostname",
27                "port": "integer"
28            }
29        },
30        "outputs": {
31            "result": "boolean",
32            "strength": "string"
33        }
34    },
35    "name" : "Check channel confidentiality"
36  }
```

2.5.3 Evaluation Rule

```
t#1 and t#2
```

```
1     {
2       "aer" : 1,
3       "description" : "Checks storage confidentiality and network confidentiality on the
            target tufarolo.eu",
4       "id" : 1,
5       "mapping" : {
6           "c#1":"t#1",
7           "c#2":"t#2"
8       },
9       "name" : "Confidentiality tufarolo.eu",
10      "related_ers" : [  ],
11      "related_tests" : [ 1, 2 ],
12      "status" : 0,
13    }
```

2.5.4 Test

Confidenzialità dello storage

```
{
    "control" : 1,
    "description" : "",
    "execution_cluster" : 1,
    "id" : 11,
    "name" : "",
    "testcase" : {
            "config" : {
                "ssh_string" : "user@tufarolo.eu:22",
                "ssh_key" : ".....",
                "device_to_check": "/dev/sda1"
            }
      },
    "__unicode__" : "t#1"
  }
```

Confidenzialità del canale

```
{
    "control" : 2,
    "description" : "",
    "execution_cluster" : 1,
    "id" : 11,
    "name" : "",
    "testcase" : {
        "config" : {
            "host" : "tufarolo.eu",
            "port" : 80
          } },
    "__unicode__" : "t#2"
  }
```

2.5.5 Driver

Confidenzialità dello storage

```
from driver import Driver
from libraries import ssh
class StorageConfidentiality(Driver):
    def connect_to_ssh(self, inputs):
    ssh.connect(self.testinstances.get("ssh").get("ssh_string"), self.testinstances..get
        ("ssh").get("ssh_key")))

    def check_is_luks(self, inputs):
        return ssh.run("/bin/cryptsetup isLuks \%s" \% self.testinstances.get())

    def appendAtomics(self):
        self.appendAtomic(self.connect_to_ssh, lambda(x): None)
        self.appendAtomic(self.check_is_luks, lambda(x): None)
```

Confidenzialità del canale

```
from driver import Driver
from libraries import ssl
class ChannelConfidentiality(Driver):
    def check_ssl(self, inputs):
        target = self.testinstances.get("config").get("target")
```

