CSA IT Italy Chapter — cloud security alliance℠

Cloud Security Alliance Italy Chapter

Portabilità, Interoperabilità e Sicurezza Applicativa

Novembre 2012

Document Sponsor

Allied Telesis

Introduzione

A livello globale, la ricerca in questo campo è soprattutto concentrata sull'eliminazione delle barriere tecniche che tendono a vincolare i Cloud Service Consumer (CSC) a un dato Cloud Service Provider (CSP) e sullo sviluppo di applicazioni sicure basate su infrastrutture cloud. Il tema, trattato dal "CSA Working Group 4: Portability, Interoperability and Application Security", è di particolare importanza per l'Italia in quanto realtà composta prevalentemente da CSC per la maggior parte costituiti da piccole e medie imprese (PMI), che hanno poco potere contrattuale nei confronti dei fornitori Cloud e minor accesso a competenze tecniche specifiche per l'orientamento nella scelta dei fornitori. Inoltre, gli altri attori del mercato cloud che possono trarre benefici dall'uso di approcci standard sui temi di portabilità, interoperabilità e sicurezza applicativa sono i Cloud Service Developer, i Cloud Service Distributor e i Cloud Service Broker, figure in parte già presenti in Italia e che probabilmente vedranno un ulteriore sviluppo nei prossimi anni.

A livello europeo, infine, c'è una grande attenzione al tema della portabilità e dell'interoperabilità, per i quali si attendono a breve interessanti sviluppi, come anticipato dall'attuale Vice Presidente della Commissione Europea, Neelie Kroes, che ne ha fatto un proprio cavallo di battaglia.

Inoltre, le attività di ricerca del CSA Italy Chapter in questo campo sono finalizzate a recepire, approfondire e contestualizzare quanto prodotto da CSA global e da altre iniziative internazionali quali ad esempio Open Data Center Alliance[1] e SIENA[2] (per la parte di portabilità e interoperabilità) e OWASP[3] (per quanto riguarda la sicurezza delle applicazioni), proponendo il riconoscimento da parte di vari organismi nazionali pubblici e privati (DigitPA, Consip, Confindustria, ABI, ecc.) di approcci standard direttamente o indirettamente derivati da queste ricerche.

Dal punto di vista delle risorse utilizzate, è bene ricordare che questo documento è stato realizzato grazie alla collaborazione dei nostri soci che hanno espresso una grande disponibilità e una grande competenza sui temi trattati e che hanno messo a disposizione del Gruppo di Lavoro tempo e risorse personali di primaria importanza.

Il tema della sicurezza applicativa è stato affrontato con la diretta collaborazione del capitolo italiano di OWASP, che ha messo a disposizione un team con cui abbiamo intenzione di proseguire con approfondimenti e nuove tematiche.

Per il prossimo futuro, infine, CSA Italy Chapter si propone di approfondire i temi qui trattati avviando dei lavori di ricerca che vadano direttamente incontro alle esigenze dei CSC italiani (soprattutto nella PA e nelle PMI), con la proposizione di requisiti e approcci che fissino ad esempio:

[1] www.opendatacenteralliance.org
[2] www.sienainitiative.eu
[3] www.owasp.org

- le tipologie di API e “data format” da utilizzare;
- le modalità con le quali vengono forniti i dati e, se del caso, il codice applicativo;
- le modalità di erogazione del supporto alla migrazione;
- i tempi, gli effort previsti e gli eventuali step transitori per le migrazioni;
- il ciclo di vita sicuro per le applicazioni;
- i principali rischi, e relative contromisure, per le applicazioni cloud.

Dato che questi temi potranno essere di volta affrontati sia su un fronte prettamente tecnologico sia un fronte più contrattuale/organizzativo, si potranno approfondire i vari aspetti con gruppi di lavoro indipendenti composti da soci con diversa estrazione e competenze. L’obiettivo finale, infatti, è quello di creare una community attiva sulla ricerca e sui temi “caldi” del cloud che si proponga come interlocutore privilegiato nei confronti degli enti e degli attori che svolgono un ruolo di guida nello sviluppo dell’Information Technology del nostro paese.

