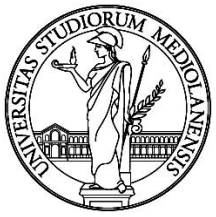


UNIVERSITÀ DEGLI STUDI DI MILANO

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

Acknowledgments

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

.

.

Capitolo 2

Security assurance: lo stato dell'arte e la sfida

2.1 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/*

2.2 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

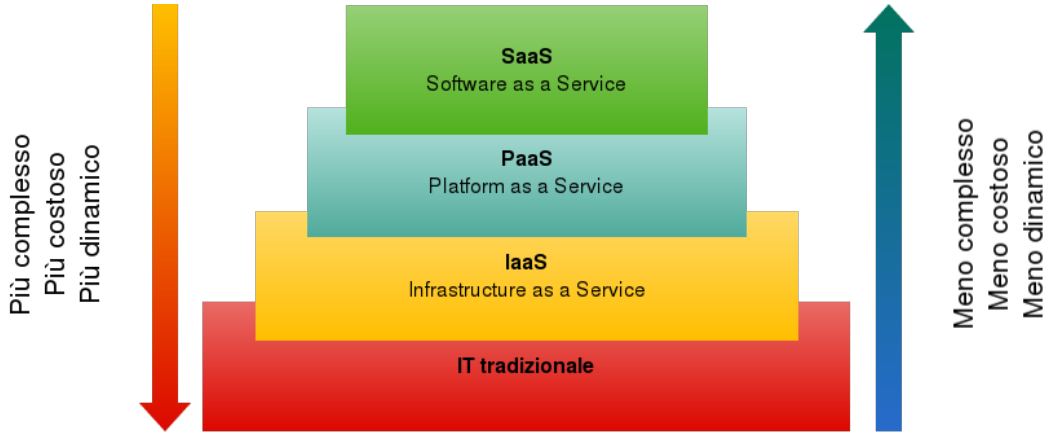
[4]Docker, *https://www.docker.com*

[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 2.1: 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].

2.3 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

2.3.1 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

2.3.2 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.

2.3.3 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.

2.4 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.

2.4.1 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.

2.4.2 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.

2.5 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

2.5.1 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.

2.5.2 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*.

2.5.3 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 containerhttp://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].

2.6 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.

Si vuole perciò realizzare 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)

Nei prossimi capitoli verrà illustrato FedRAMP, un programma governativo americano che fornisce un approccio standard per effettuare il *security assessment* e automatizzare il monitoraggio continuativo dei servizi cloud; verra mostrata la soluzione Moon Cloud per il controllo della conformità di infrastrutture, piattaforme e software sulla *cloud* basato su metodologie di testing e monitoraggio,

saranno illustrate le implementazioni di alcuni *security control* di FedRAMP in Moon Cloud per concludere con la valutazione e la validazione del framework mediante l'assessment del deployment di un'architettura software orientata a microservizi in modalità multi-layer.

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. In conclusione saranno esposti i concetti di *readiness* e di *compliance* al programma, e sarà approfondito il ruolo dello stesso 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[34]: 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[35], fornendo una metodologia per la selezione dei controlli di sicurezza e per l'esecuzione del deployment e dell'assessment.