```
6           port = self.testinstances.get("port").get("port")
7           status, strength =  ssl.check(target, port)
8           self.result.data["strength"] = strength
9           return status
10      def appendAtomics(self):
11          self.appendAtomic(self.check_ssl, lambda(x): None)
```

Capitolo 3

FedRAMP - Federal Risk and Authorization Management Program

3.1 Introduzione

In questo capitolo verrà approfondito FedRAMP, il programma federale americano per la gestione del rischio e delle autorizzazioni nella cloud. Sarà proposta un'analisi degli obiettivi del programma, specificando le problematiche in esso affrontate in relazione anche a quanto descritto nel capitolo precedente. Verrà poi esposta la struttura del documento, dopodiché ci si concentrerà sulla struttura dello stesso approfondendo i ruoli degli attori coinvolti, e il contributo che questo lavoro di tesi vuole apportare per ciascun caso trattato. In conclusione saranno esposti i concetti di *readiness* e di *compliance* al programma, e sarà approfondita l'implementazione di FedRAMP in Amazon AWS.

3.2 Cos'è FedRAMP

FedRAMP è il programma governativo americano l'applicazione del **FISMA** (Federal Information Security Management Act) nell'adozione di tecnologie cloud. Esso propone un approccio standardizzato al *security assessment*, alle autorizzazioni e al monitoraggio continuo di prodotti e servizi cloud, fornendo un insieme di requisiti di sicurezza e un programma di assessment indipendente, nato dalla collaborazione di esperti di sicurezza e di tecnologie cloud. Le entità coinvolte nella redazione di questo programma sono state molte: la General Services Administration (GSA), il National Institute of Standards and Technology (NIST), il dipartimento di Sicurezza Nazionale (Department of Homeland Security, DHS), il dipartimento della Difesa (Department of Defense, DOD), la National Security Agency (NSA), l'Office of Management and Budget (OMB).

I *cloud service provider* che vogliono offrire servizi per la pubblica amministrazione americana e gli uffici federali devono essere autorizzati tramite questo programma. Nonostante sia stato sviluppato nel contesto USA, la dinamicità e l'elasticità di FedRAMP ne ha permesso l'adozione *de-facto* anche in altre nazioni, specialmente dell'Asia orientale e del nord Europa.

3.2.1 FISMA, Federal Information Security Management Act

Il FISMA è uno standard di sicurezza, entrato in vigore come legge il 17 Dicembre 2002 come "Titolo III" dell'E-Government Act[36]: ciascun sistema che ospiti dati governativi deve essere autorizzato tramite il FISMA prima di essere messo in produzione. Esso definisce tre obiettivi principali per la sicurezza dei sistemi informativi federali:

- **Confidenzialità**, per garantire restrizioni autorizzate sull'accesso e la *disclosure* dei dati, con l'obiettivo di proteggere la privacy ed eventuale informazioni sul proprietario odegli stessi
- **Integrità**, per proteggere il dato da manipolazioni o azioni distruttive e per garantire allo stesso tempo l'autenticità e la non-repudiabilità dell'informazione
- **Disponibilità**, per assicurare condizioni di affidabilità nell'accesso al dato

A tal fine il **NIST** ha prodotto il **Federal Information Risk Management Framework** (*RMF*) il quale organizza i sistemi informatici sulla base del livello di rischio e descrive un insieme minimo di requisiti che devono essere rispettati per garantire un livello di sicurezza adeguato [37], fornendo una metodologia per la selezione dei controlli di sicurezza e per l'esecuzione del deployment e dell'assessment.

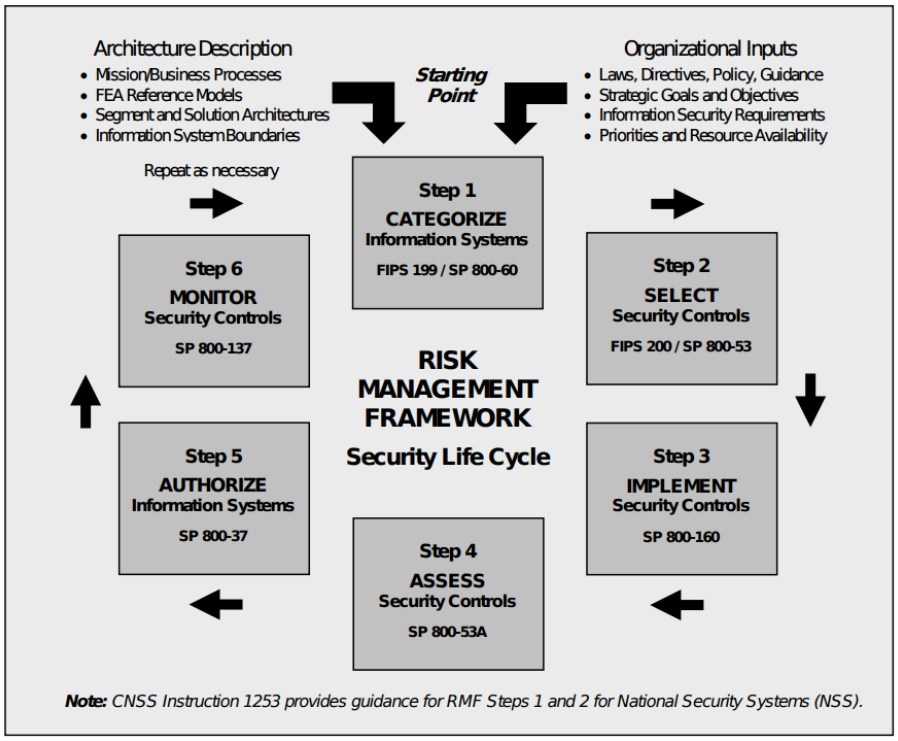


Figura 3.1: Risk Management Framework [37]

Tramite la figura 3.1 è possibile identificare le sei fasi che compongono il processo di gestione del rischio, ciclico e continuo, identificato dal framework:

- **Categorizzazione del sistema informativo**, tramite i documenti FIPS[1] 199 e NIST SP 800-60 v2[38]. Il documento FIPS 199 classifica i sistemi in base al livello di rischio, e contiene i criteri da utilizzare nella categorizzazione. Questi criteri sono basati sull'impatto potenziale di una violazione delle proprietà di confidenzialità, integrità e disponibilità sul sistema e sono: i) Rischio basso, impatto limitato, ii) Rischio medio, con serie conseguenze, iii) Rischio elevato con conseguenze gravi e catrastofiche. FIPS 199 si applica a tutti i sistemi, ad esclusione di quelli designati per l'uso della sicurezza nazionale.

- **Selezione dei controlli di sicurezza**, mediante i documenti FIPS 200 e SP 800-53. FIPS 200 fornisce i requisiti di sicurezza minimi (e i relativi controlli) per ogni categoria definita nel FIPS 199. Il documento NIST 800-53[37] invece definisce i controlli di sicurezza e fornisce le linee guida per scegliere i profili da impiegare per soddisfare i requisiti minimi di sicurezza, in base all'impatto del sistema. I controlli di sicurezza sono divisi in 17 famiglie e vengono divisi in tre classi (controlli di gestione, controlli operazionali e controlli tecnici).

- **Implementazione dei controlli**, guidata dal documento SP 800-160[39]

- **Assessment dei controlli di sicurezza**, regolato dal documento SP 800-53[37]

- **Autorizzazione del sistema informativo**, basata sul documento SP 800-37[40]

- **Fase di monitoraggio**[41]

3.2.2 Obiettivo di FedRAMP

L'obiettivo di FedRAMP è quello di fornire un framework per semplificare il processo di autorizzazione dei servizi cloud adottati dagli enti governativi USA. Prima dell'adozione di questo programma i produttori di sistemi e applicativi dovevano eseguire l'intero processo di autorizzazione per ciascuna delle agenzie che adottasse il sistema, così come ogni ente gestiva un processo di gestione del rischio a sé stante, anche nel caso in cui un'altra agenzia avesse già adottato servizi e misure di sicurezza analoghi. FedRAMP affronta la problematica nei seguenti modi[42]:

- Fornendo processi di valutazione della sicurezza e autorizzazione congiunti, basati su una serie di requisiti e controlli standardizzati, sulla base dell'impatto del sistema

- Strutturando un processo di analisi e valutazione della conformità condotto da Organizzazioni di terze parti approvate (3PAO), per valutare costantemente la capacità di un provider di servizi cloud (CSP) di soddisfare requisiti di sicurezza desiderati

[1] Federal Information Processing Standards

- Coordinando servizi di monitoraggio continuo
- Fornendo pacchetti di autorizzazione composti da servizi cloud già revisionati da una Joint Authorization Board (JAB), composta da esperti di sicurezza provienienti dal DHS, dalla GSA e del DoD.
- Offrendo un linguaggio standardizzato per aiutare i dipartimenti e gli enti governativi ad integrare i requisiti di FedRAMP all'interno dei processi interni
- Un repository di pacchetti di autorizzazione per i servizi cloud che possono essere utilizzati dal governo

L'utilizzo di un framework centralizzato ha inevitabilmente determinato un risparmio notevole anche in termini economici, sia per il governo americano, che per i cloud service provider: si stima che questo ammonti a circa $250,000 per ciascun sistema autorizzato, per un totale di circa 160 implementazioni dello standard FISMA. Il risparmio stimato per il governo è quindi di 40 milioni di dollari [43].

3.3 Struttura

Il programma fornisce un percorso che i fornitori di servizi cloud possono intraprendere per ottenere una autorizzazione provvisoria, da sottoporre in una successiva fase di *security assessment* che verrà poi revisionata dalla *JAB*. Mediante questo approccio preventivo è possibile quindi anticipare l'*assessment* dei controlli di sicurezza e di velocizzare il processo di autorizzazione definitiva dell'applicativo o sistema cloud.

3.3.1 CSP: FedRAMP readiness

Il provider che vuole partecipare a FedRAMP deve innanzitutto soddisfare una serie di requisiti di *readiness*:

1. Essere in grado di trattare eventuali processi forensi elettronici e contenziosi
2. Essere in grado di definire e descrivere chiaramente i confini del proprio sistema
3. Identificare le responsabilità del cliente e le azioni che questo deve compiere per implementare i controlli di sicurezza
4. Fornire un meccanismo di identificazione e autenticazione a due fattori per l'accesso via rete agli account privilegiati
5. Fornire un meccanismo di identificazione e autenticazione a due fattori per l'accesso via rete agli account non privilegiati
6. Fornire un meccanismo di identificazione e autenticazione a due fattori per l'accesso locale agli account privilegiati

7. Avere la possibilità di eseguire analisi del codice per le soluzioni software proprietarie

8. Avere protezioni di confine garantendo isolamento logico e fisico degli asset

9. Avere l'abilità di rimediare a situazioni di rischio elevato entro i 30 giorni (90 giorni per le situazioni di rischio moderato)

10. Fornire un inventario e configurazioni standard per tutti i dispositivi

11. Avere meccanismi di sicurezza che impediscano la fuoriuscita di informazioni nell'utilizzo di mezzi di comunicazione condivisi

12. Adottare meccanismi di crittografia per preservare la confidenzialità e l'integrità dei dati trasmessi sulla rete

Se queste condizioni sono rispettate, è possibile sottomettere un modulo di richiesta di ammissione al programma, disponibile online sul sito web di FedRAMP. A questo seguirà una notifica automatica all'ufficio di gestione del programma e alla *Joint Advisory Board*.

Oltre alle finalità precedentemente esposte, il prodotto sviluppato in questo lavoro di tesi punta a supportare il processo di verifica dei requisiti richiesti per la *readiness*. Poiché questi sono essenzialmente di carattere procedurale, saranno implementati sotto forma di questionario. Per i punti 11 e 12 possono essere forniti anche controlli tecnici, legati però alle tecnologie effettivamente implementate.

3.3.2 Processo di autorizzazione

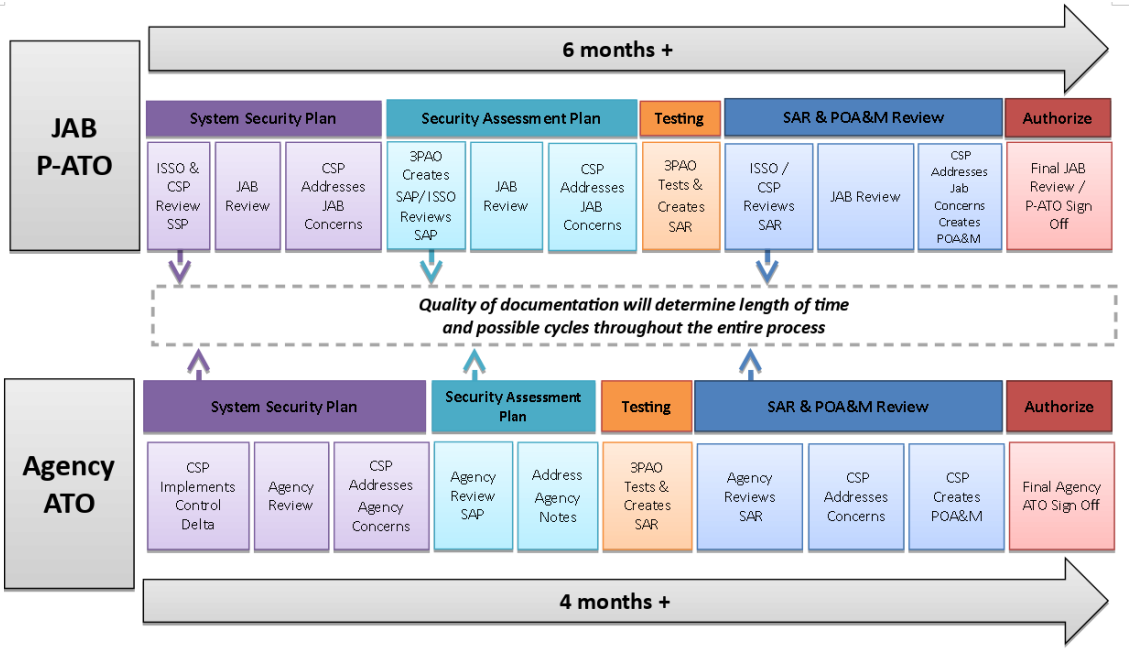


Figura 3.2: Processo di autorizzazione [42]

Nel modulo di richiesta di ammissione al programma il provider fornisce informazioni sul proprio sistema, categorizzandolo sulla base delle direttive contenute nel documento NIST SP 800-60 V2[38], e decide la *baseline* dei controlli di sicurezza da implementare in base alla sensibilità del sistema (bassa o media). A seguito di una revisione della *readiness* da parte dell'ufficio di gestione del programma, sarà possibile avviare il processo di richiesta dell'autorizzazione provisoria (P-ATO): il *cloud service provider* deve quindi ricercare ed assumere un'organizzazione di terze parti, tra quelle specificate sul sito di FedRAMP. L'attore principale è il fornitore di servizi, il quale sottometterà un *security package* e sarà designato come candidato all'autorizzazione. Lo svolgimento del processo può avvenire in due modi:

- *Processo condotto da un'agenzia federale*, che vuole far autorizzare a FedRAMP i sistemi cloud correntemente attivi. In tal caso il processo è totalmente controllato e monitorato dall'ente, il cui compito è quello di sorvegliare sull'implementazione dei controlli di sicurezza mancanti nei sistemi del fornitore di servizi. L'autorizzazione sarà quindi emessa direttamente dall'agenzia.
- *Processo mantenuto dalla Joint Authorization Board*, che analizzerà il livello di sicurezza del fornitore ed emetterà una autorizzazione provvisoria

Attori coinvolti nel processo di autorizzazione

Gli attori coinvolti sono quindi gli enti federali che desiderano adottare un servizio cloud, i fornitori del servizio, e le organizzazioni di terze parti che ne effettuano l'analisi della sicurezza.

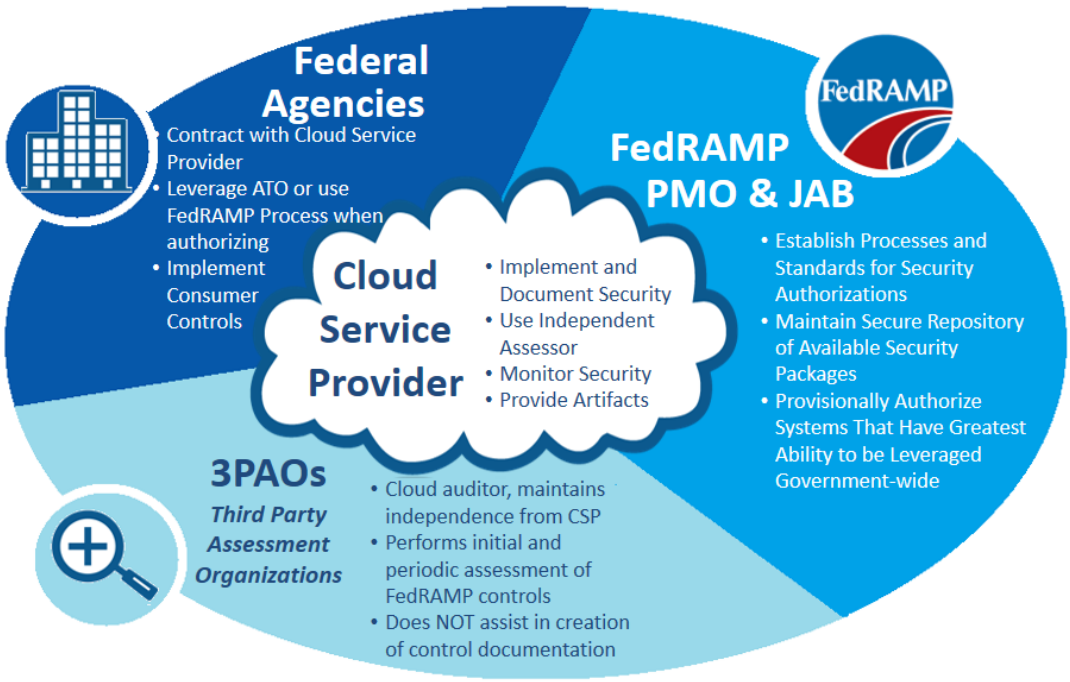


Figura 3.3: Attori coinvolti nel processo di autorizzazione [42]

Enti federali

Il ruolo degli enti federali è quello di garantire che, per tutti i progetti nei quali sono coinvolte tecnologie cloud, siano rispettati i requisiti FedRAMP, venga effettuato l'assessment dei controlli di base, e siano stati forniti i template corretti.

Le agenzie devono catalogare i propri sistemi in un inventario, specificando quali di questi siano di tipo cloud e quali invece siano sistemi tradizionali. È raccomandabile avere un referente che sia preparato a rispondere a quesiti riguardanti l'implementazione dei requisiti FedRAMP. Per facilitare ciò alcune informazioni utili potrebbero essere *i) il nome del sistema cloud, ii) la descrizione del servizio fornito dal sistema, iii) il contatto dl proprietario del sistema, iv) la data di autorizzazione, v) lo stato della compliance* [44].

In fase di migrazione di sistemi tradizionali sul cloud, così come nell'adattamento di servizi cloud pre-esistenti a FedRAMP, è necessario che i requisiti del programma siano rispettati. Le agenzie devono quindi effetturare un'analisi approfondita delle conseguenze del cambio di tecnologia, per determinare i controlli di sicurezza aggiuntivi da effettuare. Analogamente, gli stessi controlli di sicurezza devono interessare eventuali sistemi cloud installati ed utilizzati internamente (private-cloud). In tal caso è necessario predisporre un'analisi condotta da terze parti accreditate. Se, invece, il fornitore del servizio è un privato e questi non ha effettuato l'assessment dei controlli di sicurezza FedRAMP, l'ente governativo è tenuto ad informare il provider e richiederne l'adeguamento immediato.

Le agenzie, sulla base di specifiche esigenze, possono sottomettere eventuali controlli aggiuntivi rispetto a quelli basilari; questi devono devono essere adeguatamente documentati e motivati. Gli altri enti possono poi decidere di adottare questi controlli. Allo stesso modo, come già trattato, le agenzie possono riutilizzare autorizzazioni emesse per altri enti.

Sulla base del E-Government Act del 2002 (Titolo III, Sezione 3544), le agenzie devono inoltre effettuare analisi del rischio periodiche, valutando l'impatto di eventuali violazione della confidenzialitàe dell'integrità dei dati[44].

Uno degli obiettivi della piattaforma presentata in questo lavoro di tesi, è quello di fornire uno strumento a supporto delle agenzie federali per la gestione della sicurezza degli asset inventariati (sistemi tradizionali e cloud), fornendo sia meccanismi di *auto-discovery* degli stessi (ad esempio mediante l'integrazione con le API dei cloud service provider, oppure tramite la scansione delle reti locali), sia un processo di monitoraggio continuativo della stato della compliance.

Organizzazioni di terze parti (3PAO)

Affinché un servizio cloud possa essere autorizzato da FedRAMP, è necessario che un'organizzazione di terze parti ne analizzi la sicurezza mediante l'esecuzione dei controlli standardizzati nel documento NIST 800-53. Per ottenere l'abilitazione ad effettuare queste analisi, l'organizzazione può decidere di iniziare un percorso di accreditamento, il cui obiettivo è quello di garantire che che le analisi siano effettuate in maniera consistente, dettagliata e indipendente. A tal fine, l'organizzazione deve inviare sottomettere del materiale in grado di dimostrare di essere in grado sia di eseguire analisi tecniche adeguate ai livelli attesi, sia di

avere competenza nella gestione dei processi di *compliance*. Questi criteri vengono certificati dalla *American Association for Laboratory Accreditation (A2LA)* che, dopo aver verificato le effettive competenze tecniche in capo alll'organizzazione, effettua un processo di controllo della conformità rispetto allo standard ISO/IEC 17020 (Disposizioni per la transizione degli accreditamenti degli Organismi di ispezione (OdI)).

Il testing della sicurezza nei confronti dei fornitori di servizi deve essere effettuato in modo equo, tramite controlli scelti sulla base della loro categoria di sensibilità. La periodicità è annuale, e la stessa organizzazione non può effettuare una scansione per due anni consecutivi. In alcuni casi può essere necessario eseguire test automatici come utenti autenticati e con pieni privilegi, in modo da poter determinare con precisione le vulnerabilità e il relativo impatto sul sistema. Solo in questo modo, infatti, è possibile avere una visione globale del sistema (ad es. accedere al registro di sistema di Windows, agli attributi dei file di sistema, ai pacchetti e alle patch effettivamente installate). L'utilizzo di un utente con privilegi limitati può restituire sia falsi positivi (ad esempio nel caso di un test di scrittura su directory interne al sistema eseguito in un ambiente *chroot*) e falsi negativi (in caso di assunzioni derivate dall'impossibilità per l'utente di leggere determinati parametri). Eventuali analisi del codice, invece, sono demandate al *cloud service provider*.

Per guidare questo processo in modo standard, FedRAMP fornisce vari template, scaricabili dal sito ufficiale:

- *Security Assessment Plan Template*, il cui scopo è quello di descrivere il piano per l'analisi della sicurezza. Prima di redigere questo documento, l'organizzazione deve incontrarsi col fornitore di servizi cloud per discutere i test da eseguire. Eventuale supporto può essere erogato dall'*Information System Security Officier* di FedRAMP.

- *Security Assessment Test Cases*, in cui vengono descritti i casi di test sulla base del documento NIST 800-53A; alcuni di questi, tuttavia, differiscono poiché sono stati adattati al contesto *cloud*. Nel caso in cui l'organizzazione debba implementare versioni alternative dei controlli di sicurezza, è necessario che i casi di test vengano scritti in modo idoneo ad attestarne l'efficacia.

- *Security Assessment Report*, assiste la parte di reportistica, il cui obiettivo è quello di dettagliare l'analisi eseguita sui sistemi del fornitore di servizi cloud, riportando le evidenze trovate, le possibili operazioni di mitigazione e le eventuali raccomandazioni.

Il sistema progettato nell'ambito di questo progetto di tesi, mira a diventare uno strumento di supporto delle organizzazioni di terze parti. Uno dei possibili sviluppi in tal senso, potrebbe consistere nell'integrazione dei template presentati in questa sezione all'interno della piattaforma realizzata, in modo da poter guidare l'intero processo di *security assessment*, e consentire anche ad organizzazioni differenti di mantenere una cronologia delle analisi svolte su uno specifico servizio cloud.

Fornitori di servizi cloud

Il *cloud service provider* può essere sia un'entità di terze parti commerciale che un altro ente governativo od agenzia. La sua responsabilità è quella di implementare i controlli di sicurezza, di assumere un'organizzazione di terze parti indipendente che effettui l'assessment annuale e di effettuare tutte le procedure per la creazione e la manutenzione delle proprie autorizzazioni.

Le modalità con cui un fornitore di servizi può essere autorizzato sono tre:

- Il provider può inviare la documentazione appropriata al PMO (ufficio di gestione del programma FedRAMP) e alla Joint Advisory Board, che possono erogare un'autorizzazione provvisoria (P-ATO, Provisional Authorization to Operate)
- Il provider può inviare la documentazione appropriata al PMO e ad un'agenzia, che può erogare un'autorizzazione ad operare (ATO, Authorization to Operate). Un'altra agenzia può utilizzare poi la stessa autorizzazione, abbreviando i tempi di approvazione.
- Il provider può inviare la documentazione per intraprendere autonomamente un percorso di tipo "CSP supplied". In tal caso, dovrà assumere una organizzazione di terze parti che ne analizzi la sicurezza.

Quindi, affinché un sistema cloud sia conforme con FedRAMP:

- deve essere stato creato e sottomesso un pacchetto, utilizzando i template idonei
- deve essere stato eseguito l'assessment, da parte di un'organizzazione di terze parti accreditata e indipendente, mediante l'esecuzione dei controlli di sicurezza relativi al livello di sensibilità del sistema (basso o medio, in quanto i sistemi ad alta sensibilità non sono supportati dal programma e devono essere gestiti separatamente).
- l'assessment deve aver restituito risultati positivi, attestando che i requisiti di sicurezza siano effettivamente verificati
- deve essere stata erogata un'autorizzazione ad operare, provvisoria o definitiva

3.4 CSP: Ulteriori oneri

Successivamente al rilascio dell'autorizzazione provvisoria ad operare, il *cloud service provider* deve sottomettere altri documenti la cui redazione è, ancora una volta, guidata da template disponibili sul sito. Questi devono poi essere inclusi in un *security package*.

- **FIPS 199** nel quale, come precedentemente illustrato, va effettuata la categorizzazione dei sistemi in base al relativo livello di sensibilità, sulla base del documento NIST 800-60. I fornitori di servizi a livello IaaS e PaaS devono seguire le indicazioni della sezione C.3.5 di tale documento.

- **E-Authentication** per l'analisi dei processi dell'autenticazione elettronica, al fine di garantire che siano state implementate misure idonee a minimizzare il livello di rischio. I criteri da utilizzare in questo caso, sono riferiti al documento NIST 800-63.

- **PTA e PIA**, Privacy Threshold Analysis & Privacy Impact Assessment, composti da solo quattro domande che hanno lo scopo di individuare il livello di privacy relativo al sistema e di pianificare l'esecuzione degli eventuali controlli di sicurezza relativi In particolare va specificato se l'esecuzione di questi controlli implica l'utilizzo di eventuali meccanismi di autenticazione con impatti sulla privacy (ad esempio utilizzo dell'autenticazione biometrica per l'accesso ai locali) per gli operatori dell'organizzazione di terze parti che eseguono gli stessi.

- **CTW**, Control Taylor WorkBook, il cui obiettivo è quello di riassumere gli scenari di utilizzo dei servizi offerti da parte dell'agenzia.

- **CIS**, Control Implementation Summary, nel quale è indicato lo stato dell'implementazione dei controlli nel sistema e il responsabile del processo di gestione degli stessi.

- **SSP**, System Security Plan, il quale descrive le modalità con cui sono (o saranno) implementati i controlli di sicurezza previsti.

Inoltre il fornitore del servizio deve fornire un manuale utente che spieghi le modalità di utilizzo del sistema (ad esempio illustrando fornendo la documentazione per eventuali Dashboard o interfacce API).

Il ruolo del prodotto presentato nel lavoro di tesi, in tal caso, è quello di supportare il processo di sottomissione questi documenti, fornendo un framework per implementare il template relativo a ciascuno di essi.

3.5 System Security Plan

Nel System Security Plan sono descritte le implementazioni dei controlli di sicurezza in relazione all'architettura del sistema del provider. Il sistema, infrastruttura, piattaforma o applicazione che sia, è in tal caso trattato come un insieme di componenti, ognuno dei quali deve essere documentato, utilizzando terminologie chiare, non ambigue, ed aderenti il più possibile alla nomenclatura comunemente utilizzata nell'ambito di interesse del componente stesso. In particolare, dovranno essere discussi gli aspetti di virtualizzazione e di conservazione dei dati, focalizzandosi sulla determinazione dei confini determinati dall'utilizzo delle varie tecnologie.

3.5.1 Virtualizzazione dei nodi di calcolo

L'ambito di virtualizzazione è gestito dalla sezione 9 del SSP. Bisogna chiarire:

- quali componenti fanno parte del sistema fisico

- quali componenti e quali funzionalità sono parte del sistema virtualizzato o astratto

Questa suddivisione si rispecchia immediatamente nella fase di categorizzazione degli *asset*. Bisogna infatti suddividere gli eventuali sistemi in:

- sistemi standard, installati sugli host
- sistemi virtualizzati, ospiti di un *hypervisor*
- sistemi che virtualizzano, ovvero gli *hypervisor*, per cui bisogna specificare se la virtualizzazione avviene in modalità:
  - bare-metal (in cui la componente hardware è gestita direttamente dal sistema virtuale), anche detta virtualizzazione di tipo 1
  - host-based (ovvero confinata su un server, che gestisce la parte hardware), nota come virtualizzazione di tipo 2

Per i provider *IaaS* è necessario anche specificare le modalità di installazione dei sistemi virtuali. Infatti, in caso di infrastrutture cloud *full-managed*, è il cloud service provider che installa e configura i sistemi operativi, garantendo poi l'accesso al cliente (agenzia governativa); al contrario, in infrastrutture *self-managed*, è il cliente che, tramite una dashboard, effettua autonomamente il *deploy* del sistema virtuale. A questo punto bisogna distinguere ulteriori casistiche:

- Il fornitore di servizi mette a disposizione delle immagini di base, con software preinstallato
- Il cliente installa autonomamente il sistema operativo, caricando un'immagine di base, o l'immagine di un sistema pre-esistente, sull'infrastruttura del provider

Inoltre occorre specificare eventuali meccanismi di controllo degli accessi per la gestione delle risorse, l'eventuale modalità di gestione della memoria condivisa, e le tecnologie implementate per la resilienza dell'infrastruttura.

3.5.2 Virtualizzazione della rete

Grazie alle tecnologie di *software-defined networking* è possibile effettuare anche la virtualizzazione dello stack e dei componenti di rete, come switch e router. Questi eventualmente possono essere integrati con appliance fisiche che supportino protocolli SDN (*OpenFlow, FabricPath*); è necessario perciò specificare:

- quali componenti di rete siano virtualizzati
- quali invece siano apparati fisici

L'eventuale adozione di meccanismi di segregazione, come ad esempio le VLAN per il partizionamento del livello 2 dello Stack ISO/OSI, le VLAN estese, gli switch virtuali distribuiti, i gateway di sicurezza virtuali, introduce ulteriori parametri da valutare e da specificare nel System Security Plan, in particolare per

la determinazione dei confini (approfondita nella sezione 3.5.3). Innanzitutto è necessario fornire un diagramma che illustri dettagliatamente la direzione del flusso dei dati sulla rete, indipendentemente da come la topologia della stessa sia strutturata, ed evidenziando gli eventuali componenti critici della topologia che determinano il flusso stesso.

3.5.3 Determinazione dei confini e controlli di sicurezza relativi

Per determinare i confini, occorre specificare in modo chiaro ed articolato dove il layer costituito dal servizio cloud inizia e dove finisce. Ciò contribuisce alla risoluzione delle problematiche relative alla *shared responsability*: se un servizio *SaaS* che vuole essere autorizzato a FedRAMP utilizza un servizio *PaaS*, è necessario effettuare l'assessment e l'autorizzazione anche del servizio *PaaS*. Analogamente, nel caso di una *PaaS* ospitata su una *IaaS*, è importante specificare il livello a cui sono implementati i requisiti di sicurezza desiderati e gestire l'assessment in modo opportuno.

Alcune domande, relative perlopiù agli aspetti di rete e di storage, consigliate dal documento Guide to Understanding FedRAMP per la determinazione dei confini sono:

- Viene effettuato isolamento al livello fisico, mediante l'utilizzo di interfacce di rete dedicate?
- Viene effettuata segregazione a livello 2 dello stack ISO/OSI?
- Sono implementate delle VLAN? Qual'è la definizione di tenant utilizzata?
- Eventuali VLAN rispecchiano la separazione dei tenant, oppure tenant diversi possono avere accesso alla stessa VLAN?
- Viene effettuato del monitoraggio per prevenire il VLAN-hopping?
- Viene effettuato bonding sulle interfacce di rete per migliorarne prestazioni e affidabilità?
- Sono presenti ACL per fornire isolamento tra i tenant?
- È implementato il protocollo IPSec per definire i confini tra reti di tenant diversi?
- Sono definiti dei confini a livello geografico sia per i dati in transito che per quelli memorizzati?
- È possibile, per i clienti, conoscere la locazione geografica dei propri dati?
- Il sistema utilizza tecnologie DAS[2], NAS[3], o SAN[4]?
- Se il sistema ha una SAN, è connessa tramite fibra ottica o iSCSI?

[2]Direct Attached Storage
[3]Network Attached Storage
[4]Storage Area Network

Un ulteriore fattore da considerare è determinato dalle funzionalità di migrazione diretta (*live migrations*) impiegate. Ciò riguarda principalmente i fornitori di servizi *IaaS* e *PaaS* che, per ragioni di prestazioni e ridondanza, possono spostare geograficamente le risorse cloud, come macchine virtuali e container. È fondamentale, infatti, che in tali casi i dati persistano all'interno del confine designato, sia che siano memorizzati su uno storage, sia che siano in transito su una rete: gli indirizzi IP dichiarati all'interno del confine devono rimanere tali, così come il traffico di rete non deve essere veicolato attraverso regioni geografiche non dichiarate. Occorre perciò specificare se le migrazioni dirette siano fatte in modo programmato ed automatizzato, oppure in modo manuale e, nel primo caso, dichiarare le regole utilizzate per gestirle.

3.6 Controlli di sicurezza per la conformità - NIST 800-53 e FedRAMP

3.6.1 Categorie dei controlli

I controlli di sicurezza di FedRAMP sono basati sul documento NIST 800-53. Alcuni, di carattere essenzialmente procedurale, sono stati introdotti da FedRAMP, per altri sono stati proposti miglioramenti. La catalogazione dei controlli è effettuata sulla base del livello di sensibilità (basso e moderato); essi sono inoltre suddivisi in famiglie, ciascuna delle quali è contrassegnata univocamente da un *ID*[45]. Ogni famiglia appartiene a una classe (Tecnico, Operativo, Management), che ne identifica l'ontologia. Nella tabella 3.1, è proposto un conteggio dei controlli di sicurezza in ogni famiglia, per le *baseline* relative ai livelli di sensibilità basso e moderato.

ID	Famiglia	Classe	Livello Basso	Livello moderato
AC	Controllo degli accessi	Tecnico	11	43
AT	Awareness & training	Operativo	4	5
AU	Audit and accountability	Tecnico	10	19
CA	Certification, Accdeditation & Security Assessment	Management	8	15
CM	Configuration Management	Operativo	8	26
CP	Contingency Planning	Operativo	6	24
IA	Identification and authentication	Tecnico	15	27
IR	Incident response	Operativo	7	18
MA	Maintenance	Operativo	4	11
MP	Media protection	Operativo	4	10
PE	Physical and environmental protection	Operativo	10	20
PL	Planning	Management	3	6
PS	Personnel security	Operativo	8	9
RA	Risk assessment	Management	4	10
SA	System and services acquisition	Management	6	22
SC	System and communications protection	Tecnico	10	32
SI	System and information integrity	Operativo	7	28
TOT	-	-	**125**	**325**

Tabella 3.1: Famiglie di controlli[46][47]

3.7 FedRAMP in Amazon Web Services e Azure

Amazon e *Microsoft* sono due esemi di fornitori di servizi aver seguito il programma di autorizzazione FedRAMP, soddisfacendo i controlli di sicurezza previsti

tramite i modelli illustrati in questo capitolo.

Il servizio AWS che garantisce la compliance FedRAMP prende il nome di *GovCloud*, ed ha ricevuto un'autorizzazione P-ATO e diverse ATO per il livello di sensibilità più elevato. Inoltre anche altri servizi AWS, appartenenti alle regioni *Stati Uniti occidentali* e *Stati Uniti orientali* sono risultati conformi al programma FedRAMP, ottenendo autorizzazioni ATO per il livello di sensibilità *moderato*.

Per quanto riguarda Microsoft invece, è il servizio *Azure* (e Azure per enti pubblici) ad aver ricevuto una P-ATO per il livello di sensibilità *moderato*. Inoltre, il servizio *Microsoft Dynamics CRM Online per enti pubblici* ha ricevuto una ATO dall'HUD mentre Microsoft Office 365 per il Governo degli Stati Uniti ha ricevuto una ATO dal DHHS (Dipartimento della Salute e dei Servizi Umani).