Indice

Si ringrazia

Coordinatore del Gruppo di Lavoro

Matteo Cavallini

Autori/Contributori

Matteo Cavallini,

Alberto Manfredi

Yvette Agostini,

Domenico Catalano,

Mario Cola,

Antonio Parata (OWASP),

Francesco Beatino,

Eugenio De Santis

Document Sponsor

ALLIED TELESIS

CSAIT Staff

Paolo Foti

1.0 Portabilità e interoperabilità

La portabilità e interoperabilità in ambito cloud computing possono essere considerate due caratteristiche fortemente correlate al concetto di resilienza per l'azienda che fruisce di servizi di cloud computing. La valutazione dei rischi connessi a progetti in a questo specifico ambito non può perciò prescindere dalla valutazione delle problematiche connesse a questi argomenti.

Il tema della portabilità di dati ed applicazioni tra diversi fornitori di servizi cloud è attualmente percepito come molto importante per gli utenti finali, in quanto la situazione presente è di sostanziale difficoltà nel conseguire questo obiettivo ed i fornitori di servizi cloud non sono, nella maggioranza dei casi, propensi a facilitare la portabilità in quanto essa viene percepita come un fattore che faciliterebbe la competizione, in particolare sui prezzi.

1.1 Definizione di portabilità

Nell'ambito del cloud computing, per portabilità dei servizi, si intende la possibilità di effettuare una migrazione "semplice" delle applicazioni, macchine virtuali e dei dati da un ambiente cloud ad un altro. Affinché ciò sia fattibile, è necessario che l'ambiente cloud di partenza e di arrivo siano caratterizzati dall'essere interoperabili, ovvero che l'ambiente applicativo sia effettivamente replicabile presso diversi fornitori di servizi cloud. La portabilità può però assumere anche una molteplicità di aspetti diversi: è un concetto che, ad esempio, è riferibile anche al caso della confederazione di cloud privati nell'ambito di una piattaforma di gestione unificata, presso un fornitore di servizi cloud pubblici. Per comprendere appieno il significato e la portata del concetto di portabilità in ambito cloud devono essere considerati anche gli aspetti meno tecnologici quali ad esempio quelli connessi al trasferimento di licenze e di diritti d'uso dei software e dei dati.

Proprio per illustrare in maniera diretta e semplice questi aspetti tenendo in debito conto le relazioni che esistono tra le varie componenti nell'ambito dei servizi cloud, il Jericho Forum ha elaborato una rappresentazione grafica che viene di seguito riportata:

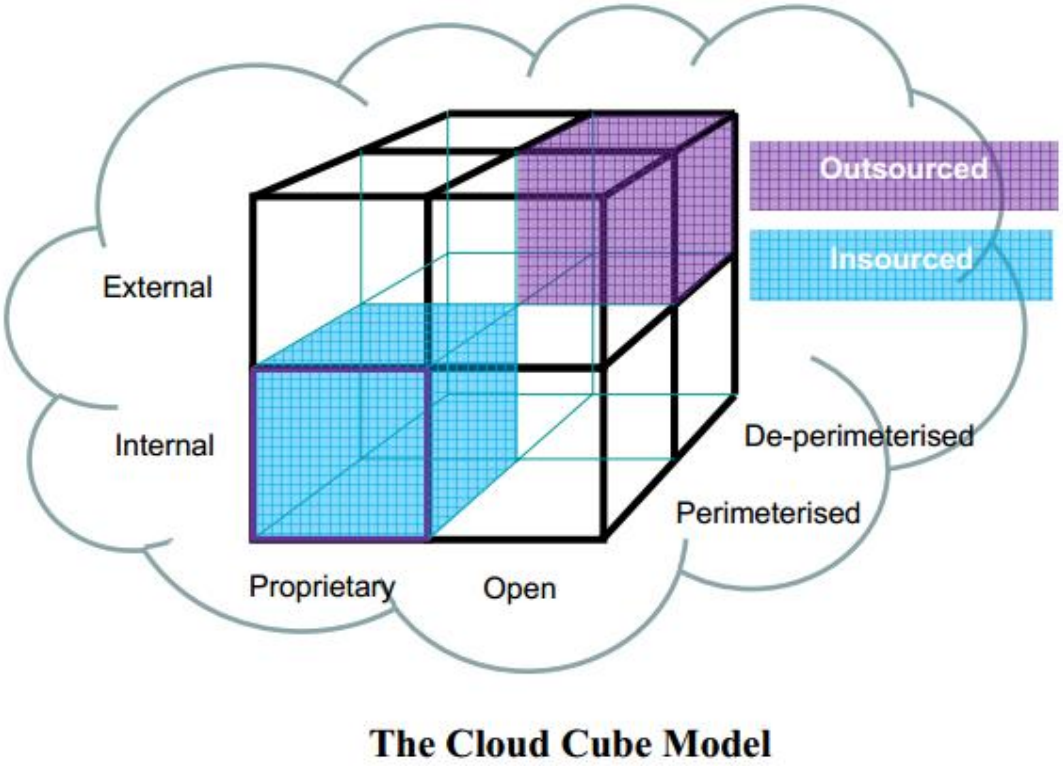

Figura 1: Modello cubico del cloud secondo Gericho forum[4]

Nella figura, l'asse "Proprietary-Open" tratta in maniera specifica del tema della portabilità e interoperabilità e, in generale, il conseguimento della portabilità è generalmente dipendente dal fatto che i servizi cloud appartengano allo stesso ottavo di spazio (ottante) del modello cubico del cloud computing, infatti nei servizi cloud che ricadono in ottanti differenti del cubo, la portabilità dei servizi medesimi è condizionata ad un passaggio intermedio.

1.2 Definizione di interoperabilità

L'interoperabilità, invece, consiste nella possibilità di condividere gli stessi strumenti di gestione, macchine virtuali ed altre risorse cloud, tra una pluralità di fornitori di servizi e piattaforme di cloud computing. La portabilità dovrebbe rendere i dati e codice "comprensibili" anche da un sistema ricevente, messo a disposizione da un diverso fornitore di servizi cloud, indipendentemente dalle specifiche caratteristiche delle piattaforme sia hardware che software utilizzate.

La necessità di avere servizi cloud interoperabili nasce principalmente dall'esigenza di evitare, per quanto possibile, situazioni di lock-in, considerando che può rendersi necessario migrare ad altri fornitori di cloud (a

[4] Fonte: https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

causa ad esempio dell'insoddisfazione per i livelli di servizio, o a causa della cessazione del servizio del fornitore, dei cambiamenti strategici di business che possono aver modificato le necessità di ricorso al cloud, o, infine, la scelta di migrare verso nuovi e migliori servizi erogati da altri CSP). In particolare, può essere opportuno prevedere un piano di trasferimento dei dati da un cloud provider ad un altro, tenendo in considerazione i costi ad esso associati in diversi scenari di crescita dei dati gestiti. Una situazione analoga, anche se maggiormente articolata, si viene a creare quando si tratta di trasferire non solamente dati statici ma intere applicazioni con le relative logiche e componenti. La standardizzazione ed i formati cosiddetti aperti sono quindi da considerare come fattori abilitanti sia per l'interoperabilità che per la portabilità. Quindi queste due caratteristiche dovrebbero essere integrate già a livello progettuale; ma attualmente la problematica principale è la rapida evoluzione del settore, governato dall'offerta dei fornitori cloud, alcuni dei quali lavorano in quasi monopolio, mentre il lavoro di standardizzazione in questo settore è ancora in definizione. Ad esempio IEEE ha varato da poco un gruppo di progetto relativo alla portabilità (http://standards.ieee.org/news/2011/cloud.html) per la redazione di due standard ad essa relativi: P2301™ Draft Guide for Cloud Portability and Interoperability Profiles e IEEE P2302™, Draft Standard for Intercloud Interoperability and Federation che si pensa possano porre le basi per standard effettivamente condivisi e ampiamente utilizzati.