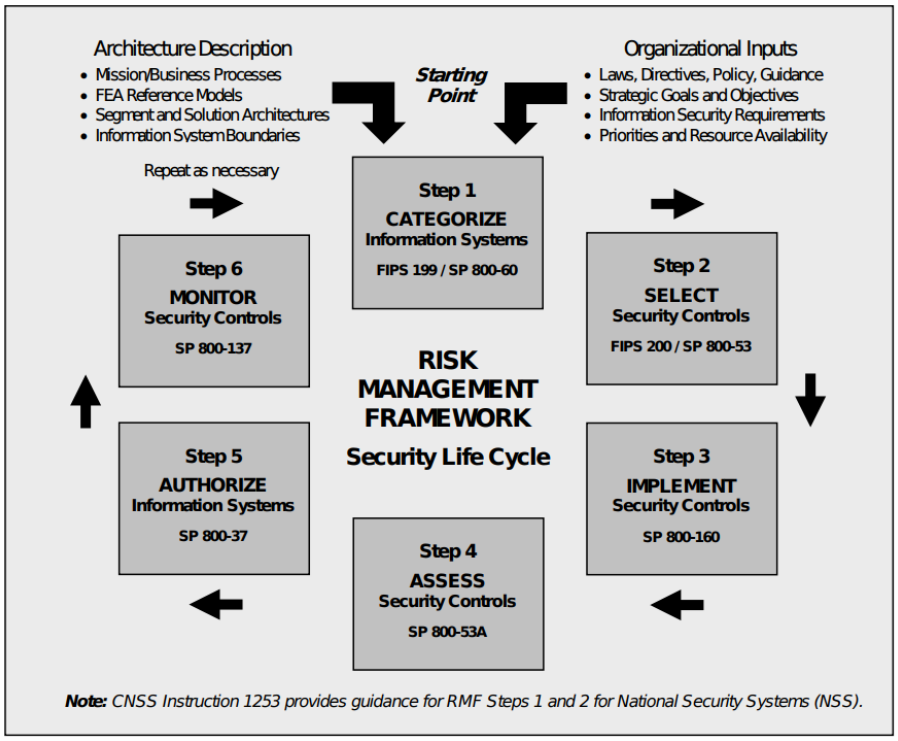


Figura 3.1: Risk Management Framework, da [35]

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 SP 800-60. 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 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

- **Assessment dei controlli di sicurezza**, regolato dal documento SP 800-53/A

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

- **Fase di monitoraggio**

3.2.2 Obiettivo di FedRAMP

L'obiettivo di FedRAMP è quindi 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:

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

- Offrendo un programma di analisi della conformità in grado di produrre

- 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.

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 Attori coinvolti

Gli attori coinvolti in FedRAMP 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.

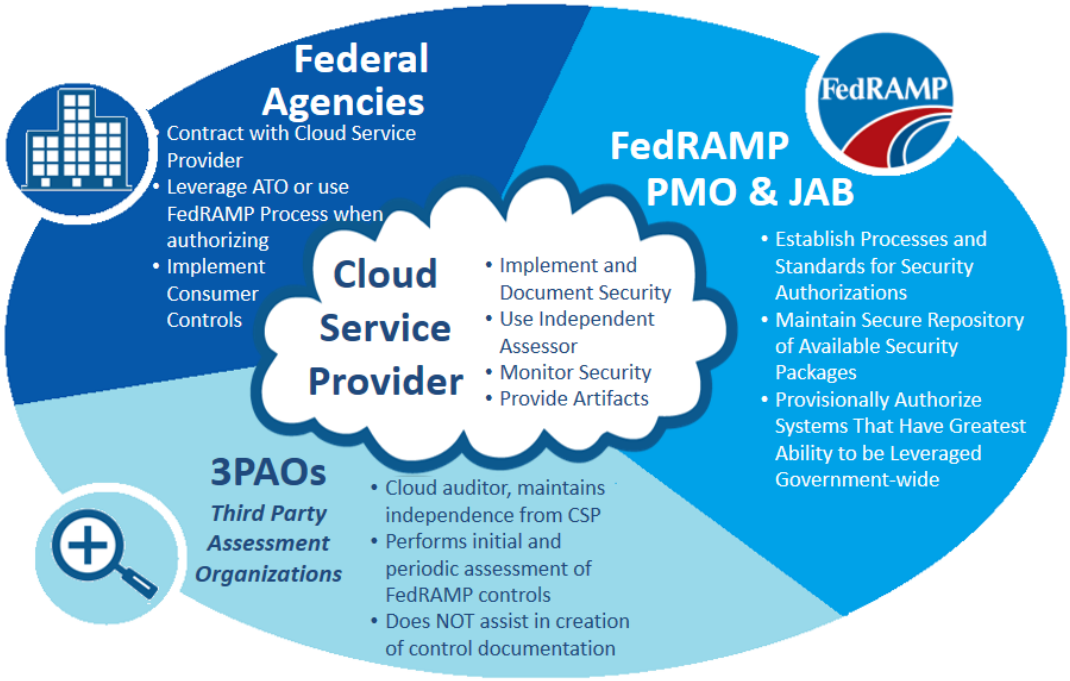


Figura 3.2: Risk Management Framework, da []

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.*

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'en-

te 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.