Capitolo 4

Implementazione dei controlli di sicurezza FedRAMP in Moon Cloud

4.1 Introduzione

In questo capitolo verrà effettuata un'analisi dei controlli di sicurezza elencati nel capitolo precedente, classificandoli in *controlli automatici* e *controlli procedurali*. Dopodiché verra offerta una possibile implementazione per ciascuna delle due tipologie di controlli, i quali verranno integrati in Moon Cloud. Per i controlli automatici sarà utilizzato OpenSCAP[1], uno strumento per l'auditing realizzato da Red Hat e certificato dal NIST. I controlli procedurali invece, eseguono l'*processi di business* e vanno ad indirizzare tutte quelle proprietà di carattere puramente qualitativo per cui è fondamentale l'interazione umana. Questi saranno implementati con un *driver Moon Cloud ad interazione umana*, che somministra un questionario online ad un target.

4.2 Analisi dei controlli di sicurezza

Verranno ora proposte alcune tabelle di riepilogo dei controlli di sicurezza di FedRAMP, suddivisi per famiglia, dei quali viene indicata la *baseline* di riferimento e la tipologia (*A*, automatizzabile / *P* procedurale (interazione umana) / *A/P* composizione di approccio automatico e manuale); i controlli contrassegnati in grassetto sono di primo livello, quelli invece presentati con stile normale, sono specializzazioni.

I controlli di sicurezza, essendo proposti in modo astratto così da poter coprire il più vasto numero di scenari, vanno poi comunque studiati e implementati sulla base delle caratteristiche e del contesto del sistema target.

4.2.1 Access Control

ID	Nome	Baseline	Tipo
AC-1	access control policy and procedures	Basso	P

[1] https://www.openscap.org

ID	Nome	Baseline	Tipo
AC-2	account management	Basso	A/P
AC-2 (1)	automated system account management	Moderato	A/P
AC-2 (2)	removal of temporary / emergency accounts	Moderato	A
AC-2 (3)	disable inactive accounts	Moderato	A/P
AC-2 (4)	automated audit actions	Moderato	A
AC-2 (5)	inactivity logout	Moderato	A
AC-2 (7)	role-based schemes	Moderato	A
AC-2 (9)	restrictions on use of shared groups / accounts	Moderato	A
AC-2 (10)	shared / group account credential termination	Moderato	A/P
AC-2 (12)	account monitoring / atypical usage	Moderato	A/P
AC-3	access enforcement	Basso	A/P
AC-4	information flow enforcement	Moderato	A/P
AC-4 (21)	physical / logical separation of information flows	Moderato	A/P
AC-5	separation of duties	Moderato	A/P
AC-6	least privilege	Moderato	A/P
AC-6 (1)	authorize access to security functions	Moderato	A
AC-6 (2)	non-privileged access for nonsecurity functions	Moderato	A
AC-6 (5)	privileged accounts	Moderato	A
AC-6 (9)	auditing use of privileged functions	Moderato	A
AC-6 (10)	prohibit non-privileged users from execution of privileged functions	Moderato	A
AC-7	unsuccessful logon attempts	Basso	A
AC-8	system use notification	Basso	A
AC-10	concurrent session control	Moderato	A
AC-11	session lock	Moderato	A
AC-11 (1)	pattern-hiding displays	Moderato	A
AC-12	session termination	Moderato	A
AC-14	"permitted actions without identification or authentication"	Basso	A/P
AC-17	remote access	Basso	A/P
AC-17 (1)	automated monitoring / control	Moderato	A
AC-17 (2)	protection of confidentiality / integrity using encryption	Moderato	A/P
AC-17 (3)	managed access control points	Moderato	A
AC-17 (4)	privileged commands / access	Moderato	A/P
AC-17 (9)	disconnect / disable access	Moderato	A/P
AC-18	wireless access	Basso	A/P
AC-18 (1)	authentication and encryption	Moderato	A/P
AC-19	access control for mobile devices	Basso	A
AC-19 (5)	full device / container-based encryption	Moderato	A

ID	Nome	Baseline	Tipo
AC-20	use of external information systems	Basso	A
AC-20 (1)	limits on authorized use	Moderato	A
AC-20 (2)	portable storage devices	Moderato	A
AC-21	information sharing	Moderato	A/P
AC-22	publicly accessible content	Basso	A/P

La classe *AC* include tutti quei controlli di sicurezza aventi obiettivo la verifica della corretta implementazione delle politiche di *controllo degli accessi*. Essendo questa categoria di carattere tecnico, la totalità dei controlli proposti è facilmente automatizzabile: solo per *AC-1*, che definisce l'aspetto procedurale, abbiamo la necessità di richiedere un'interazione umana. La componente procedurale emerge, a complemento dell'approccio automatico, in 19 casi su 43 (44%): è il caso ad esempio dei controlli di gestione dell'accounting (*AC-2 e controlli complementari*, attività solitamente integrata nei processi di business e pertanto condotta generalmente in modo manuale ma, che tramite opportune tecniche di *software-integration* può essere monitorata anche in maniera automatica.

4.2.2 Awareness & training

ID	Nome	Baseline	Tipo
AT-1	security awareness and training policy and procedures	Basso	P
AT-2	security awareness training	Basso	P
AT-2 (2)	insider threat	Moderato	P
AT-3	role-based security training	Basso	P
AT-4	security training records	Basso	P

I controlli della famiglia *awareness and training* sono soltanto 5, e per ciascuno di essi è richiesta intrinsecamente l'interazione umana. Questa, infatti, misura il grado di consapevolezza dell'utente rispetto alle politiche e alle procedure di sicurezza.

L'approccio ibrido può essere utilizzato qualora si voglia adottare un sistema automatico per la valutazione delle conoscenze dell'utente oppure l'individuazione di minacce provenienti dall'esterno.

4.2.3 Audit and accountability

ID	Nome	Baseline	Tipo
AU-1	"audit and accountability policy and procedures"	Basso	P
AU-2	audit events	Basso	P
AU-2 (3)	reviews and updates	Medio	P
AU-3	content of audit records	Basso	A
AU-3 (1)	additional audit information	Medio	P

ID	Nome	Baseline	Tipo
AU-4	audit storage capacity	Basso	A
AU-5	response to audit processing failures	Basso	A
AU-6	"audit review, analysis, and reporting"	Basso	P
AU-6 (1)	"process integration"	Medio	P
AU-6 (3)	"correlate audit repositories"	Medio	P
AU-7	audit reduction and report generation	Medio	A
AU-7 (1)	automatic processing	Medio	A
AU-8	time stamps	Basso	A
AU-8 (1)	synchronization with authoritative time source	Medio	A
AU-9	protection of audit information	Basso	A
AU-9 (2)	audit backup on separate physical systems / components	Medio	A
AU-9 (4)	access by subset of privileged users	Medio	A/P
AU-11	audit record retention	Basso	A
AU-12	audit generation	Basso	A

Dei 19 controlli sull'*auditing*, 11 possono essere effettuati in maniera completamente automatica, 1 richiede un approccio ibrido e 7 richiedono l'interazione umana. Per cui si può affermare che nel 63% dei casi, è adottabile un approccio automatico.

4.2.4 Certification, Accreditation & Security Assessment

ID	Nome	Baseline	Tipo
CA-1	"security assessment and authorization policy and procedures"	Basso	P
CA-2	security assessments	Basso	P
CA-2 (1)	independent assessors	Basso	P
CA-2 (2)	specialized assessments	Moderato	P
CA-2 (3)	external organizations	Moderato	P
CA-3	system interconnections	Basso	P
CA-3 (3)	unclassified non-national security system connections	Moderato	P
CA-3 (5)	restrictions on external system connections	Moderato	P
CA-5	plan of action and milestones	Basso	P
CA-6	security authorization	Basso	P
CA-7	continuous monitoring	Basso	P
CA-7 (1)	independent assessment	Moderato	P
CA-8	penetration testing	Moderato	P
CA-8 (1)	independent penetration agent or team	Moderato	P
CA-9	internal system connections	Basso	P

I controlli di questa classe sono tutti di tipo procedurale, e non possono essere automatizzati: si tratta infatti di una serie di dichiarazioni che il responsabile

della sicurezza IT del provider deve compilare.

4.2.5 Configuration Management

ID	Nome	Baseline	Tipo
CM-1	"configuration management policy and procedures"	Basso	P
CM-2	baseline configuration	Basso	P
CM-2 (1)	previews and updates	Moderato	P
CM-2 (2)	automation support for accuracy / currency	Moderato	P
CM-2 (3)	retention of previous configurations	Moderato	P
CM-2 (7)	configure systems, components, or devices for high-risk areas	Moderato	P
CM-3	configuration change control	Moderato	P
CM-4	security impact analysis	Basso	P
CM-5	access restrictions for change	Moderato	A/P
CM-5 (1)	automated access enforcement / auditing	Moderato	A
CM-5 (3)	signed components	Moderato	A
CM-5 (5)	"access restrictions for change | limit production / operational privileges"	Moderato	A
CM-6	configuration settings	Basso	A/P
CM-6 (1)	automated central management / application / verification	Moderato	P
CM-7	least functionality	Basso	A/P
CM-7 (1)	periodic review	Moderato	P
CM-7 (2)	prevent program execution	Moderato	A
CM-7 (5)	authorized software / whitelisting	Moderato	A
CM-8	information system component inventory	Basso	A/P
CM-8 (1)	updates during installations / removals	Moderato	A/P
CM-8 (3)	automated unauthorized component detection	Moderato	A
CM-8 (5)	no duplicate accounting of components	Moderato	A
CM-9	configuration management plan	Moderato	P
CM-10	software usage restrictions	Basso	A/P
CM-10 (1)	open source software	Moderato	P
CM-11	user-installed software	Basso	A/P

I controlli appartenenti a questa famiglia rientrano nella tipologia "controllo operativo". Molti di questi sono quindi controlli essenzialmente procedurali, in quanto conssistono nel verificare l'esistenza e la conformità delle policy per la gestione dei cambiamenti. Gran parte delle conseguenze di queste policy, però, contengono elementi di carattere tecnico; per questa ragione, in alcuni casi, l'esecuzione degli stessi può avvenire in modo automatico o semi-automatico. In particolare i meccanismi automatici possono essere utilizzati in 14 casi su 26, garanten-

do quindi una copertura del 53%. Di questi 14 controlli effettuabili in maniera automatica, la metà devono però essere eseguiti con un approccio ibrido.

4.2.6 Contingency Planning

ID	Nome	Baseline	Tipo
CP-1	"contingency planning policy and procedures"	Basso	P
CP-2	contingency plan	Basso	P
CP-2 (1)	coordinate with related plans	Moderato	P
CP-2 (2)	capacity planning	Moderato	P
CP-2 (3)	resume essential missions / business functions	Moderato	P
CP-2 (8)	identify critical assets	Moderato	P
CP-3	contingency training	Basso	P
CP-4	contingency plan testing	Basso	P
CP-4 (1)	coordinate with related plans	Moderato	P
CP-6	alternate storage site	Moderato	A/P
CP-6 (1)	separation from primary site	Moderato	P
CP-6 (3)	accessibility	Moderato	P
CP-7	alternate processing site	Moderato	P
CP-7 (1)	separation from primary site	Moderato	P
CP-7 (2)	accessibility	Moderato	P
CP-7 (3)	priority of service	Moderato	P
CP-8	telecommunications services	Moderato	P
CP-8 (1)	priority of service provisions	Moderato	P
CP-8 (2)	single points of failure	Moderato	P
CP-9	information system backup	Basso	A/P
CP-9 (1)	testing for reliability / integrity	Moderato	A
CP-9 (3)	separate storage for critical information	Moderato	A/P
CP-10	information system recovery and reconstitution	Basso	P
CP-10 (2)	transaction recovery	Moderato	A/P

La realizzazione del piano di contingenza è di carattere prettamente procedurale per definizione; l'obiettivo è infatti quello di studiare gli impatti sul business di possibili incidenti informatici, pianificare le operazioni di *incident response*, un piano per il recupero dall'incidente (*disastery recovery*) e le eventuali misure prese per garantire la *business continuity*.

Proprio le ultime citate sono l'oggetto dei pochi controlli parzialmente automatizzabili: nel caso del *CP-6*, ad esempio, che prevede l'esistenza di una locazione alternativa per lo *storage* dei dati, si può verificare che entrambe le locazioni siano sempre sincronizzate e che le proprietà di confidenzialità e integrità nella ridondanza geografica siano rispettate.

La stessa considerazione può essere fatta per i sistemi di backup dei dati (CP-9) e dei log delle transazioni (CP-10), tenendo anche conto del fatto che le in-

formazioni critiche devono essere trattate separatamente (CP-9 (3)). Eventuali sistemi automatici possono essere utilizzati anche per la verifica dell'affidabilità, l'integrità, il testing (e la effettiva possibilità di recupero dati).

L'approccio automatico può essere usato nel 16% dei casi.

4.2.7 Identification and Authentication

ID	Nome	Baseline	Tipo
IA-1	"identification and authentication policy and procedures"	Basso	P
IA-2	"identification and authentication (organizational users)"	Basso	P
IA-2 (1)	network access to privileged accounts	Basso	A
IA-2 (2)	network access to non-privileged accounts	Moderato	A
IA-2 (3)	local access to privileged accounts	Moderato	A
IA-2 (5)	"identification and authentication (organizational users) | group authentication"	Moderato	A
IA-2 (8)	network access to privileged accounts - replay resistant	Moderato	A
IA-2 (11)	remote access - separate device	Moderato	A
IA-2 (12)	acceptance of piv credentials	Basso	A
IA-3	device identification and authentication	Moderato	A
IA-4	identifier management	Basso	P
IA-4 (4)	identify user status	Moderato	P
IA-5	authenticator management	Basso	A/P
IA-5 (1)	password-based authentication	Basso	A
IA-5 (2)	pki-based authentication	Moderato	A
IA-5 (3)	in-person or trusted third-party registration	Moderato	A
IA-5 (4)	automated support for password strength determination	Moderato	A
IA-5 (6)	protection of authenticators	Moderato	A
IA-5 (7)	no embedded unencrypted static authenticators	Moderato	A
IA-5 (11)	hardware token-based authentication	Basso	A
IA-6	authenticator feedback	Basso	A
IA-7	cryptographic module authentication	Basso	A
IA-8	identification and authentication (non- organizational users)	Basso	A
IA-8 (1)	acceptance of piv credentials from other agencies	Basso	A
IA-8 (2)	acceptance of third-party credentials	Basso	A
IA-8 (3)	use of ficam-approved products	Basso	A
IA-8 (4)	use of ficam-issued profiles	Basso	A

I controlli della famiglia di *identificazione e autenticazione* sono perlopiù di carattere tecnico e pertanto in gran parte automatizzabili (nell'85% dei casi). Questi hanno una stretta correlazione con i controlli della famiglia *controllo degli accessi* e di *auditing*, già trattate, e manifestano la necessità per il provider di mantenere *accountability* e *non-repudiation*. Pertanto si tratta di controlli effettuati sulla resistenza delle credenziali agli attacchi, sulla sicurezza del processo di autenticazione e sulla possibilità di ricondurre con esattezza tutte le operazioni svolte sul sistema all'attore che le ha compiute, sia esso un servizio automatico o un utente umano. Molti di questi, tuttavia, sono anche di carattere ibrido o procedurale, poiché basati sulle dichiarazioni del provider stesso.

4.2.8 Incident response

ID	Nome	Baseline	Tipo
IR-1	incident response policy and procedures	Basso	P
IR-2	incident response training	Basso	P
IR-3	incident response testing	Moderato	P
IR-3 (2)	coordination with related plans	Moderato	P
IR-4	incident handling	Basso	P
IR-4 (1)	automated incident handling processes	Moderato	P
IR-5	incident monitoring	Basso	P
IR-6	incident reporting	Basso	P
IR-6 (1)	automated reporting	Moderato	P
IR-7	incident response assistance	Basso	P
IR-7 (1)	automation support for availability of information / support	Moderato	P
IR-7 (2)	coordination with external providers	Moderato	P
IR-8	incident response plan	Basso	P
IR-9	information spillage response	Moderato	P
IR-9 (1)	responsible personnel	Moderato	P
IR-9 (2)	training	Moderato	P
IR-9 (3)	post-spill operations	Moderato	P
IR-9 (4)	exposure to unauthorized personnel	Moderato	P

Nel caso dell'*incident response*, le attività sono essenzialmente procedurali, per definizione. La componente automatica può essere aggiunta in alcuni casi come misura complementare, ad esempio nel caso di *IR-4* (meccanismi di gestione degli incidenti automatici), *IR-5* (esistenza di meccanismi efficaci per il monitoraggio degli incidenti), *IR-6* (meccanismi di reporting automatico) e *IR-9* (fuoriuscita di informazioni per esposizione delle stesse a personale non autorizzato). Per soddisfare*IR-4*, ad esempio, si può controllare la presenza e la corretta configurazione di meccanismi di protezione istantanei (ad esempio reazioni automatiche del firewall in relazione ad eventuali pattern di attacco) Nel caso di *IR-5* possono essere effettuate misurazioni sulla presenza e la corretta configurazione di meccanismi IDS e IPS, unitamente alla frequenza degli aggiornamenti delle definizioni.

4.2.9 Maintenance

ID	Nome	Baseline	Tipo
MA-1	system maintenance policy and procedures	Basso	P
MA-2	controlled maintenance	Basso	P
MA-3	maintenance tools	Moderato	A/P
MA-3 (1)	inspect tools	Moderato	A
MA-3 (2)	inspect media	Moderato	A
MA-3 (3)	prevent unauthorized removal	Moderato	A
MA-4	nonlocal maintenance	Basso	P
MA-4 (2)	document nonlocal maintenance	Moderato	P
MA-5	maintenance personnel	Basso	P
MA-5 (1)	individuals without appropriate access	Moderato	P
MA-6	timely maintenance	Moderato	A/P

Anche in questo caso ci troviamo in presenza di controlli di carattere perlopiù procedurale, nonostante l'approccio automatico possa essere utilizzato per garantire la correttezza delle operazioni svolte (ad esempio in *MA-3(1)*, *MA-3(2)* e *MA-3(3)*)

4.2.10 Media protection

ID	Nome	Baseline	Tipo
MP-1	media protection policy and procedures	Basso	P
MP-2	media access	Basso	P
MP-3	media marking	Moderato	P
MP-4	media storage	Moderato	P
MP-5	media transport	Moderato	A/P
MP-5 (4)	cryptographic protection	Moderato	A/P
MP-6	media sanitization	Basso	P
MP-6 (2)	equipment testing	Moderato	P
MP-7	media use	Basso	A/P
MP-7 (1)	prohibit use without owner	Moderato	A/P

Questa categoria di controlli riguarda perlopiù processi di business nei quali è implicato l'utilizzo di dispositivi multimediali per il trasferimento delle informazioni. Si tratta perciò di controlli che devono essere verificati con interazione umana, anche se possono essere effettuate alcune verifiche in modo automatico, come nel caso della proprietà *MP-5* che verifica l'utilizzo della crittografia nel trasporto dei dati effettuato con dispositivi multimediali (CD, DVD, Pendrive).

4.2.11 Physical and environmental protection

ID	Nome	Baseline	Tipo
PE-1	"physical and environmental protection policy and procedures"	Basso	A/P
PE-2	physical access authorizations	Basso	P
PE-3	physical access control	Basso	A/P
PE-4	access control for transmission medium	Moderato	A/P
PE-5	access control for output devices	Moderato	A/P
PE-6	monitoring physical access	Basso	A/P
PE-6 (1)	intrusion alarms / surveillance equipment	Moderato	A/P
PE-8	visitor access records	Basso	A/P
PE-9	power equipment and cabling	Moderato	A/P
PE-10	emergency shutoff	Moderato	A/P
PE-11	emergency power	Moderato	A/P
PE-12	emergency lighting	Basso	A/P
PE-13	fire protection	Basso	A/P
PE-13 (2)	suppression devices / systems	Moderato	A/P
PE-13 (3)	automatic fire suppression	Moderato	A/P
PE-14	temperature and humidity controls	Basso	A/P
PE-14 (2)	monitoring with alarms / notifications	Moderato	A/P
PE-15	water damage protection	Basso	A/P
PE-16	delivery and removal	Basso	A/P
PE-17	alternate work site	Moderato	A/P

Questa categoria di controlli riguarda la sicurezza dell'ambiente fisico nel quale operano i sistemi del fornitore di servizi. Si tratta di aspetti in gran parte controllabili tramite metodologie automatiche e manuali: l'eventuale presenza di certificazioni per gli impianti con controlli a cadenza periodica può già essere un'ottima metrica di valutazione; eventuali meccanismi di monitoraggio automatico possono essere adottati mediante l'integrazione con eventuali dispositivi e sonde IoT.

4.2.12 Planning

ID	Nome	Baseline	Tipo
PL-1	security planning policy and procedures	Basso	P
PL-2	system security plan	Basso	P
PL-2 (3)	plan / coordinate with other organizational entities	Moderato	P
PL-4	rules of behavior	Basso	P
PL-4 (1)	social media and networking restrictions	Moderato	P
PL-8	information security architecture	Moderato	P

I controlli appartenenti a questa categoria riguardano la redazione del *system security plan* già trattato nel capitolo precedente. Si tratta, ancora una volta, di una serie di informazioni che il responsabile della sicurezza IT deve fornire.

4.2.13 Personnel security

ID	Nome	Baseline	Tipo
PS-1	personnel security policy and procedures	Basso	P
PS-2	position risk designation	Basso	P
PS-3	personnel screening	Basso	P
PS-3 (3)	information with special protection measures	Moderato	P
PS-4	personnel termination	Basso	P
PS-5	personnel transfer	Basso	P
PS-6	access agreements	Basso	P
PS-7	third-party personnel security	Basso	P
PS-8	personnel sanctions	Basso	P

Questa classe di controlli è riferita alla sicurezza e al controllo del comportamento del personale IT. Si tratta di controlli di carattere procedurale. Le informazioni relativa ai controlli di *Personnel Security* possono essere rilasciate dal responsabile della sicurezza interno al provider e possono essere eventualmente comprovate mediante la somministrazione periodica di questionari al personale stesso.

4.2.14 Risk assessment

ID	Nome	Baseline	Tipo
RA-1	risk assessment policy and procedures	Basso	P
RA-2	security categorization	Basso	P
RA-3	risk assessment	Basso	P
RA-5	vulnerability scanning	Basso	A/P
RA-5 (1)	update tool capability	Moderato	A
RA-5 (2)	update by frequency / prior to new scan / when identified	Moderato	A
RA-5 (3)	breadth / depth of coverage	Moderato	A/P
RA-5 (5)	privileged access	Moderato	A
RA-5 (6)	automated trend analyses	Moderato	A
RA-5 (8)	review historic audit logs	Moderato	P

Il processo di analisi del rischio è per definizione procedurale. Tuttavia, in ambito IT, è spesso supportato da strumenti automatici e modelli per la raccolta di informazioni utili a supporto dell'analisi. Molte funzionalità di *risk analysis* possono essere quindi automatizzate: tra queste la gestione e gli aggiornamenti di eventuali definizioni dei *tool* utilizzati e il *vulnerability scanning*. Per individuare le vulnerabilità possiamo considerare due approcci:

- **Vulnerability scan statico**, che analizza le vulnerabilità sulla base della versione dei prodotti installati, confrontando i numeri di rilascio con le vulnerabilità note.
- **Vulnerability scan dinamico**, che effettua una vera e propria scansione verso il sistema *target*, in modo più invasivo.

Il metodo automatico, in questo caso, può essere applicato nel 60% dei casi.

4.2.15 System and services acquisition

ID	Nome	Baseline	Tipo
SA-1	"system and services acquisition policy and procedures"	Basso	P
SA-2	allocation of resources	Basso	P
SA-3	system development life cycle	Basso	P
SA-4	acquisition process	Basso	P
SA-4 (1)	functional properties of security controls	Moderato	P
SA-4 (2)	design / implementation information for security controls	Moderato	P
SA-4 (8)	continuous monitoring plan	Moderato	P
SA-4 (9)	functions / ports / protocols / services in use	Moderato	P
SA-4 (10)	use of approved piv products	Moderato	P
SA-5	information system documentation	Basso	P
SA-8	security engineering principles	Moderato	P
SA-9	external information system services	Basso	P
SA-9 (1)	"risk assessments / organizational approvals	Moderato	P
SA-9 (2)	identification of functions / ports / protocols / services	Moderato	P
SA-9 (4)	consistent interests of consumers and providers	Moderato	P
SA-9 (5)	processing, storage, and service location"	Moderato	P
SA-10	developer configuration management	Moderato	P
SA-10 (1)	software / firmware integrity verification	Moderato	A
SA-11	developer security testing and evaluation	Moderato	P
SA-11 (1)	static code analysis	Moderato	A
SA-11 (2)	threat and vulnerability analyses	Moderato	A
SA-11 (8)	dynamic code analysis	Moderato	A

Questa classe è relativa al processo di acquisizione del software da terze parti, e contiene perlopiù controllo di sicurezza di tipo procedurale. Tra questi, alcune attività possono però essere automatizzate, parzialmente o totalmente, mediante l'utilizzo di strumenti pilotabili. Tra queste possiamo riconoscere il controllo della configurazione dello sviluppatore, con la verifica dell'integrità degli strumenti

software utilizzati, e tutta la fase di testing del software, comprendente anche analisi statica e dinamica.

4.2.16 System and communication protection

ID	Nome	Baseline	Tipo
SC-1	"system and communications protection policy and procedures"	Basso	P
SC-2	application partitioning	Moderato	A
SC-4	information in shared resources	Moderato	A
SC-5	denial of service protection	Basso	A
SC-6	resource availability	Moderato	A
SC-7	boundary protection	Basso	A
SC-7 (3)	access points	Moderato	A
SC-7 (4)	external telecommunications services	Moderato	A
SC-7 (5)	deny by default / allow by exception	Moderato	A
SC-7 (7)	prevent split tunneling for remote devices	Moderato	A
SC-7 (8)	route traffic to authenticated proxy servers	Moderato	A
SC-7 (12)	host-based protection	Moderato	A
SC-7 (13)	isolation of security tools / mechanisms / support components"	Moderato	A
SC-7 (18)	fail secure	Moderato	A
SC-8	transmission confidentiality and integrity	Moderato	A
SC-8 (1)	cryptographic or alternate physical protection	Moderato	A
SC-10	network disconnect	Moderato	A
SC-12	cryptographic key establishment and management"	Basso	A
SC-12 (2)	symmetric keys	Moderato	A
SC-12 (3)	asymmetric keys	Moderato	A
SC-13	cryptographic protection	Basso	A
SC-15	collaborative computing devices	Basso	A
SC-17	public key infrastructure certificates	Moderato	A
SC-18	mobile code	Moderato	A
SC-19	voice over internet protocol	Moderato	A
SC-20	"secure name /address resolution service (authoritative source)"	Basso	A
SC-21	"secure name /address resolution service (recursive or caching resolver)"	Basso	A
SC-22	"architecture and provisioning for name/address resolution service"	Basso	A
SC-23	session authenticity	Moderato	A
SC-28	protection of information at rest	Moderato	A
SC-28 (1)	cryptographic protection	Moderato	A
SC-39	process isolation	Basso	A

I controlli di "System and communication protection policy and procedures" mirano a verificare l'applicazione delle politiche su sistemi e meccanismi di comunicazione. hanno tutti un immediato risvolto tecnico, per questa ragione sono totalmente automatizzabili, con l'eccezione di *SC-1* che ne definisce la parte procedurale.

4.2.17 System and information integrity

ID	Nome	Baseline	Tipo
SI-1	system and information integrity policy and procedures	Basso	P
SI-2	flaw remediation	Basso	A/P
SI-2 (2)	automated flaw remediation status	Moderato	A/P
SI-2 (3)	time to remediate flaws / benchmarks for corrective actions	Moderato	A/P
SI-3	malicious code protection	Basso	A
SI-3 (1)	central management	Moderato	A
SI-3 (2)	automatic updates	Moderato	A
SI-3 (7)	nonsignature-based detection	Moderato	A
SI-4	information system monitoring	Basso	A
SI-4 (14)	wireless intrusion detection	Moderato	A
SI-4 (16)	correlate monitoring information	Moderato	A
SI-4 (1)	system-wide intrusion detection system	Moderato	A
SI-4 (23)	host-based devices	Moderato	A
SI-4 (2)	automated tools for real-time analysis	Moderato	A
SI-4 (4)	inbound and outbound communications traffic	Moderato	A
SI-4 (5)	system-generated alerts	Moderato	A
SI-5	security alerts, advisories, and directives	Basso	A
SI-6	security function verification	Moderato	A
SI-7	software, firmware, and information integrity	Moderato	A
SI-7 (1)	integrity checks	Moderato	A
SI-7 (7)	integration of detection and response	Moderato	A
SI-8	spam protection	Moderato	A
SI-8 (1)	central management	Moderato	A
SI-8 (2)	automatic updates	Moderato	A
SI-10	information input validation	Moderato	A
SI-11	error handling	Moderato	A
SI-12	information handling and retention	Basso	A
SI-16	memory protection	Basso	A

I controlli appartenenti a questa classe mirano a verificare la corretta funzionalità dei meccanismi per la preservazione dell'integrità dei sistemi e delle informazioni. Sono perlopiù automatizzabili, tuttavia potrebbe essere necessaria un'intera-

zione umana per l'esecuzione dei controlli *SI-2*, *SI-2(2)* e *SI-2(3)*, riguardanti le tempistiche di risoluzione di problematiche di sicurezza.

4.2.18 Conclusioni della fase di analisi

Dall'analisi effettuata si evince che dei 325 controlli delle *baseline* bassa e moderata, 130 sono completamente automatizzabili (40%), 133 richiedono interazione umana (41%) e 62 richiedono un approccio misto tra automazione e interazione umana (19%). Molti di questi controlli, inoltre, sono relativi ad attività di monitoraggio continuativo, pertanto possono essere soddisfatti con la semplice adozione di *Moon Cloud* o altre soluzioni di monitoraggio. Si andrà ora a definire due metodologie per la copertura di tutti quei controlli di carattere procedurale, tecnico ed operativo. La prima metodologia consiste nella gestione dei controlli automatizzabili, mediante l'integrazione di Moon Cloud con il protocollo SCAP; la seconda, invece, prevede la somministrazione di questionari agli attori coinvolti nei controlli di tipo procedurale ad interazione umana.

4.3 Implementazione dei controlli automatici - SCAP

Per implementare i controlli automatizzabili di FedRAMP in Moon Cloud, è stato creato un driver con il supporto al protocollo *SCAP* (Security Content Automation Protocol). *SCAP* è una *suite* composta da sei specifiche il cui obiettivo è standardizzare il formato e la nomenclatura con cui i prodotti di sicurezza rappresentano le informazioni relative alle configurazioni e alle vulnerabilità dei software noti. SCAP utilizza alcuni documenti e dataset di riferimento (es. *NVD, National Vulnerability Database*), forniti e mantenuti dal NIST e dal DHS. Le finalità di SCAP:

- Massimizzare l'interoperabilità tra strumenti di tipologia diversa
- Facilitare l'integrazione tra soluzioni di produttori differenti
- Favorire lo sviluppo collaborativo dei documenti e dei dataset di riferimento

I documenti utilizzati sono di tipo *XML*[2], in modo da risultare facilmente leggibili da umani ed eventualmente eseguibili da software automatici. A questi possono poi essere applicati dei fogli di trasformazione [3] per la trasposizione dei contenuti significativi in altri formati, permettendo sia di creare dei report, sia di adattare gli stessi ad altri framework.

I componenti di *SCAP* possono essere divisi nelle seguenti categorie:

- Linguaggi (XCCDF[4], OVAL[5], OCIL[6])

[2] eXtensible Markup Language
[3] XSL(T)
[4] eXtensible Configuration Checklist Description Format
[5] Open Vulnerability and Assessment Language
[6] Open Checklist Interactive Language

- Enumerazioni (CPE[7], CCE[8], CVE[9])
- Sistemi di misurazione e *scoring* (CVSS[10], CCSS[11])
- Sistemi di *trustworthiness* (TMSAD[12])

Questi componenti sono definiti in modo separato, ma possono essere eventualmente collegati in un'unica *datastream collection*, come indicato nel documento NIST 800-126, eventualmente firmata tramite *XML Signature* per garantire integrità e autenticità.

4.3.1 SCAP: i linguaggi

Di seguito saranno dettagliate le caratteristiche dei linguaggi del protocollo SCAP: *XCCDF*, *OVAL* e *OCIL*.

XCCDF

L'obiettivo dell'*eXtensible Configuration Checklist Description Format* è quello di definire uno standard per la rappresentazione di regole di sicurezza, e la descrizione dei casi in cui queste devono essere applicate. A questo fine, *XCCDF* fornisce la possibilità di descrivere in maniera *human-readable*, assegnando un titolo, una descrizione e un identificativo.

Il processo di compliance implementato in XCCDF è basato su tre componenti principali: una *policy*, descritta in prosa, che descrive come i sistemi devono esesre configurati; un *assessment*, per determinare la compliance di un sistema alla *policy* e una fase di *remediation*, per rendere i sistemi compliant.

Il documento XCCDF è quindi un *benchmark* nel quale vengono definite delle regole (*recommendations*) e dei valori, che possono essere eventualmente raggruppati e organizzati secondo un'alberatura.