1.3 I rischi correlati

I rischi legati alla mancanza di portabilità e interoperabilità sono generali e riguardano ampi settori dell'informatica; nei servizi cloud, però, vengono ad essere amplificati e resi ancor più importanti per i CSC. Infatti, servizi aperti e condivisi tra diversi clienti quali, appunto, i servizi cloud, aumentano le necessità di implementazione di robusti meccanismi per ripristinare il servizio anche all'esterno della infrastruttura cloud che li ospita. Tutto ciò implica che, in questi ambienti, i livelli di rischio siano maggiori rispetto ai tradizionali ambienti elaborativi. Inoltre, la portabilità e l'interoperabilità sono caratteristiche essenziali sia per cogliere appieno i grandi vantaggi legati alla flessibilità e all'elasticità dei servizi cloud, sia per garantire che sia sempre possibile:

- internalizzare nuovamente un servizio che era stato spostato su una piattaforma cloud esterna,
- cambiare il proprio CSP con un altro che offre servizi migliori o SLA più consoni alle proprie esigenze
- esternalizzare un servizio cloud sviluppato su una cloud privata o di community.

Come ricordato anche nella "Security Guidance" di CSA[5] e nella versione italiana della Guidance 2.1 queste problematiche sono principalmente legate ad alcune attuali lacune negli standard e a un'inadeguata selezione dei fornitori con relativa perdita di trasparenza in termini di utilizzo dei servizi.

Inoltre, ENISA, nel documento "Cloud Computing - Benefits, Risks and Recommendations"[6] attribuisce al rischio di lock-in un'alta probabilità in quanto allo stato attuale, l'offerta di servizi non garantisce strumenti, procedure, formati dati ed interfacce dei servizi adeguatamente standardizzati.

[5] cloudsecurityalliance.org/wp-content/themes/csa/guidance-download-box.php

Effettuando poi, un'analisi suddivisa per tipologia di modello di erogazione dei servizi cloud, emerge che per gli utenti di servizi SaaS la problematica maggiore consiste nell'estrazione della banca dati del fornitore. Infatti, nel caso in cui il CSP non abbia predisposto e reso disponibili strumenti per l'estrazione dei dati, o se questi strumenti non operano delle estrazioni in un formato standard, è necessario sviluppare meccanismi opportuni, con un notevole aumento di costi per la migrazione e con tempistiche ed esiti finali poco prevedibili a priori. Per le applicazioni sviluppate su PaaS, invece, il rischio maggiore risiede principalmente nelle API. Infatti, le problematiche di lock-in sorgono quando il codice utilizza API non standard (proprietarie o con sostanziali modifiche e personalizzazioni) da parte del fornitore. In questo caso potrebbero aumentare drasticamente i costi di riscrittura del codice in caso di migrazione, o di sviluppo di interfacce ad hoc per la comunicazione con servizi ospitati da altri fornitori. E' da notare che, analogamente a servizi SaaS, anche nel PaaS esistono problematiche legate alla portabilità delle informazioni su cui tuttavia l'utente ha la possibilità di esercitare un maggior controllo. Infine, nei servizi IaaS le principali preoccupazioni sorgono nel caso in cui il formato con cui sono rappresentate le macchine virtuali (tipicamente le partizioni del sistema operativo e metadati che descrivono le componenti hardware virtualizzate) non sia standard. Un'altra problematica riguarda lo storage in modalità as a Service, infatti l'elevato numero di dati salvati in tali infrastrutture rende maggiormente complicata la loro migrazione e le policy di gestione dei permessi di accesso ai dati potrebbero essere significativamente differenti da fornitore a fornitore.