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). Come già spiegato, 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 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*. In questo modulo il provider fornisce informazioni sul proprio sistema, categorizzandolo sulla base delle direttive contenute nel documento NIST SP 800-60 V2, 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.

Oltre alle finalità precedentemente esposte, il prodotto sviluppato in questo lavoro di tesi punta a supportare il processo di verifica dei requisiti tecnici richiesti per la *readiness*. In particolare si vogliono fornire controlli di sicurezza per i punti 3, 4, 5, 11 e 12. I restanti requisiti, di carattere meramente procedurale, saranno invece implementati separatamente sotto forma di questionario.

3.5 Documenti aggiuntivi

5.3. After Acceptance into the FedRAMP Program After acceptance into the FedRAMP JAB Provisional Authorization process, there are certain documents requiring submission. The FedRAMP PMO created templates for documents that the CSP must edit and modify based on the security controls implemented in its system. All templates are available on the FedRAMP website. Guidance on how to fill out the various templates and develop the required documents are described in the sections that follow.

After acceptange in to the program, there are other documents that have to be submitted for which templates are provided. Those are discussed in the next slides.

FIPS 199 Allow the CSPs to categorize and record the sensitivity level of the system according to the NIST SP 800-60 Revision 1 Volume 2. IaaS and PaaS providers must select information types from section C.3.5

E-Authentication Template An e-Authentication template is provided for performing an e-Authentication analysis. The objective is to ensure that the CSP has implemented technical solutions that matches the sensitivity of the system and the data it stores and the processes. The guidance document is NIST SP 800-63, Revision 1, Electronic Authentication Guidance. e-Authentication template is provided on FedRAMP's website.

Privacy threshold Analysis Privacy impact assessment CSPs are required to fill out a Privacy Threshold Analysis (PTA). FedRAMP provides a PTA/PIA template, that consists of four short questions designed to determine if the system qualifies as a Privacy Sensitive System. If so, then a Privacy Impact Assessment (PIA) is also required. In accordance with NIST SP 800-144, organizations are ultimately accountable for the security and privacy of data held by a cloud provider

on their behalf. CSPs must consider whether their security controls (for their own support staff) use PII for any authentication mechanisms (e.g. fingerprint scanners, hand scanners, iris scanners). If the CSP system requires PII from agency customers, for example, to enroll users in authentication mechanisms, then the impending collection of that PII on first use by agency customers should be made known. When performing the independent security assessment, the 3PAO will review the PTA and/or PIA to make certain determinations and findings that are incorporated into the Security Assessment Report (SAR).

CTW Template

The purpose of the Control Tailoring Workbook (CTW) template is to summarize the exception scenarios of the service offering for prospective agency customers. This template is completed after the System Security Plan has been completed, and must be consistent with information found in the System Security Plan.

CIS Template Complete the Control Implementation Summary (CIS) template to indicate the implementation status of the controls for the system. CSPs need to indicate in the CIS the entity responsible to implement and manage the control. In some cases, implementation and management of a control may require joint ownership by the CSP and the customer agency The CIS is a living document and updates are expected throughout the development of the System Security Plan.

User guide CSPs must provide a User Guide that explains how prospective users (government agencies) will use the system. If the system has a self-service control panel, the User Guide must explain clearly how to use the control panel. Submit the User Guide with the System Security Plan.

Components, boundaries, architecture The System Security Plan template documents and describes how all required security controls are implemented. The CSP system likely has multiple components. Each component needs to be named and described in Section 9.2 of the System Security Plan. Wherever possible, use component names that are already familiar and used within the organization. Components may be described by a unique name (e.g. "Home Base") or by functionality (e.g. "the Hypervisor"). Discussing virtualization This section includes general guidance on discussing virtualization in System Security Plans. There are numerous ways that virtualization can be implemented, and many different virtualization products. The FedRAMP PMO does not make recommendations on virtualization models or products. Whatever virtualization architecture model is used, CSP documentation in all aspects must be clear about which components are parts of the physical host system which components are parts of virtual abstraction layers When discussing the functionality of different components, indicate whether the component is a standard host operating system guest (virtual) operating system. For each physical host that provides the capability to implement guest systems, discuss whether the virtualization technique is based on: hosted virtualization bare metal virtualization