```
1  <Benchmark id="Linux">
2      <title> Guidance for Securing Linux</title>
3      <platform idref="cpe:/o:generic:linux"/>
4      <Profile id="profilo1">...</Profile>
5      <Group id="parte1">
6          <Group id="PasswordPolicy">
7                  <Value> ... </Value>
8                  <Rule> ... </Rule>
9          </Group>
10         <Group id="AuditPolicy">
11             <Rule> ... </Rule>
12         </Group>
13     </Group>
14     <Group id="parte2">
15         ...
```

[7] Common Platform Enumeration, *http://cpe.mitre.org*
[8] Common Configuration Enumeration *http://cce.mitre.org*
[9] Common Vulnerability Exposure *http://cve.mitre.org*
[10] Common Vulnerability Scoring System *https://nvd.nist.gov/vuln-metrics/cvss*
[11] Common Configuration Scoring System
[12] Trust Model for Security Automation Data

```
16      </Group>
17  </Benchmark>
```

Ogni *benchmark* ha un titolo (`<title/>`) ed è riferito a una piattaforma (`<platform />`). Possono essere poi definiti vari profili (`<profile/>`) che permettono di selezionare le regole da verificare o applicare. Le regole sono organizzate in gruppi (`<Group/>`) gerarchici i quali a loro volta hanno un *id*, un titolo (`<title/>`) e una descrizione (`<description/>`).