Il rischio connesso alla mancanza di portabilità e interoperabilità è quindi da considerarsi elevato in termini di impatto e, al momento, in assenza di standard e best practice ampiamente consolidati e condivisi, è da considerarsi anche molto probabile. In virtù di queste considerazioni, quindi, è bene che nei contratti di servizi cloud i CSC verifichino l'adozione di specifiche clausole che diano idonee garanzie del raggiungimento di livelli di rischio compatibili con quelli prescelti in fase di analisi.

1.4 Gli obiettivi da raggiungere

Nel 2011, la Open Data Center Alliance[7], un consorzio IT che riunisce i leader di mercato allo scopo di trovare un approccio lato utente, di lungo periodo e compatibile con i requisiti per i data center, ha reso pubblici i primi requisiti per il cloud computing, documentati in 8 modelli di utilizzo (ODCAU) che prioritizzano i requisiti secondo il punto di vista degli utilizzatori e che hanno lo scopo di contribuire a risolvere le problematiche di adozione del cloud computing. Gli ambiti considerati sono: SecureFederation, Automation, Common Management & Policy, and Transparency.

Nell'ambito dello usage model dedicato all'Automation viene trattato anche il caso della "Virtual Machine Interoperability"[8] che, sostanzialmente, parte dal presupposto di base che le macchine virtuali create in un hypervisor e/o che girano su una determinata piattaforma cloud possano essere spostate in una differente piattaforma e/o hypervisor, pur continuando a erogare i propri servizi senza modifiche sostanziali. Nel

[6] www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
[7] www.opendatacenteralliance.org
[8] www.opendatacenteralliance.org/docs/VM_Interoperability_Rev_1.1_b.pdf

documento vengono quindi forniti alcuni strumenti di base per l'analisi dei possibili scenari e l'individuazione dei requisiti idonei affinché venga garantita l'interoperabilità delle macchine virtuali in ambito cloud.

Come precedentemente ricordato anche CSA nella Security Guidance sottolinea l'importanza degli obiettivi da raggiungere nel campo della portabilità ed interoperabilità per garantire che le migrazioni di servizi cloud verso soluzioni cloud pubbliche, private o ibride siano efficaci ed efficienti. Infatti, qualora questi elementi venissero trascurati in fase di progetto, le conseguenze derivanti potrebbero ridurre o addirittura annullare gli auspicati benefici derivanti dalla migrazione stessa e generare problemi di costosa soluzione e/o ritardi di progetto. In particolare ci si potrebbe trovare a dover gestire situazioni di:

- lock-in (relativamente all'applicazione, alla piattaforma o al fornitore) con una sostanziale riduzione delle capacità di orientarsi verso un'altra offerta cloud o un altro fornitore;
- malfunzionamenti delle applicazioni spostate su una infrastruttura cloud alternativa, a causa dell'incompatibilità tra le piattaforme, le applicazioni o i servizi erogati;
- reingegnerizzazione del processo e/o cambiamenti nel codice per conservarne l'originaria operatività;
- cambiamenti inattesi dei dati causati dalla carenza di "*data format*" portabili ed interoperabili;
- modifiche sostanziali alle applicazioni e/o software di gestione;
- manifestazione di lacune di sicurezza e/o vulnerabilità latenti causate da differenze nelle politiche di sicurezza, nella gestione delle chiavi o nella protezione dei dati, da parte di differenti fornitori cloud.

Infine, dal punto di vista dell'interoperabilità, grande attenzione deve essere dedicata alle Cloud Provider API, ossia alle interfacce di programmazione che permettono all'utente di interagire con i vari servizi erogati da un CSP attraverso servizi di tipo REST e/o SOAP. Le Cloud API sono, infatti, divise in 3 principali segmenti: Infrastruttura, Servizi ed Applicazioni rispettivamente per i modelli IaaS, PaaS e SaaS.

Le API d'infrastruttura (IaaS) consentono la modifica delle risorse disponibili su cui far operare le applicazioni. Le funzioni includono il provisioning (creazione, modifica, cancellazione delle componenti, ad es. macchine virtuali) e la configurazione (assegnazione e cambiamento di attributi dell'architettura quali la sicurezza e le configurazioni di rete).