Guest operating systems can be deployed in several ways: the CSP provides a self-service menu driven control panel where customers can setup and configure their own virtual machines within a controlled environment the CSP installs and configures unique virtual machines instances directly for the customer thereby

eliminating the need for a self-service portal. When discussing administration, access control, and configuration settings of virtual machines, CSPs need to be clear about whether their service offers a self-serve solution or a CSP administered solution. The roles and authorizations associated with both of these solutions must be detailed in the System Security Plan (Table 9-1) User Roles and Privileges. Network components can also be virtualized. When discussing a network component (or device) that is a virtual component, be clear about the fact that the item discussed is virtual and not physical (VLANs, Virtual Ethernet Modules, Virtual Firewalls, Virtual Switches, Virtual Distributed Switches, Virtual Security Gateways, Virtual Routers, NAT Virtual Interfaces).

Discussing virtualization - boundaries and inherited controls When describing the boundaries of the cloud system, it is important to accurately and clearly articulate where the cloud service layers begin and end. If a PaaS service provider is building its service on top of an IaaS service provider, the PaaS provider needs to ensure that their security control boundaries begin where the IaaS security control boundaries end. Alternately, a SaaS provider must understand where the PaaS security control boundaries end. The security controls for an upper layer service needs to begin where the lower layer security controls end. There are many possible configurations for layering security and FedRAMP does not make recommendations on specific service models. When discussing boundaries, include information on how different tenants are separated from each other in a multi-tenant environment.

Questions to consider when describing boundaries: Will the boundaries leverage any existing Provisional Authorizations? What is the definition of a tenant? For the service offering, will multiple tenants share the same VLAN(s)? Are there controls that prevent VLAN hopping? Are virtual machine zones on unique network segments isolated? Are separate physical network adapters used to isolate virtual machine zones? Is layer-2 isolation performed? Is isolation through traffic encapsulation used? Do port groups define any boundaries? If port groups are used, are they all in the same layer-2 domain or do they span multiple layer-2 domains? Are multiple Network Interface Cards (NICs) bonded together? How do firewalls provide isolation between tenants?

Questions to consider when describing boundaries: How does router ACLs provide isolation between tenants? Are IPsec tunnels used to define boundaries? Is sharding used? Are network filters used that control what packets are sent to or from a virtual machine? Are network zones used? If yes, how are zones defined? Will U.S. federal agencies be multi-tenanted with non-government entities? Are NAT virtual interfaces (NVI) or domain specific NAT configurations used? How does NAT play a role in containing network traffic within the boundary? What kind of NAT is used? (e.g. static, dynamic, overloading, overlapping) Are NAT IP pools used? Are geo IP location boundaries used? Define the geographic location (City, State) where customer data is stored? Will it be possible for agency tenants to know the geographic location (City, State) where their data is stored?

Discussing live migrations

Live migrations of virtual machines have the potential to confuse a common understanding of the information system boundaries. Therefore, when describing boundaries, it is important to discuss the live migration strategy for the

information system. Live migrations have the ability to move an entire virtual machine to another host or instead, move a virtual machine's data store (configuration file and virtual disks) to another physical host without actually moving the virtual machine. Complicating this, it is also possible to move and store a virtual machine's configuration files, and disks in separate locations. The FedRAMP PMO does not make recommendations on live migration strategies. Whatever the live migration strategy is, be clear as to how live migrations are managed. IP addresses declared within the boundary must remain protected by the security controls noted in the System Security Plan even if the IP addresses are moved around. Questions to consider in the discussion of live migration: Are live migrations performed manually, or scheduled and automated? If live migrations are automated, what are the rules that govern the migration?