```
1  <Group id="PasswordPolicy">
2      <title> Password Policy</title>
3      <description>
4          Oltre ad istruire gli utenti sull'utilizzo di password forti...
5      </description>
6      <Rule>...</Rule>
7      <Value>...</Value>
8  </Group>
```

Queste informazioni, così come fornite, non sono ovviamente interpretabili da un software, occorre perciò completare la definizione dell'XCCDF con un meccanismo in grado di rendere il documento eseguibile ed automatizzabile; ciò è possibile con il linguaggio *OVAL*. Una regola (`<Rule/>`) può quindi referenziare uno o più controlli OVAL:

```
1  <Rule id="password_strength">
2      <title>Robustezza della password</title>
3      <description />
4      <reference href="http://cce.mitre.org">CCE-2920-7</reference>
5      <rationale>La password deve essere lunga almeno 10 caratteri e
           contenere caratteri speciali, lettere maiuscole, minuscole e
           numeri</rationale>
6      <fixtext>
7          Applicare la policy con /etc/login.defs
8      </fixtext>
9      <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
10         <check-export value-id="minimum_strength" export-name="oval:
               ..."/>
11         <check-content-ref href="..." name=""/>
12     </check>
13 </Rule>
```

OVAL

OVAL, *Open Vulnerability and Assessment Language*, ha come obiettivo proprio quello di automatizzare le operazioni di assessment descritte dall'XCCDF. Il processo di *assessment* può essere diviso in tre passaggi:

- Rappresentazione delle informazioni relative al sistema da testare (*OVAL system characteristics*)
- Definizione delle condizioni che un sistema deve avere affinché abbia una vulnerabilità (*OVAL definition*)
- Reporting (*OVAL results*)

Il linguaggio può essere poi esteso con specifiche aggiuntive magari istanziate su una singola tecnologia (ad es. *Oval Language UNIX Component Model Specification* per i sistemi operativi UNIX e UNIX-like, o *OVAL Language Windows Component Model Specification* per i sistemi Windows). Dal punto di vista del componente implementato, la parte più importante da considerare è rappresentata dalla *OVAL definition*, che è richiamata dalle regole XCCDF. L'obiettiivo è quello di descrivere: *i)* le condizioni che un sistema deve avere affinché abbia una determinata vulnerabilità, *ii)* definizione di eventuali rimedi e patch, *iii)* definizioni per definire le condizioni da verificare per determinare se un determinato software o componente è installato, *iv)* definizioni per la *compliance* ad una politica o ad una definizione specifica.

Sulla base di ciò è possibile, tramite OVAL, determinare se una regola *XCCDF* sia valida o meno sul sistema testato. Si tratta, tuttavia, di un linguaggio orientato all'automazione, che pertanto non può essere applicato in caso di verifiche umane e procedurali, come molti dei controlli di sicurezza analizzati. In questi casi il linguaggio adatto è OCIL, *Open Checklist Interactive Language*.

4.3.2 Il framework OpenSCAP

Uno dei tanti progetti che implementano il protocollo SCAP è Red Hat *OpenSCAP*[13]. Questo fornisce una serie di strumenti open-source:

- una libreria per l'elaborazione di contenuti SCAP
- una libreria per la valutazione dei documenti XCCDF e OVAL
- una serie di XSLT per la trasformazione dei documenti in XML in formati *human-readable* come HTML
- contenuto SCAP (*OpenSCAP security guide*) per l'assessment e la valutazione di varie soluzioni software note, sia a livello operativo che a livello applicativo

OpenSCAP è disponibile nei repository delle distribuzioni Linux ed è composto da:

- tool da riga di comando per la valutazione di XCCDF e OVAL (*oscap-base*)
- demone per l'esecuzione periodica dei test OVAL (*oscap-daemon*)
- piattaforma per la produzione di contenuti SCAP (*oscap-workbench*)
- database per la centralizzazione delle evidenze (*SCAP Timony*)
- addon Anaconda[14] per l'applicazione automatica delle *remediation* in fase di setup
- strumento per il controllo della sicurezza e della compliance in container *Docker*

[13] https://www.open-scap.org

[14] strumento per l'installazione di sistemi operativi Red Hat-based, ivi compresi Fedora e CentOS

4.3.3 Driver OpenSCAP per Moon Cloud

Al fine di effettuare i controlli NIST 800-53 per FedRAMP in Moon Cloud, è stato implementato un apposito driver Moon Cloud per OpenSCAP, in grado di pilotare il tool *oscap* su un server remoto per effettuarne l'analisi; la comunicazione tra il driver e l'host target avviene tramite il protocollo SSH, implementato con la libreria Python *paramiko*.

Come prima cosa, vengono letti i parametri per la connessione: *hostname* o indirizzo IP del target, la porta TCP per SSH, e le credenziali di un utente privilegiato; è supportata l'autenticazione sia tramite password che mediante chiave pubblica.

Viene quindi avviata la connessione SSH e, tramite essa, viene creata una directory temporanea sul server. Questa directory andrà a contenere gli XCCDF selezionati, e sarà eliminata alla fine dell'esecuzione. A seguire, viene effettuato un controllo della presenza di OpenSCAP sul server, che rappresenta un prerequisito per l'esecuzione. Se il file eseguibile *oscap* non viene trovato, il test si blocca ed avvia la sequenza di rollback.

Dopo aver interpreato le configurazioni di OpenSCAP ricevute in input (file XCCDF da considerare, profilo scelto, eventuale download di risorse remote specificate nel XCCDF), viene lanciato il comando *oscap*; il report HTML generato viene eventualmente caricato su un bucket di *Microsoft Azure Storage*. Il flusso di esecuzione si conclude con la rimozione delle cartelle temporanee e la chiusura della connessione SSH.

Il driver supporta gli XCCDF presenti nella *OpenSCAP Security Guide*, ovvero:

ssg-centos5	ssg-rhel5	ssg-ubuntu1404	ssg-sl5
ssg-centos6	ssg-rhel6	ssg-ubuntu1604	ssg-sl6
ssg-centos7	ssg-rhel7	ssg-fedora	ssg-sl7
ssg-debian8	ssg-sle11	ssg-sle12	ssg-opensuse
ssg-wrlinux	ssg-fuse6	ssg-chromium	ssg-firefox
ssg-webmin	ssg-rhel-osp7	ssg-webmin	ssg-jre

I profili relativi a ciascun XCCDF sono ottenibili con il comando:

```
oscap info file.xml
```

Flusso di esecuzione

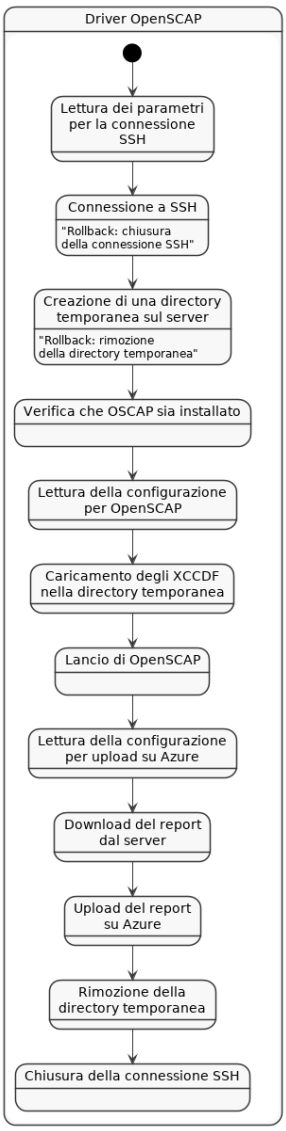


Figura 4.1: Flusso di esecuzione del driver

Metadata