Le API di servizi (PaaS) forniscono un'interfaccia in una specifica capacità fornita da un servizio esplicitamente creato per abilitare la capacità. Database, messaging, web portal, storage sono tutti esempi di API di servizi.

Le API di Applicationi (SaaS) forniscono metodi per interfacciare ed estendere le applicazioni nel Web. Le API di Applicazioni si collegano ad applicazioni come CRM, ERP, social media e help desk.

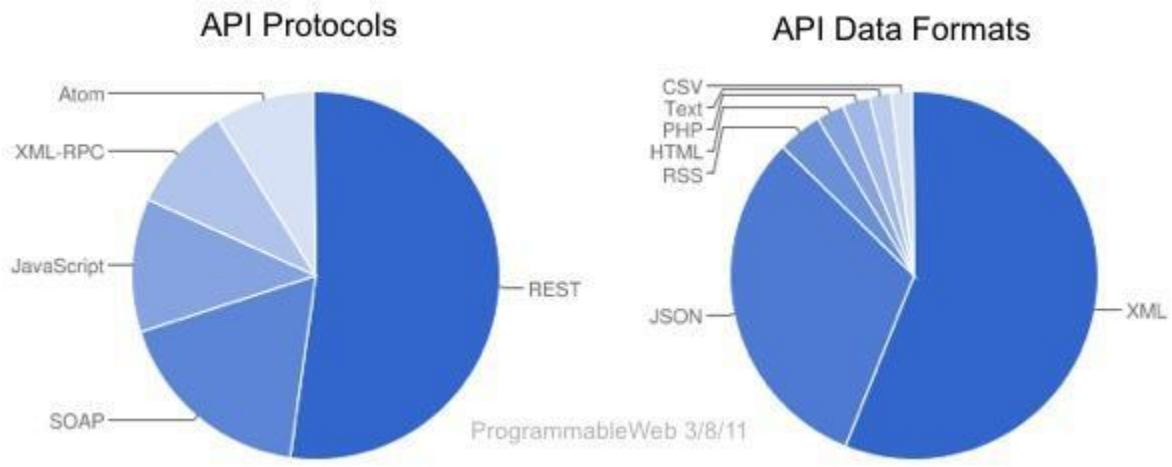

Figura 2: Tipologie e protocolli formati dalle API

I grafici mostrati in Figura 2 descrivono la tendenza e l'orientamento delle tipologie dei protocolli e del formato dati delle API.

E' da sottolineare, infine, l'esistenza di API multi-piattaforma consentono di accedere a servizi di diversi provider senza la necessità di introdurre modifiche nel codice applicativo.

Questo quadro contribuisce a chiarire l'importanza di un'accurata e puntuale definizione dei requisiti di portabilità e interoperabililtà per le API nei contratti di servizi cloud.

Da ultimo, infine, non deve essere trascurato l'aspetto puramente contrattuale riferito alle clausole e agli SLA dedicato ai servizi a supporto delle attività di migrazione. Infatti, è possibile intuire facilmente quanto possano essere importanti adeguati livelli di consulenza sia da parte del CSP uscente sia che di quello entrante oppure la possibilità di usufruire di servizi aggiuntivi quali la cifratura dei dati o la verifica di completezza e correttezza dei dati oggetto di migrazione.

1.5 Particolari ambiti di applicazione: Security as a Service

Uno dei settori maggiormente in crescita nell'ambito dei servizi cloud è il cosiddetto "Security as a Service" (SecaaS), ossia l'erogazione di servizi di sicurezza in modalità cloud. Questa crescita è testimoniata oltre che dalla sempre più vasta offerta di servizi presenti sul mercato anche dall'attenzione del mondo della ricerca e dalle analisi degli osservatori di mercato che prevedono un alto tasso di crescita di questi servizi a partire dal 2013.