Discussing storage components

In the description of system components, include information about storage components that are inside the boundary. If using a fiber channel storage array, insert a diagram that shows how the storage connects to the fiber channel fabric and include the switches in the diagram. Questions to consider when describing storage components: Does the system use Direct Attached Storage (DAS), Network Attached Storage (NAS), or Storage Area Networks (SANs)? If using a SAN, what is used to connect hosts in a cluster (fiber channel or iSCSI)? Which fiber channel or iSCSI connections are considered within the boundary? Are different types of storage devices used on different network segments? Are clusters used? How many hosts are on a cluster and which clusters are in the boundary? Do the storage devices use a multipath environment? Are the storage devices set up to be persistent or non-persistent?

Data flow Diagram

Describes how network traffic flows through the platform and offering. A data flow diagram focuses more on the direction of the network traffic and less on the actual network topology. However, certain components of the system's network topology need to be included to illustrate the direction that the network traffic flows through the system.

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

3.6.1 Categorie dei controlli

3.6.2 Controlli procedurali

AC-1,AC-2(a),AC-2(b),AC-2(c),AC-2(d),AC-2(e),AC-2(f),AC-2(g),AC-2(h),AC-2(i),AC-2(j),AC-2(7)(a),AC-5,AC-6(1),AC-8(b),AC-11(b),AC-17(a),AC-17(b),AC-17(4),AC-17(5),AC-17(6),AC-19(b),AC-19(1),AC-19(2),AC-19(3),AC-19(4)(a),AC-19(4)(b),AC-20(a),AC-20(b),AC-20(1)(a),AC-20(1)(b),AC-20(2),AC-21(a),AC-21(b),AC-22(a),AC-22(b),AC-22(c),AC-22(d),AC-22(e),AU-2(b),AU-6(a),AU-6(b),AU-6(3),CA-1(a),CA-1(b),CA-2(a),CA-2(b),CA-2(c),CA-2(d),CA-2(1),CA-2(2),CA-3(a),CA-3(b),CA-3(1),CA-3(2),CA-

5(a),CA-5(b),CA-6(a),CA-6(b),CA-6(c),CM-3(a),CM-3(b),CM-3(c),CM-3(d),CM-3(e),CM-3(f),CM-3(4),CM-7(3),IA-1(a),IA-1(b)

3.6.3 Controlli automatizzabili

i

AC-3(4),AC-14(a),AC-14(b),AC-14(1),AC-17(c),AC-17(d),AC-17(e),AC-18(b),AC-18(c),AC-18(4),AC-19(c),AC-19(f),AC-19(g),AU-3,AU-8,AU-9(4)(b),AU-12(b),CM-8(3)(a),IA-2,IA-5(e),IA-6,IA-8"

AC-2(1),AC-7(a),PM-11,PM-10,PM-9,PM-8,PM-7,PM-6,PM-5,PM-4,PM-3,PM-2,PM-1,AC-17(3),AC-18(a),AC-18(b),AC-18(5),AC-21(1),CP-10(2),AT-1(a),AT-1(b),AT-2,AT-3,AT-3(2),AT-4(a),AT-4(b),AT-2,AT-2(1),AT-3,AT-3(1),AT-3(2),AT-5,AU-1(a),AU-1(b),AU-2(3),AU-6(1),AU-6(3),AU-7,AU-7(1),CA-7(a),CA-7(b),CA-7(c),CA-7(d),CA-7(1),CA-7(2),CM-1(a),CM-1(b),CM-2,CM-2(1)(a),CM-2(1)(b),CM-2(1)(c),CM-2(2),CM-2(5)(a),CM-2(5)(b),CM-3(2),CM-4,CM-4(2),CM-5,CM-5(2),CM-5(5)(b),CM-6(a),CM-6(b),CM-6(c),CM-6(1),CM-7(1),CM-8(a),CM-8(b),CM-8(c),CM-8(d),CM-8(e),CM-8(1),CM-8(4),CM-8(5),CM-8(6),CM-9(a),CM-9(b),CM-9(c),CP-1(a),CP-1(b),CP-2(a),CP-2(b),CP-2(c),CP-2(d),CP-2(e),CP-2(f),CP-2(1),CP-2(2),CP-3,CP-4(a),CP-4(b),CP-4(1),CP-6,CP-6(1),CP-6(2),CP-7(a),CP-7(b),CP-7(1),CP-7(2),CP-7(3),CP-7(5),CP-8,CP-(8)(1)(a),CP-8(1)(b),CP-8(2),CP-9(a),CP-9(b),CP-9(c),CP-9(d),CP-9(1),CP-9(3),CP-10,CP-10(2),CP-10(3),IA-4(a),IA-4(b),IA-4(c),IA-4(d),IA-4(e),IA-4(4),IA-5(a),IA-5(d),IA-5(3),IA-5(6),IA-5(7),IR-1(a),IR-1(b),IR-2(a),IR-2(b),IR-3,IR-4(a),IR-4(b),IR-4(c),IR-4(1),IR-6,IR-7,IR-7(1),IR-7(2),IR-8(a),IR-8(b),IR-8(c),IR-8(d),IR-8(e),MA-1(a),MA-2(a),MA-2(b),MA-2(c),MA-2(d),MA-2(e),MA-2(1),MA-3,MA-3(1),MA-3(2),MA-3(3),MA-4(a),MA-4(b),SI-1(a),SI-1(b),SI-2(a),SI-2(b),SI-2(c),SI-3(a),SI-3(b),SI-3(c),SI-3(d),SI-3(1),SI-1(2),SI-1(3),SI-4(a),SI-4(b),SI-4(c),SI-4(d),SI-4(e),SI-4(2),SI-4(4),SI-4(5),SI-4(6),SI-5(a),SI-5(b),SI-5(c),SI-5(d)