```
{
  "driver-name": "OpenSCAP_SSH",
  "description" : "",
  "schema" : {
        "read_ssh_configuration" : {
            "properties" : {
                "hostname" : {
                    "title" : "SSH Connection String",
                    "type" : "string",
                    "required": true
                },
                "username" : {
                    "title" : "Username",
                    "type" : "string",
                    "required": true
                },
```

```
17                  "password": {
18                      "title":"Password",
19                      "type":"password"
20                  },
21                  "private_key": {
22                      "title": "SSH Private Key",
23                      "type":"string",
24                  },
25                  "private_key_passphrase": {
26                      "title":"Passphrase",
27                      "type":"password"
28                  }
29              },
30              "title" : "Target",
31              "type" : "object"
32          },
33          "read_xccdf_configuration":{
34              "properties": {
35                  "xccdf": {
36                      "title": "XCCDF",
37                      "type": "string",
38                      "required": true
39                  },
40                  "profile": {
41                      "title": "Profile",
42                      "type": "string",
43                      "required":"true"
44                  },
45                  "fetch_remote_resources": {
46                      "title": "Fetch remote resources declared in XCCDF",
47                      "type": "boolean",
48                      "default": false
49                  }
50              },
51              "title": "OpenSCAP settings",
52              "type":"object"
53          },
54          "read_azure_configuration":{
55              "properties": {
56                  "user": {
57                      "title": "Username",
58                      "type": "string",
59                      "required": true
60                  },
61                  "access_key": {
62                      "title": "Access Key",
63                      "type": "password",
64                      "required":true
65                  },
66                  "container_name": {
67                      "title": "Azure Container name",
68                      "type": "string",
69                      "required":true
70                  }
71              },
72              "title": "Azure settings",
73              "type":"object"
74          }
75
76      },
77      "inputs": {
78          "read_ssh_configuration": {
79              "hostname": "string",
80              "username": "string",
81              "password": "password",
82              "private_key": "string",
83              "private_key_passphrase": "string"
84          },
85          "read_xccdf_configuration": {
86              "xccdf": "string",
87              "profile": "string",
88              "fetch_remote_resources": "boolean"
```

```
89          },
90          "read_azure_configuration": {
91              "user": "string",
92              "access_key": "password",
93              "container_name": "string"
94          }
95      },
96      "outputs": {
97          "report": "string"
98      }
99  }
```

Il codice del driver è stato allegato nell'Appendice A

4.4 Controlli ad interazione umana

Poiché, come già ampiamente trattato, non è possibile eseguire in maniera automatica tutti i controlli di sicurezza, l'obiettivo di questa tesi è anche quello di fornire uno strumento per la verifica dei controlli di carattere procedurale che prevedono intrinsecamente un'interazione umana.

La modalità scelta è la somministrazione di questionari agli attori coinvolti nel controllo. A tal fine, una delle possibili strategie è quella di utilizzare il linguaggio OCIL presente nel framework SCAP.

OCIL è un framework generico per la creazione di questionari ad interazione umana e non automatizzabili, definito nel documento NIST Interagency Report 7692 – Specification for the Open Checklist Interactive Language (OCIL) Version 2.0. Le funzionalità di OCIL sono:

- Possibilità di definire domande (con risposte di tipo booleano, scelta multipla, numerico, stringa)
- Possibilità di definire risposte predefinite per ciascuna domanda
- Possibilità di definire le azioni conseguenti alla risposta dell'utente
- Possibilità di catalogare le risposte date

Un esempio di OCIL per la valutazione della *FedRAMP readiness* è presente in appendice B

4.4.1 Driver Survey per Moon Cloud

Si è voluto perciò integrare in Moon Cloud un driver ad interazione umana che, tramite un web-service, proponga all'utente un questionario e generi un report di feedback. Nel caso di Moon Cloud, i questionari non sono descritti in OCIL ma utilizzando lo standard JSON Schema[15]; è possibile eventualmente effettuare la traduzione mediante un foglio di trasformazione *XSLT*.

Il test effettua il download della definizione del questionario da sottoporre, dopodiché esegue una web-application, autenticata con nome utente e password, che offre il questionario all'utente. Il questionario viene effettivamente erogato

[15]JSON Schema *http://www.json-schema.org/*

sul web tramite un reverse proxy per architetture a microservizi chiamato *traefik*[16]; questo è in grado di leggere la lista dei container attivi dalle *API* di Docker, filtrarle in base alle etichette applicate al container, ed esporre all'esterno i servizi.

I *container* di tipo *Survey* vengono quindi avviati con l'etichetta *proxied_survey* e sono forniti in HTTPS. La generazione del certificato è stata automatizzata utilizzando il protocollo *ACME*[17] e il servizio LetsEncrypt[18].

Una volta avviato il web service, viene inviata una notifica a mezzo *e-mail* per il destinatario, con il link per accedere e compilare lo stesso. Al momento della sottomissione del questionario, viene generato un report in PDF, che è successivamente caricato in *Windows Azure Storage* analogamente al report *OSCAP* trattato nella sezione 4.3.3.

La difficoltà principale riscontrata nella realizzazione di questo driver consiste nell'introduzione di un processo manuale all'interno del framework Moon Cloud, ingegnerizzato per eseguire test in modo automatico. Il flusso di esecuzione, in questo caso, è invece caratterizzato da una fase bloccante che termina soltanto dopo un'azione manuale dell'utente; lo *scheduler* di Moon Cloud, pertanto, programma l'esecuzione dei test allocando un thread pool di dimensione fissa, modificabile tramite il parametro *–max-concurrency* e generalmente calcolata in base alla potenza computazionale e al numero di core disponibili sull'*execution node*.

L'esecuzione di un numero elevato di test di tipo *Survey* ha perciò comportato una saturazione del *thread pool*, rendendo impossibile l'esecuzione anche di test automatici. Questo problema è stato affrontato dapprima aumentando il valore di *max-concurrency*, poi facendo scalare orizzontalmente il framework; tuttavia è necessaria una reingegnerizzazione del processo di esecuzione di queste tipologie di test, che devono essere trattati separatamente dai test automatici.

A tal fine sono state proposte due soluzioni:

- La prima soluzione proposta è implementabile aggiungendo un *timer* di durata massima all'esecuzione del test: quando il timer scade, il test viene rimosso restituendo un risultato *False* e il container del driver relativo viene cancellato.

- La seconda soluzione proposta consiste nell'eseguire il container del driver in background, per poi monitorarne lo stato con un ulteriore test ad esecuzione periodica. In questo caso avremmo quindi una evaluation rule così composta:

  ```
  a#1 implies a#2
  ```

  In questo modo *a#1* lancia il driver "survey" in background terminande con valore "true", mentre *a#2* viene eseguito periodicamente per raccogliere il risultato del questionario, e restituisce "false" finché il questionario non è stato compilato.

[16]Traefik: https://www.traefik.io
[17]ACME, *https://tools.ietf.org/html/draft-ietf-acme-acme-04*
[18]https://www.letsencrypt.com

Flusso di esecuzione

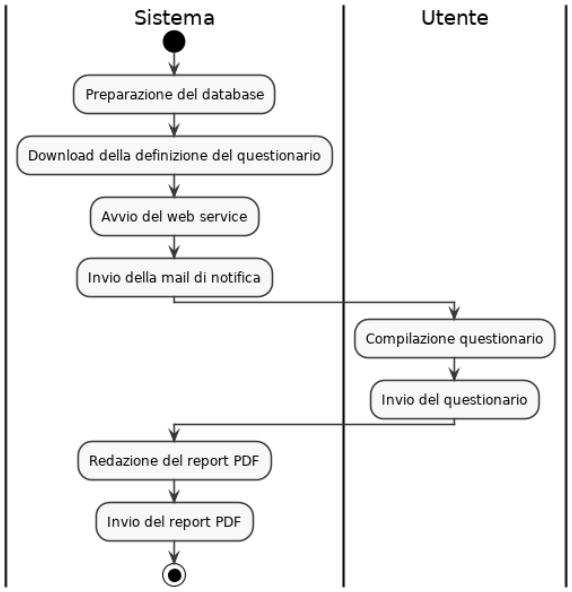


Figura 4.2: Flusso di esecuzione del driver

Metadata

```
{
  "driver-name": "SurveyControl",
  "description": "",
  "schema": {
    "applicant": {
      "type": "object",
      "title": "Applicant Information",
      "properties": {
        "name": {
          "type": "string",
          "title": "Full Name"
        },
        "company": {
          "type": "string",
          "title": "Company"
        },
        "default_sender": {
          "type": "string",
          "title": "E-Mail address"
        }
      }
    },
        "survey_definition": {
            "type": "object",
            "title": "Survey definition",
            "properties": {
                "survey_url": {
                    "type": "string"
                    "title": "Survey definition URL"
                }
            }
        },
        "notification_email_settings": {
      "type": "object",
      "title": "SMTP Client Configuration",
      "properties": {
        "": {
```

```
38            "type": "boolean",
39            "title": "Use moon-cloud email service (it must be selected)",
40            "default": true
41          }
42        }
43      },
44      "notification_email_subject": {
45        "type": "object",
46        "title": "Recipient Information",
47        "properties": {
48          "name": {
49            "type": "string",
50            "title": "Full Name"
51          },
52          "email": {
53            "type": "string",
54            "title": "E-Mail address"
55          }
56        }
57      },
58          "read_azure_configuration":{
59              "properties": {
60                  "user": {
61                      "title": "Username",
62                      "type": "string",
63                      "required": true
64                  },
65                  "access_key": {
66                      "title": "Access Key",
67                      "type": "password",
68                      "required":true
69                  },
70                  "container_name": {
71                      "title": "Azure Container name",
72                      "type": "string",
73                      "required":true
74                  }
75              },
76              "title": "Azure settings",
77              "type":"object"
78          }
79    }
80  }
```

Capitolo 5

Validazione del framework

In questo capitolo verrà proposta una validazione di un deployment di test del framework Moon Cloud, mediante la valutazione della sicurezza tramite l'esecuzione del driver sviluppato a tutti i livelli dello stack cloud (infrastruttura, piattaforma, software).

5.1 Deployment di Moon Cloud

Il deployment dell'ambiente di test è stato effettuato su un'architettura multi-layer così composta:

- A livello di infrastruttura, un nodo fisico, Dell PowerEdge T430 equipaggiato con processore Intel(R) Xeon(R) CPU E5-2630 v4 (10 core fisici e 40 thread logici), 48GB di RAM e 5 dischi da 1TB ciascuno in configurazione RAID 1. Su questa macchina è stato installato il sistema operativo CentOS 7.2, e il software Open Stack Newton. Successivamente sono state create 3 macchine virtuali con sistema operativo CentOS 7.2, in un flavor con 4GB di RAM e 10GB di disco.

- A livello di piattaforma, un cluster Docker Swarm di 2 nodi per i componenti core di Moon Cloud. La terza macchina virtuale è stata utilizzata come nodo di esecuzione per un cluster di dimensione unaria.

- A livello software, i componenti di Moon Cloud: 7 servizi core, gestiti tramite container Docker sul cluster swarm e 3 microservizi per la gestione del nodo di esecuzione.
  Componenti Core

  - API
  - Database
  - Repository
  - Database *time-series* per i risultati
  - Evaluation Manager
  - RabbitMQ per la comunicazione tra API e Container

- Traefik (reverse proxy) per l'esposizione delle API

Componenti execution node e execution cluster

- Execution Manager
- Monitor Execution Manager
- Traefik (reverse proxy) per l'esposizione di alcune tipologie di test

5.2 Sicurezza del deployment

L'analisi della sicurezza è stata effettuata a livello di infrastruttura, analizzando le configurazioni sul sistema operativo del server fisico e le caratteristiche del setup OpenStack; a livello di piattaforma, analizzando le configurazioni del template utilizzato per le macchine virtuali Docker e i container Moon Cloud; a livello applicativo, analizzando la sicurezza nei meccanismi di integrazione dei vari componenti.

5.2.1 Infrastruttura

Analisi OpenSCAP del server fisico

Il test è stato eseguito utilizzando il driver realizzato, specificando in input il documento XCCDF "*ssg-centos7*" unitamente al profilo "*nist-800-171-cui*". Il documento *JSON* dato in input al test è il seguente:

```
{
    "read_ssh_configuration": {
    },
    "read_xccdf_configuration": {
        "xccdf":"ssg-centos7",
        "profile":"nist-800-171-cui",
        "fetch_remote_resources": true
    },
    "read_azure_configuration": {
    }
}
```

I risultati restituiti in output segnalano:

- 119 valutazioni effettuate con successo
- 72 valutazioni fallite

In particolare, delle 72 valutazioni fallite, 11 sono state catalogate da OpenSCAP con *severity* bassa, 50 con severity media e 11 con severity elevata; lo score della copertura XCCDF ottenuto è 71.17%.

▼ AC-2(2)		
Set Password Warning Age	low	pass
Set Account Expiration Following Inactivity	medium	fail
▼ AC-2(3)		
Set Account Expiration Following Inactivity	medium	fail
▼ AC-2(4)		
▼ AC-2(5)		
Set SSH Idle Timeout Interval	low	fail
Set SSH Client Alive Count	medium	fail
▼ AC-2(7)(b)		
▼ AC-3		
Disable SSH Support for .rhosts Files	medium	pass
Disable Host-Based Authentication	medium	pass
Disable SSH Root Login	medium	fail
Disable SSH Access via Empty Passwords	high	fail
Use Only FIPS 140-2 Validated Ciphers	medium	fail
▼ AC-3(3)		
▼ AC-3(4)		
Ensure All Files Are Owned by a User	medium	pass
Ensure All Files Are Owned by a Group	medium	pass

Figura 5.1: Estratto del report

In figura 5.1 è riportata una parte del report generato dal controllo sviluppato; il documento completo è disponibile in formato HTML all'indirizzo:
https://mooncloudashboard.blob.core.windows.net/pdfcontainer/f4a1943cff
o nel repository GIT
https://github.com/patriziotufarolo/tesi_magistrale/.

La valutazione delle *OVAL* mediante il driver realizzato è durata 872 secondi; di seguito sono riportate le statistiche relative all'utilizzo delle risorse nell'esecuzione del test. Queste sono state raccolte tramite il software `pidstat`, isolando esclusivamente i processi coinvolti nel processo di assessment.

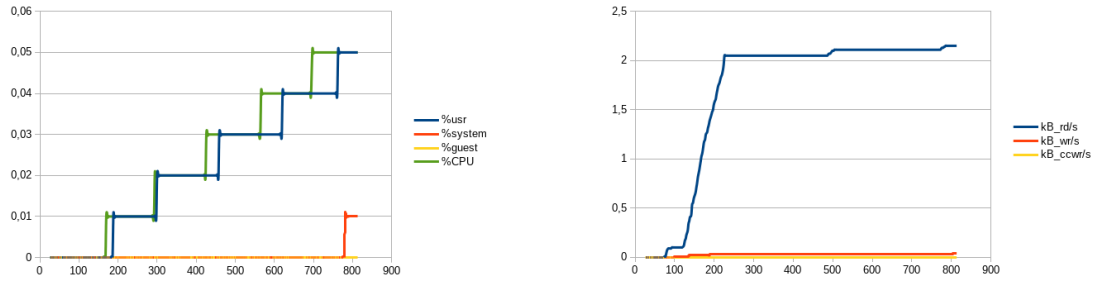


Figura 5.2: Utilizzo della CPU e carico IO

Dalla figura 5.2 è possibile notare come l'impatto del test sulle prestazioni del target sia minimo, registrando picchi di carico sulla CPU inferiori all'0.06% per tutta la durata dell'esecuzione. Anche dal punto di vista delle operazioni di input/output il test si è dimostrato assolutamente non invasivo, registrando picchi in lettura di pochi KB.

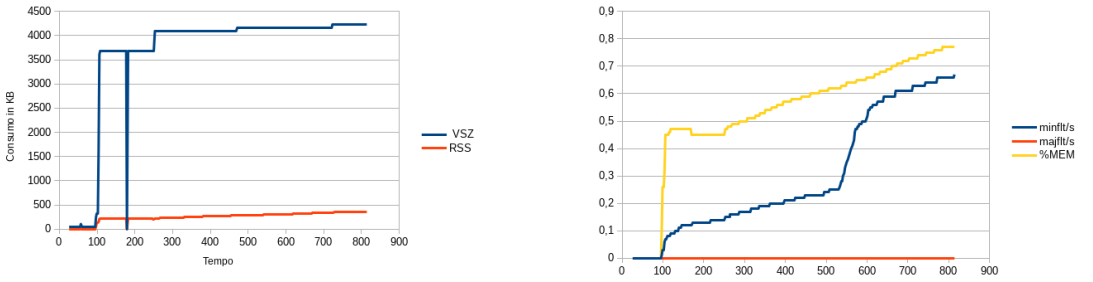


Figura 5.3: Utilizzo della memoria

In figura 5.3 è stato invece illustrato l'utilizzo della memoria durante l'esecuzione del test, che rimane sempre inferiore all'1%. Anche in questo caso l'impatto prestazionale è minimo; il *footprint* di *OpenSCAP* e delle relative *probes* non raggiunge i 5MB in memoria virtuale (VSZ), rimanendo inoltre sotto i 500 KB in memoria RAM(*RSS*).

Un test di questo tipo si presta particolarmente a scenari di esecuzione programmata e automatica, per effettuare monitoraggio continuativo.

Analisi di OpenStack

I documenti XCCDF forniti da OpenSCAP non sono risultati efficienti per l'assessment dei controlli di sicurezza per Open Stack, in quanto le definizioni *OVAL* non sono state redatte Questa sezione, pertanto, fa riferimento al paper "A Security Benchmark for OpenStack". Ogni raccomandazione citata nell'articolo è mappata sui requisiti FedRAMP corrispondenti. A causa del fatto che l'implementazione dei controlli automatici per alcuni di queste non sono disponibili, l'analisi è stata fatta in modo manuale ispezionando le configurazioni.

5.2.2 Piattaforma

Analisi OpenSCAP sul template delle macchine virtuali

test finished started at 1496218136 ended at 1496218350 lasted -214 seconds
report available at https://mooncloudddashboard.blob.core.windows.net/pdfcontainer/b7321
–

Analisi del cluster Docker Swarm

5.2.3 Applicazione

Analisi dei componenti software

L'analisi applicativa sulla piattaforma Moon Cloud è stata svolta analizzando le configurazioni dei servizi e la loro implementazione.

Di seguito i punti critici individuati:

[R7] Configure Centralized Remote Logging. Fallito

[R8] Maintain Time Synchronization Services. Passato

[R9] Review and Minimize Hypervisor Attack Surface. Non eseguito

[R10] Review and Minimize Virtual Machine Manager Attack Surface. Non eseguito

[R11] Use Templates to Deploy Virtual Machines. Passato

[R12] Disconnect unauthorized devices from Virtual Machines. Non applicabile

[R13] Disable MAC Address Changes and Promiscuous Mode on Guests. Hypervisor or Network virtualizators should deny MAC address changes on the Vnic (*Virtual*) Passato

[R14] Ensure Network Isolation through VLANs. Passato

[R15] Port Groups Should not be Configured to Reserved VLANs. Passato

[R16] Secure Access to Cloud Application Programming Interfaces. Fallito

[R17] Encrypt Data at Rest. Fallito

[R18] Establish Appropriate Resource Isolation. Passato [R19] Evaluate Denial of Service Scenarios and Mitigations. Fallito [R20] Do Not Use or Set Guest Customization Passwords. Passato [R21] Evaluate and Minimize Cloud Architecture Dependencie Non eseguito [R22] Audit Sensible and Configuration Files. Fallito [R23] Storage Reliability. Fallito [R24] Data Remanence Avoidance Fallito
5.2. SICUREZZA DEL DEPLOYMENT

Capitolo 6

Conclusioni e sviluppi futuri

6.1 Conclusioni

In questo lavoro di tesi sono state analizzate le problematiche conseguenti alla migrazione di servizi verso la cloud, illustrando le tecniche sviluppate dalla letteratura. È stato poi presentato *Moon Cloud*, un framework sviluppato dal laboratorio SESAR Lab[1] dell'Università degli Studi di Milano, il cui obiettivo è quello di implementare una metodologia automatica per la valutazione della sicurezza, delle performance e di altre proprietà non funzionali, offrendo un processo di assurance basato su attività di auditing e raccolta di evidenze.

Successivamente è stato approfondito *FedRAMP*, il programma federale per l'autorizzazione e l'analisi del rischio per l'adozione dei servizi cloud nelle agenzie governative, caratterizzando le fasi critiche del programma e illustrando come Moon Cloud possa costituire uno strumento di supporto per i vari attori. Questa fase ha puntato a fornire delle linee guida per tutte quelle realtà, anche operanti fuori dagli Stati Uniti, che vogliano usufruire dei vantaggi della *cloud* nell'erogazione dei propri servizi, pur mantenendo livelli di rischi accettabili; si è voluto infatti dimostrare come la soluzione *Moon Cloud* possa essere adattata a vari casi d'uso fornendo, nello scenario specifico, supporto a ciascuno degli attori coinvolti nel programma FedRAMP.

La metodologia di *assurance* utilizzata in tal senso, permette sia di effettuare l'assessment automatico di proprietà non funzionali mediante l'esecuzione di test, sia di analizzare proprietà di sicurezza di carattere procedurale, andando ad ispezionare processi di business condotti perlopiù da attori umani.

Analizzando i controlli di sicurezza di FedRAMP, sono stati caratterizzati i controlli, dividendo quelli eseguibili in maniera automatica da quelli eseguibili in modo manuale. Al fine di garantire una buona copertura dei controlli automatizzabili, in aggiunta ai driver già implementati in Moon Cloud, è stato quindi realizzato un ulteriore *driver* per integrare il prodotto OpenSCAP. Per i controlli di tipo procedurale o non implementabili in modo automatico, invece, è stato fornito un driver per l'esecuzione di sondaggi, che si integra nel flusso di esecuzione di Moon Cloud ed esegue una web application dedicata.

Infine, il framework Moon Cloud è stato validato mediante l'analisi della sicurezza del *deployment* multi-tier di un'architettura a microservizi, Moon Cloud

[1] SEcure Service-oriented Architectures Research Lab - *http://sesar.di.unimi.it*

stesso, offrendo una prospettiva sulle performance di esecuzione. Questa attività di analisi è stata articolata in tre fasi:

1. Analisi della sicurezza dell'infrastruttura, eseguita mediante l'esecuzione del driver OpenSCAP sviluppato per analizzare le configurazioni del sistema operativo sottostante, per il quale sono state recensite le prestazioni

2. Analisi della sicurezza del software IaaS OpenStack, effettuata sulla base del paper "A security benchmark for OpenStack" con tecniche automatiche e manuali

3. Analisi della sicurezza degli host appartenenti al cluster Docker Swarm, eseguendo ancora una volta il driver OpenSCAP

4. Esecuzione del driver Moon Cloud per il security benchmark CIS Docker

5. Analisi statica dei container Moon Cloud

6. Analisi della sicurezza dei componenti Moon Cloud

6.2 Sviluppi futuri

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 della compliance per altri standard di settore.

Pertanto, se da una parte l'approccio fornito può essere utilizzato per effettuare controlli di compliance verso altre normative e politiche di sicurezza, (come ad esempio PCI-DSS, HIPAA e la famiglia di standard ISO-27000), da un'altra è possibile adattare le tecniche presentate a contesti alternativi, pur utili a garantire livelli di sicurezza elevati all'interno di un'organizzazione. Uno tra questi, può essere la valutazione delle competenze in ambito di sicurezza informatica dei dipendenti di un'azienda, la valutazione del grado di accettabilità delle misure di sicurezza adottate, l'automazione di valutazioni comportamentali ad esempio con test di *phishing* controllati.

La capacità di effettuare analisi periodiche e la forte possibilità di integrazione con componenti di terze parti, unite al supporto a tecnologie standard e validate da istituti autorevoli (in questo caso il NIST) permettono a *Moon Cloud* di posizionarsi sul mercato come soluzione di monitoraggio per la *security assurance*; in ogni caso, i componenti sviluppati possono essere ulteriormente raffinati e perfezionati. Per quanto riguarda il driver *OpenSCAP*, è possibile produrre *XCCDF* per l'esecuzione di test di sicurezza relativi ad altre tecnologie. Uno dei limiti del driver è costituito dalla necessità di avere il pacchetto *oscap* installato sul server target; in tal senso, una delle possibili soluzioni adottabili, potrebbe essere quella di effettuare un fork di *OpenSCAP* per implementare l'esecuzione remota dei controlli, riconducendo l'approccio *OpenSCAP* alla metodologia *Moon Cloud*.

La web application fornita per l'erogazione dei questionari nel controllo *Survey*, invece, può essere adattata allo standard *OCIL* mediante la redazione di un foglio *XSLT* per la traduzione da *OCIL* a *JSON Schema*; possono essere inoltre

introdotti meccanismi per garantire l'autenticità e l'integrità dei dati inviati, mediante l'utilizzo di dispositivi per la firma digitale e di tecnologie per lo storage sicuro dei report.

Infine, poiché il materiale SCAP relativo al prodotto OpenStack non si è rivelato di qualità idonea per guidare un processo di valutazione della sicurezza, un ulteriore sviluppo potrebbe consistere nell'integrazione del lavoro illustrato nell'articolo *A Security Benchmark for OpenStack*, eventualmente ampliato ed adattato alle soluzioni dei vari partner della OpenStack Foundation.

Appendice A

Driver di integrazione con OpenSCAP

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import sys
import spur
import uuid

from xml.etree import cElementTree as ElementTree

from driver import Driver
from test.ssh_client import CustomSshShell
from azure.storage.blob import BlockBlobService, ContentSettings

__author__ = "Patrizio Tufarolo"
__email__ = "patrizio@tufarolo.eu"

__description__ = "This driver controls a remote OpenSCAP instance through SSH"

ocil_cs = "http://scap.nist.gov/schema/ocil/2"
xccdf_ns = "http://checklists.nist.gov/xccdf/1.1"


class SSHConnection(object):
    def read_ssh_configuration(self, inputs):
        ssh_connection_ti = self.testinstances.get("read_ssh_configuration",
                                                   {})

        assert ssh_connection_ti is not None
        hostname = ssh_connection_ti.get("hostname")
        port = ssh_connection_ti.get("port", 22)
        username = ssh_connection_ti.get("username")
        password = ssh_connection_ti.get("password", None)
        private_key = ssh_connection_ti.get("private_key", None)
        private_key_passphrase = None
        if private_key is not None:
            private_key_passphrase = ssh_connection_ti.get(
                "private_key_passphrase",
                None)

        return hostname, port, username, password, \
            private_key or None, private_key_passphrase or None

    def ssh_connection(self, inputs):
        hostname, port, username, password, \
            private_key, private_key_passphrase = inputs
        self.ssh_client = \
            CustomSshShell(hostname=hostname,
                           username=username,
                           password=password,
                           port=port,
```

```
50                              private_key=private_key,
51                              private_key_passphrase=private_key_passphrase,
52                              missing_host_key=spur.ssh.MissingHostKey.warn,
53                              shell_type=spur.ssh.ShellTypes.sh
54                              )
55          return isinstance(self.ssh_client, spur.SshShell)
56
57      def ssh_create_tmp_dir(self, ssh_client_ok):
58          self.temp_dir = None
59          assert ssh_client_ok and isinstance(self.ssh_client, spur.SshShell)
60          self.temp_dir = self.ssh_client.run(
61              ["mktemp", "--directory"], encoding="ascii").output.strip()
62
63      def ssh_remove_tmp_dir(self, inputs):
64          assert self.temp_dir
65          self.ssh_client.run(["rm", "-rf", self.temp_dir])
66
67      def ssh_close(self, inputs):
68          self.ssh_client.__exit__()
69
70
71  class XCCDFEvaluator(SSHConnection):
72      def read_xccdf_configuration(self, inputs):
73          xccdf_ti = self.testinstances.get("read_xccdf_configuration", None)
74          xccdf = xccdf_ti.get("xccdf", None)
75          profile = xccdf_ti.get("profile", None)
76          assert xccdf is not None and profile is not None
77          fetch_remote_resources = xccdf_ti.get("fetch_remote_resources", False)
78          return xccdf, profile, fetch_remote_resources
79
80      @staticmethod
81      def get_xccdf_references(xccdf):
82          result = []
83          xccdftree = ElementTree.parse(
84              "/usr/src/app/test/ssg/{xccdf}-xccdf.xml".format(xccdf=xccdf)
85          )
86          check_content_refs = xccdftree.findall(
87              ".//{%s}check-content-ref" % xccdf_ns
88          )
89
90          for check_content_ref in check_content_refs:
91              check_content_ref_href_attr = check_content_ref.get("href")
92              if check_content_ref_href_attr.startswith("http://") or \
93                      check_content_ref_href_attr.startswith("https://"):
94                  continue
95              refhref = check_content_ref.get("href")
96              if refhref not in result:
97                  result.append(refhref)
98
99          return result
100
101     def upload_files(self, inputs):
102         xccdf, profile, fetch_remote_resources = inputs
103         with self.ssh_client._connect_sftp() as sftp:
104             sftp.put(
105                 "/usr/src/app/test/ssg/{xccdf}-xccdf.xml".format(xccdf=xccdf),
106                 self.temp_dir + "/" + "{xccdf}-xccdf.xml".format(xccdf=xccdf)
107             )
108
109             for document in self.get_xccdf_references(xccdf):
110                 sftp.put(
111                     "/usr/src/app/test/ssg/{document}"
112                     .format(document=document),
113                     self.temp_dir + "/" + "{document}".
114                     format(document=document)
115                 )
116         return xccdf, profile, fetch_remote_resources
117
118     def get_report(self, inputs):
119         with self.ssh_client._connect_sftp() as sftp:
120             sftp.get(
121                 "{temp_dir}/report.html".format(temp_dir=self.temp_dir),
```

```
122                 "/tmp/report.html"
123             )
124         return inputs
125
126     def evaluate_xccdf(self, inputs):
127         xccdf, profile, fetch_remote_resources = inputs
128         ssh_command = [
129             "oscap",
130             "xccdf",
131             "eval",
132             "--profile", "{profile}".format(profile=profile),
133             "--results-arf", "{temp_dir}/results.arf.xml".format(
134                 temp_dir=self.temp_dir
135             ),
136             "--progress",
137             "--report",
138             "{temp_dir}/report.html".format(
139                 temp_dir=self.temp_dir
140             ),
141             "{temp_dir}/{xccdf}-xccdf.xml".format(
142                 temp_dir=self.temp_dir, xccdf=xccdf
143             )
144         ]
145         index = 7
146         if not self.verifyRoot():
147             ssh_command = ["sudo"] + ssh_command
148             index += 1
149         if fetch_remote_resources:
150             ssh_command.insert(index, "--fetch-remote-resources")
151         print ssh_command
152         out = self.ssh_client.run(ssh_command,
153                                   stdout=sys.stderr,
154                                   stderr=sys.stderr,
155                                   use_pty=True,
156                                   allow_error=True).output.strip().split("\n")
157         initial_result = "pass"
158         for line in out:
159             if line.strip() == "":
160                 continue
161             if ":" not in line:
162                 continue
163             if line.startswith("Downloading"):
164                 continue
165
166             splitted = line.split(":")
167             if len(splitted) < 2:
168                 continue
169
170             try:
171                 initial_result = initial_result and splitted[1] != "fail"
172                 self.result.put_value(splitted[0], splitted[1])
173             except IndexError:
174                 continue
175
176         return initial_result
177
178
179 class AzureUploader(object):
180     def read_azure_configuration(self, inputs):
181         azure_ti = self.testinstances.get("read_azure_configuration", {})
182         azure_user = azure_ti.get("user", None)
183         azure_access_key = azure_ti.get("access_key", None)
184         azure_container_name = azure_ti.get("container_name", None)
185         self.azure_user = azure_user
186         self.azure_access_key = azure_access_key
187         self.azure_container_name = azure_container_name
188         return inputs
189
190     def upload_to_azure(self, inputs):
191         try:
192             azure_user, \
193                 azure_access_key, \
```

```
194                 azure_container_name = \
195                 self.azure_user, \
196                 self.azure_access_key, \
197                 self.azure_container_name
198 
199             if azure_user is None or azure_access_key is None \
200                     or azure_container_name is None:
201                 return inputs
202             block_blob_service = BlockBlobService(account_name=azure_user,
203                                                   account_key=azure_access_key)
204 
205             blob_name = str(uuid.uuid4()).replace("-", "")[:10]
206             block_blob_service.create_blob_from_path(
207                 self.azure_container_name, blob_name,
208                 "/tmp/report.html",
209                 content_settings=ContentSettings(content_type="text/html")
210             )
211             report_url = block_blob_service.make_blob_url(
212                 self.azure_container_name, blob_name
213             )
214             self.result.put_value("report", report_url)
215         except:
216             self.logger.error("Error during report upload")
217         return inputs
218 
219 
220 class OpenSCAP_SSH(Driver, XCCDFEvaluator, AzureUploader):
221 
222     def verifyOscapInstalled(self, inputs):
223         try:
224             assert self.ssh_client.run(["/usr/bin/which", "oscap"])
225             return True
226         except AssertionError:
227             return False
228 
229         return inputs
230 
231     def verifyRoot(self):
232         return self.ssh_client.run([
233             "/usr/bin/id", "-u"
234         ]).output.strip() == "0"
235 
236     def appendAtomics(self):
237         self.appendAtomic(self.read_ssh_configuration, lambda rollback: False)
238         self.appendAtomic(self.ssh_connection, self.ssh_close)
239         self.appendAtomic(self.ssh_create_tmp_dir, self.ssh_remove_tmp_dir)
240         self.appendAtomic(self.verifyOscapInstalled, lambda rollback: None)
241         self.appendAtomic(self.read_xccdf_configuration, lambda rollback: None)
242         self.appendAtomic(self.upload_files, lambda rollback: None)
243         self.appendAtomic(self.evaluate_xccdf, lambda rollback: None)
244         self.appendAtomic(self.read_azure_configuration, lambda rollback: None)
245         self.appendAtomic(self.get_report, lambda rollback: None)
246         self.appendAtomic(self.upload_to_azure, lambda rollback: None)
247         self.appendAtomic(self.ssh_remove_tmp_dir, lambda rollback: None)
248         self.appendAtomic(self.ssh_close, lambda rollback: None)
```