CSA ha avviato da tempo un gruppo di ricerca per facilitare e supportare lo sviluppo del mercato SecaaS, ovvero la disponibilità di applicazioni e servizi di sicurezza via cloud o per infrastrutture e applicazioni cloud-based o per sistemi/applicazioni presenti presso il cliente.

Da un recente sondaggio di CSA sono state individuate le seguenti categorie di servizi di sicurezza di interesse per una modalità di fruizione "as a service":

- Identity and Access Management (IAM)
- Data Loss Prevention (DLP)
- Web security
- Email security
- Security assessments
- Intrusion management
- Security Information and Event Management (SIEM)
- Encryption
- Business continuity and disaster recovery
- Network security

E' però evidente che per la crescita di questa tipologia di servizi di sicurezza erogati in modalità as a service, data la loro natura e la loro importanza per i CSC, si riesca a gestire il problema della portabilità e interoperabilità garantendo ai CSC di riuscire a gestire questi nuovi servizi in maniera analoga a quanto già viene fatto con le proprie infrastrutture o con quanto viene erogato dai vari outsourcer presenti sul mercato.

1.6 L'importanza per il nostro Paese

L'Italia, in particolare, è nella condizione di beneficiare dei servizi erogati in modalità cloud in quanto, per la stragrande maggioranza dei casi, i potenziali CSC appartengono alla Piccola e Media Impresa o alle Pubbliche Amministrazioni centrali o locali. Entrambe queste categorie di potenziali CSC trarrebbero dei significativi benefici dalla realizzazione di servizi che non presuppongono costi iniziali di avviamento e che sono erogabili sulla basi di accordi a consumo, caratteristiche che li rendono fortemente appetibili in situazioni in cui il cliente non è in condizione sia di valutare che, di conseguenza, effettuare grandi investimenti economici o non è dotato di robuste strutture interne dedicate all' IT (senza dimenticare il problema dell'acquisizione di nuove competenze professionali). E' di tutta evidenza, però, che questi indubbi benefici potrebbero essere vanificati, in tutto o in parte, in condizioni in cui la portabilità e l'interoperabilità dei dati o del codice fosse poco sviluppata, bloccando di fatto il CSC in una condizione di vulnerabilità e sudditanza nei confronti del CSP.

E' quindi oltremodo importante che in Italia si dedichi una particolare attenzione a questi temi e che si trovino quanto prima soluzioni, a livello contrattuale e a livello tecnologico per garantire la piena possibilità di fruizione dei servizi cloud alle nostre imprese e alle nostre PA.

1.7 Le opportunità per il mercato Europeo

L'importanza della portabilità e interoperabilità dei servizi cloud è stata evidenziata in diversi studi di settore e, dal 2009, in diversi progetti di ricerca finanziati dalla comunità europea tra cui citiamo:

- RESERVOIR[9] per l'interoperabilità dei servizi IaaS
- HELIX Nebula[10] per la creazione di una piattaforma cloud condivisa con la comunità scientifica (di cui CSA è uno dei partner)

Diverse iniziative di ricerca e progettazione concrete su questi temi vengono catalogate e divulgate dal 2010 dall'iniziativa SIENA – Standards and Interoperability for Einfrastructures implemeNtation initiAtive – un consorzio di centri di ricerca, università, industrie di settore ed esperti appartenenti all' EU27[11]che nella sua mission propone l'adozione e l'evoluzione di una infrastruttura di elaborazione digitale interoperabile.

L'influenza di questi due requisiti nello sviluppo del mercato cloud, e in generale dell'informatica, è stata recepita in particolar modo dal settore della Pubblica Amministrazione ed ha portato diversi governi a contestualizzarle nelle Agende Digitali sia in campo nazionale che europeo. Nel primo ambito citiamo il programma UK G-Cloud[12] mentre a livello europeo è stato istituito dal 2010 il programma Agenda Digitale coordinato dal Commissario NeelieKroes[13].