3.7 FedRAMP in Amazon AWS

Certificazioni di conformità di AWS Per visualizzare i report di conformità AWS, utilizza AWS Artifact, un portale self-service per l'accesso on demand. Per istruzioni sull'utilizzo di Artifact, guarda il nostro video sulla home page Artifact. In caso di domande, compila il modulo seguente per essere contattato da un rappresentante aziendale di Amazon Web Services.

AWS ha soddisfatto i controlli di sicurezza previsti dal programma FedRAMP (basati su NIST SP 800-53), ha impiegato modelli predefiniti per i pacchetti di sicurezza pubblicati nel repository FedRAMP, ha sostenuto la valutazione di un'entità di controllo indipendente accreditata e soddisfa i requisiti di monitoraggio continuo del programma FedRAMP. I sistemi conformi sono i seguenti:

AWS GovCloud (US) ha ricevuto un'autorizzazione provvisoria del Joint Authorization Board (JAB P-ATO) e diverse autorizzazioni operative per il livello di impatto High. I servizi coperti dall'autorizzazione provvisoria del Joint Authorization Board nella regione AWS GovCloud (US) sono disponibili nella pagina relativa alla copertura di conformità dei servizi AWS. Per consultare un elenco completo delle agenzie che hanno rilasciato autorizzazioni operative per la regione AWS GovCloud (US), visita la pagina FedRAMP Compliant Systems.

Regioni AWS Stati Uniti occidentali/orientali: hanno ricevuto diverse autorizzazioni operative per il livello di impatto Moderate. I servizi coperti dalle autorizzazioni provvisorie per le regioni AWS Stati Uniti occidentali/orientali sono disponibili nella pagina relativa alla copertura di conformità dei servizi AWS. Per consultare un elenco completo delle agenzie che hanno rilasciato autorizzazioni operative per le regioni AWS Stati Uniti occidentali/orientali, visita la pagina FedRAMP Compliant Systems.

La conformità con il programma FedRAMP farà aumentare i costi dei servizi AWS? No, la conformità al programma FedRAMP da parte di AWS non provocherà alcun aumento dei costi in alcuna regione.

Quali regioni AWS sono coperte? AWS ha ottenuto due Agency ATO FedRAMP separate, una a copertura della regione AWS GovCloud (Stati Uniti), l'altra delle regioni Stati Uniti occidentali e orientali.

I clienti di AWS possono richiedere l'accesso ai pacchetti di sicurezza FedRAMP di AWS tramite il FedRAMP PMO o all'account manager delle vendite di AWS.