Appendice B

FedRAMP readiness

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <ocil xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3    xsi:schemaLocation="http://www.mitre.org/ocil/1.0 ocil.xsd" xmlns="
       http://www.mitre.org/ocil/1.0">
4    <generator>
5      <schema_version>1.0</schema_version>
6      <timestamp>2017-05-20T12:06:31</timestamp>
7      <author organization="Universita degli Studi di Milano">Patrizio
      Tufarolo</author>
8    </generator>
9
10   <document>
11     <title>FedRAMP Readiness</title>
12     <description>Questionario per la FedRAMP readiness</description>
13   </document>
14
15   <boolean_question_test_action question_ref="ocil:mitre.org:question:1
       " id="ocil:mitre.org:testaction:1">
16     <when_true>
17       <result>SUCCESS</result>
18     </when_true>
19
20     <when_false>
21       <result>FAIL</result>
22     </when_false>
23
24   </boolean_question_test_action>
25
26
27
28   [...]
29
30
31
32   <boolean_question id="ocil:mitre.org:question:1" model="MODEL_YES_NO"
       >
33     <question_text>L'organizzazione e in grado di affrontare processi
         elettronici ed eventuali contenziosi?</question_text>
34   </boolean_question>
35
```

```
36    <boolean_question id="ocil:mitre.org:question:2" model="MODEL_YES_NO"
          >
37      <question_text>L'organizzazione e in grado di determinare e
            descrivere in modo chiaro i confini del sistema?</question_text
            >
38    </boolean_question>
39    <boolean_question id="ocil:mitre.org:question:3" model="MODEL_YES_NO"
          >
40      <question_text>L'organizzazione ha meccanismi per gestire la shared
             responsability?</question_text>
41    </boolean_question>
42
43    <boolean_question id="ocil:mitre.org:question:4" model="MODEL_YES_NO"
          >
44      <question_text>E presente un meccanismo di autenticazione a due
            fattori per l'accesso via rete tramite account privilegiati?</
            question_text>
45    </boolean_question>
46
47    <boolean_question id="ocil:mitre.org:question:5" model="MODEL_YES_NO"
          >
48      <question_text>E presente un meccanismo di autenticazione a due
            fattori per l'accesso via rete tramite account non privilegiati
            ?</question_text>
49    </boolean_question>
50
51    <boolean_question id="ocil:mitre.org:question:6" model="MODEL_YES_NO"
          >
52      <question_text>E presente un meccanismo di autenticazione a due
            fattori per l'accesso locale tramite account privilegiati?</
            question_text>
53    </boolean_question>
54
55    <boolean_question id="ocil:mitre.org:question:7" model="MODEL_YES_NO"
          >
56      <question_text>Si ha la possibilit\'a di effettuare analisi del
            codice per le soluzioni software adottate?</question_text>
57    </boolean_question>
58
59    <boolean_question id="ocil:mitre.org:question:8" model="MODEL_YES_NO"
          >
60      <question_text>Sono predisposte protezioni di confine per l'
            isolamento fisico degli asset?</question_text>
61    </boolean_question>
62
63    <boolean_question id="ocil:mitre.org:question:8" model="MODEL_YES_NO"
          >
64      <question_text>Sono predisposte protezioni di confine per l'
            isolamento logico degli asset?</question_text>
65    </boolean_question>
66
67    <boolean_question id="ocil:mitre.org:question:8" model="MODEL_YES_NO"
          >
68      <question_text>Si \'e in grado di rimediare a situazioni di rischio
             elevato entro 30 giorni?</question_text>
69    </boolean_question>
70
```

```
71    <boolean_question id="ocil:mitre.org:question:9" model="MODEL_YES_NO"
          >
72      <question_text>Viene redatto un inventario dei dispositivi?</
            question_text>
73    </boolean_question>
74
75    <boolean_question id="ocil:mitre.org:question:10" model="MODEL_YES_NO
          ">
76      <question_text>Si hanno meccanismi di sicurezza per evitare data
            leakage?</question_text>
77    </boolean_question>
78
79    <boolean_question id="ocil:mitre.org:question:11" model="MODEL_YES_NO
          ">
80      <question_text>Si hanno meccanismi di crittografia dei dati in
            transito sulla rete?</question_text>
81    </boolean_question>
82
83  </ocil>
```

Bibliografia

[1] National Institute of Standards e Technology (Peter Mell Timothy Grance). *The NIST Definition of Cloud Computing*. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] S. Dhar. «From outsourcing to Cloud computing: Evolution of IT services». In: Technology Management Conference (ITMC), 2011 IEEE International. IEEE.

[3] Claudio A. Ardagna et al. «From Security to Assurance in the Cloud: A Survey». In: *ACM Comput. Surv.* 48.1 (lug. 2015), 2:1–2:50. ISSN: 0360-0300. DOI: 10.1145/2767005. URL: http://doi.acm.org/10.1145/2767005.

[4] N. Gruschka e L. L. Iacono. «Vulnerable Cloud: SOAP Message Security Validation Revisited». In: *2009 IEEE International Conference on Web Services*. Lug. 2009, pp. 625–631. DOI: 10.1109/ICWS.2009.70.

[5] Sven Bugiel et al. «AmazonIA: When Elasticity Snaps Back». In: *Proceedings of the 18th ACM Conference on Computer and Communications Security*. CCS '11. Chicago, Illinois, USA: ACM, 2011, pp. 389–400. ISBN: 978-1-4503-0948-6. DOI: 10.1145/2046707.2046753. URL: http://doi.acm.org/10.1145/2046707.2046753.

[6] Thomas Ristenpart et al. «Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds». In: *Proceedings of the 16th ACM Conference on Computer and Communications Security*. CCS '09. Chicago, Illinois, USA: ACM, 2009, pp. 199–212. ISBN: 978-1-60558-894-0. DOI: 10.1145/1653662.1653687. URL: http://doi.acm.org/10.1145/1653662.1653687.

[7] M. Green. «The Threat in the Cloud». In: *IEEE Security Privacy* 11.1 (gen. 2013), pp. 86–89. ISSN: 1540-7993. DOI: 10.1109/MSP.2013.20.

[8] Huan Liu. «A New Form of DOS Attack in a Cloud and Its Avoidance Mechanism». In: *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*. CCSW '10. Chicago, Illinois, USA: ACM, 2010, pp. 65–76. ISBN: 978-1-4503-0089-6. DOI: 10.1145/1866835.1866849. URL: http://doi.acm.org/10.1145/1866835.1866849.

[9] F. Rocha e M. Correia. «Lucy in the sky without diamonds: Stealing confidential data in the cloud». In: *2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*. Giu. 2011, pp. 129–134. DOI: 10.1109/DSNW.2011.5958798.

[10] Sören Bleikertz et al. «Client-controlled Cryptography-as-a-service in the Cloud». In: *Proceedings of the 11th International Conference on Applied Cryptography and Network Security*. ACNS'13. Banff, AB, Canada: Springer-Verlag, 2013, pp. 19–36. ISBN: 978-3-642-38979-5. DOI: 10.1007/978-3-642-38980-1_2. URL: http://dx.doi.org/10.1007/978-3-642-38980-1_2.

[11] S. De Capitani di Vimercati et al. «Three-server swapping for access confidentiality». In: *IEEE Transactions on Cloud Computing* PP.99 (2015), pp. 1–1. ISSN: 2168-7161. DOI: 10.1109/TCC.2015.2449993.

[12] S. De Capitani di Vimercati et al. «Integrity for join queries in the cloud». In: *IEEE Transactions on Cloud Computing* 1.2 (lug. 2013), pp. 187–200. ISSN: 2168-7161. DOI: 10.1109/TCC.2013.18.

[13] S. A. Almulla e Chan Yeob Yeun. «Cloud computing security management». In: *2010 Second International Conference on Engineering System Management and Applications*. Mar. 2010, pp. 1–7.

[14] Hassan Takabi e James B.D. Joshi. «Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment». In: *45th Hawaii International Conference on System Sciences (HICSS-45)*. IEEE, 2012, pp. 5500–5508. URL: http://d-scholarship.pitt.edu/13526/.

[15] Philogene A. Boampong e Luay A. Wahsheh. «Different Facets of Security in the Cloud». In: *Proceedings of the 15th Communications and Networking Simulation Symposium*. CNS '12. Orlando, Florida: Society for Computer Simulation International, 2012, 5:1–5:7. ISBN: 978-1-61839-785-0. URL: http://dl.acm.org/citation.cfm?id=2331762.2331767.

[16] F. John Krautheim. «Private Virtual Infrastructure for Cloud Computing». In: *Proceedings of the 2009 Conference on Hot Topics in Cloud Computing*. HotCloud'09. San Diego, California: USENIX Association, 2009. URL: http://dl.acm.org/citation.cfm?id=1855533.1855538.

[17] Stefan Berger et al. «vTPM: Virtualizing the Trusted Platform Module». In: *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*. USENIX-SS'06. Vancouver, B.C., Canada: USENIX Association, 2006. URL: http://dl.acm.org/citation.cfm?id=1267336.1267357.

[18] Michael Velten e Frederic Stumpf. «Secure and Privacy-Aware Multiplexing of Hardware-Protected TPM Integrity Measurements among Virtual Machines». In: *Information Security and Cryptology – ICISC 2012: 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*. A cura di Taekyoung Kwon, Mun-Kyu Lee e Daesung Kwon. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 324–336. ISBN: 978-3-642-37682-5. DOI: 10.1007/978-3-642-37682-5_23. URL: http://dx.doi.org/10.1007/978-3-642-37682-5_23.

[19] Jakub Szefer e Ruby B. Lee. «Hardware-Enhanced Security for Cloud». In: *Secure Cloud Computing*. Berlin: Springer, 2014, pp. 57–76. URL: http://link.springer.com/chapter/10.1007%2F978-1-4614-9278-8_3.

[20] C. A. Ardagna et al. «On the Management of Cloud Non-Functional Properties: The Cloud Transparency Toolkit». In: *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*. Mar. 2014, pp. 1–4. DOI: 10.1109/NTMS.2014.6814039.

[21] K.M. Goertzel et al. *Software Security Assurance: A State-of-the Art Report (SOAR)*. Information Assurance Technology Analysis Center, 2007. URL: https://books.google.it/books?id=xxHPMgEACAAJ.

[22] Iain MacNeil e Xiao Li. «"Comply or Explain": market discipline and non-compliance with the Combined Code». In: *Corporate Governance: An International Review* 14.5 (2006), pp. 486–496. URL: http://EconPapers.repec.org/RePEc:bla:corgov:v:14:y:2006:i:5:p:486-496.

[23] L. M. Riungu, O. Taipale e K. Smolander. «Research Issues for Software Testing in the Cloud». In: *2010 IEEE Second International Conference on Cloud Computing Technology and Science*. Nov. 2010, pp. 557–564. DOI: 10.1109/CloudCom.2010.58.

[24] Z. Chiba et al. «A survey of intrusion detection systems for cloud computing environment». In: *2016 International Conference on Engineering MIS (ICEMIS)*. Set. 2016, pp. 1–13. DOI: 10.1109/ICEMIS.2016.7745295.

[25] M. Ficco, L. Tasquier e R. Aversa. «Intrusion Detection in Cloud Computing». In: *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. Ott. 2013, pp. 276–283. DOI: 10.1109/3PGCIC.2013.47.

[26] E. et al. Damiani. *Cumulus. D2.3 Certification models v.2*. Seventh Framework Programme - CUMULUS FP7, 2014.

[27] Marco Anisetti et al. «A Test-based Security Certification Scheme for Web Services». In: *ACM Trans. Web* 7.2 (mag. 2013), 5:1–5:41. ISSN: 1559-1131. DOI: 10.1145/2460383.2460384. URL: http://doi.acm.org/10.1145/2460383.2460384.

[28] E. Damiani et al. «WS-Certificate». In: *2009 Congress on Services - I*. Lug. 2009, pp. 637–644. DOI: 10.1109/SERVICES-I.2009.132.

[29] M. Anisetti, C. Ardagna e E. Damiani. «2012». In: (Low-Cost Security Certification Scheme for Evolving Services).

[30] Ernesto Damiani Marco Anisetti Claudio Ardagna. «A Test-Based Security Certification Scheme for Web Services». In: *ACM Transactions on the Web (TWEB)* (2013).

[31] M. Anisetti, C. A. Ardagna e E. Damiani. «Security Certification of Composite Services: A Test-Based Approach». In: *2013 IEEE 20th International Conference on Web Services*. Giu. 2013, pp. 475–482. DOI: 10.1109/ICWS.2013.70.

[32] G. Spanoudakis, E. Damiani e A. Maña. «Certifying Services in Cloud: The Case for a Hybrid, Incremental and Multi-layer Approach». In: *2012 IEEE 14th International Symposium on High-Assurance Systems Engineering*. Ott. 2012, pp. 175–176. DOI: 10.1109/HASE.2012.16.

[33] N. S. Chauhan, A. Saxena e J. Murthy. «An Approach to Measure Security of Cloud Hosted Application». In: *2013 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*. Ott. 2013, pp. 1–6. DOI: 10.1109/CCEM.2013.6684427.

[34] Moon Cloud. *Moon Cloud Website*. 2017. URL: https://www.moon-cloud.eu/.

[35] M. Anisetti et al. «A Security Benchmark for OpenStack». In: *2017 IEEE International Conference on Cloud Computing*. Giu. 2017.

[36] United States. General Accounting Office. *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation : Report to Congressional Requesters*. U.S. General Accounting Office, 2004. URL: https://books.google.it/books?id=jyTjnQAACAAJ.

[37] National Institute Of Standards. *NIST SP 800-53 r4 - Recommended Security Controls for Federal Information Systems*. 2013. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[38] National Institute Of Standards. *NIST SP 800-60 v2r1 - Guide for mapping types of information and information systems to security categories*. 2003. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.

[39] National Institute Of Standards. *NIST SP 800-160 - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. 2016. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

[40] National Institute Of Standards. *NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems*. 2010. URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[41] National Institute Of Standards. *NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. 2011. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

[42] FedRAMP. *Guide to Understanding FedRAMP, v2*. 2014. URL: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx.

[43] L. Taylor. «FedRAMP: History and Future Direction». In: *IEEE Cloud Computing* 1.3 (set. 2014), pp. 10–14. ISSN: 2325-6095. DOI: 10.1109/MCC.2014.54.

[44] FedRAMP. *FedRAMP Security Assessment Framework*. URL: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf.

[45] FedRAMP. *FedRAMP Security Controls Preface*. URL: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/03/FedRAMP-Security-Controls-Preface-FINAL-1.pdf.

[46] FedRAMP. *FedRAMP HHH Low Baseline Security Controls*. URL: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2016/07/FedRAMP-Low-HHH-Baseline-Controls-2016-05-18.xlsx.

[47] FedRAMP. *FedRAMP HHH Moderate Baseline Security Controls*. URL: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2016/07/FedRAMP-Moderate-HHH-Baseline-Controls-2016-05-18.xlsx.