Le agenzie governative statunitensi possono richiede l'accesso al pacchetto di sicurezza FedRAMP di AWS tramite il FedRAMP PMO compilando un modulo di richiesta di accesso al pacchetto e inviandolo all'indirizzo info@fedramp.gov, oppure contattando l'account manager delle vendite di AWS.

I partner di AWS e i clienti potenziali possono anche richiedere l'accesso al pacchetto di sicurezza FedRAMP di AWS per i partner contattando l'account manager delle vendite di AWS.

Un funzionario autorizzato di un'agenzia può impiegare uno dei pacchetti di sicurezza FedRAMP di AWS ed esaminarne la documentazione per decidere in base ai rischi di assegnare un'autorizzazione operativa (ATO) ad AWS. Le agenzie sono responsabili per il rilascio delle autorizzazioni operative in AWS e in generale per le autorizzazioni dei componenti dei loro sistemi non coperte dall'autorizzazione operativa di AWS. Per ulteriori informazioni sul modello di responsabilità condivisa di AWS, contatta l'account manager delle vendite di AWS.

Impiegando le funzionalità di sicurezza offerte da AWS e dall'ecosistema di fornitori, potrai controllare e monitorare la creazione di sistemi disponibili in modo che integrino le policy di gestione della sicurezza, della privacy e o del rischio dell'agenzia.

Scoprilo leggendo cosa sono stati in grado di realizzare clienti, partner e integratori di sistemi grazie ad AWS:

Blog

Appian Cloud sfrutta l'infrastruttura di Amazon Web Services e l'autorizzazione FedRAMP. Leggi tutto

Casi di studio AWS

Dipartimento di Stato degli Stati Uniti

US Food and Drug Administration (FDA)

US Centers for Disease Control and Prevention (CDC)

NASA/JPL: Desert Research and Training Studies

NASA/JPL e Amazon SWF

NASA/JPL: la missione Curiosity su Marte

All'interno del documento Concept of Operations (CONOPS) del programma FedRAMP, quando un'autorizzazione è stata assegnata, il livello di protezione di un CSP viene monitorato secondo il processo di valutazione e autorizzazione. Per ottenere una nuova autorizzazione di una ATO FedRAMP da un anno all'altro, i CSP devono monitorare i propri controlli di sicurezza, effettuarne delle valutazioni periodiche e dimostrare che la sicurezza della loro offerta di servizi mantiene sempre un livello accettabile. La valutazione della continuità della conformità è responsabilità delle agenzie federali che impiegano il programma di monitoraggio continuo FedRAMP, nonché dei funzionari autorizzati e relativi team. I funzionari autorizzati e i relativi team esamineranno gli artefatti forniti tramite il processo di monitoraggio continuo FedRAMP di AWS, oltre alle prove di implementazione di controlli specifici della singola agenzia che fanno parte dei requisiti esterni ai controlli FedRAMP, in modo continuo. Per ulteriori informazioni, consulta la policy o il programma di sicurezza dei sistemi informatici della tua agenzia.

Capitolo 4

Moon Cloud: un framework per il monitoraggio e la verifica della sicurezza

4.1 Introduzione

.

4.2 Architettura e componenti

.

.

.

.

4.3 Moon Cloud come strumento di verifica della compliance

.

4.3.1 Controlli di sicurezza

.

.

.

.

4.3.2 Regole di valutazione

.

.

.

.

Capitolo 5

Implementazione dei controlli di sicurezza FedRAMP in Moon Cloud

5.1 Controlli automatici

5.1.1 Una sezione per ogni security control implementato

5.2 Controlli ad interazione umana

5.2.1 Questionari per l'assessment dei processi di business

Capitolo 6

Validazione del framework

6.1 Deployment di Moon Cloud

6.2 Sicurezza del deployment

6.2.1 Caratteristiche del deployment

6.2.2 Confidenzialità

6.2.3 Integrità

6.2.4 Disponibilità e affidabilità

6.2.5 Data remainance

6.3 Scalabilità e Prestazioni

6.3.1 una sezione per ogni security control eseguito

Capitolo 7

Conclusioni e sviluppi futuri

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] 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.

[35] SP NIST. «NIST SP 800-53». In: *Recommended Security Controls for Federal Information Systems* (2003), pp. 800–53.