Le proposte di CSA per promuovere l'interoperabilità e portabilità, sulla base anche dell'importante contributo fornito alla consultazione del 2011 sulla strategia della commissione europea sul cloud computing[14], vanno nella direzione di istituire uno specifico processo di acquisto nella pubblica amministrazione che possa evitare il problema del lock-in nell'offerta seguendo le indicazioni fornite dal programma EIF – European Interoperability Framework for pan-European eGovernment services – e dagli standard aperti (vedi paragrafo precedente).

Sulla base dell'esperienza di CSA con il governo federale degli US ed il NIST viene riconosciuta l'importanza della PA nel guidare l'adozione del cloud computing in particolare nelle nazioni in cui il mercato cloud è ancora immaturo, vi è poca informazione, in particolare su leggi e norme applicabili, ed è tradizionalmente resistente al cambiamento e non in grado di esprimere requisiti chiari e completi sui servizi cloud desiderati.

Sicuramente il settore pubblico potrà abilitare l'adozione del cloud promuovendo azioni tese a definire lo sviluppo di standard tecnici e di linee guida per la classificazione di servizi e dati tenendo in debito conto le problematiche di portabilità e interoperabilità e di compliance alle normative esistenti.

---

[9] www.reservoir-fp7.eu
[10] www.facebook.com/HelixNebula.TheScienceCloud
[11] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Glossary:EU-27
[12] http://gcloud.civilservice.gov.uk/
[13] http://ec.europa.eu/digital-agenda/
[14] https://cloudsecurityalliance.org/wp-content/uploads/2011/11/CSA_EU_Response_Final.pdf

In particolare si auspica lo sviluppo e la pubblicazione di linee guida, checklist, “buyer’s guide”, template per redigere Service Level Agreements (SLA) e Request for Proposals (RFP) per servizi comuni e standardizzati che indirizzino i potenziali CSC nella individuazione dei propri requisiti avendo una maggiore confidenza nella correttezza delle proprie scelte.

2.0 La sicurezza applicativa nel cloud

La sicurezza delle applicazioni Web è un tema che, con il passare del tempo, sta assumendo sempre maggiore importanza e valore. Attualmente, la maggior parte degli episodi di intrusione o di attacco ad organizzazioni pubbliche e private è veicolata attraverso lo sfruttamento di una qualche vulnerabilità in applicazioni Web. Questo scenario che, già di per sé, merita una grande attenzione da parte di chi sviluppa ed esercisce sistemi informatici, è ulteriormente complicato dalla diffusione del cloud computing.

2.1 Implicazioni e portata del tema

Gli ambienti cloud, grazie alle loro caratteristiche intrinseche e ai loro vantaggi, consentono degli approcci allo sviluppo applicativo contraddistinti da una rapidità, una flessibilità e una economicità che non ha eguali rispetto ai tradizionali ambienti IT. Il cloud, d'altra parte, comporta però anche una maggiore complessità, una maggiore dispersione delle responsabilità e una minore capacità di governo sia da parte del Cloud Service Provider (CSP) sia del Cloud Service Consumer (CSC). Lo sviluppo e l'esercizio di applicazioni Web in ambienti cloud richiede quindi un rigore e un'attenzione agli aspetti di sicurezza superiore a quello che viene normalmente riservato allo sviluppo in ambienti tradizionali. L'approccio deve essere orientato alla massima garanzia, assimilabile a quello riservato allo sviluppo di applicazioni critiche destinate ad essere fruite attraverso Internet. Devono, inoltre, essere tenuti in debito conto tutti gli aspetti peculiari degli ambienti cloud quali, ad esempio, la potenziale incompatibilità tra vendor diversi o le difficoltà nel garantire una adeguata protezione ai dati in tutte le varie fasi del processo elaborativo (creazione, transito, elaborazione e storage).

La soluzione migliore dunque consiste nell'utilizzare al meglio gli approcci già ampiamente testati nello sviluppo di applicazioni Web (Secure Software Development Life Cycle - SSDLC) e porre un'opportuna cura nell'individuazione di contromisure adeguate alla criticità dei dati e delle applicazioni, che tengano efficacemente conto delle peculiarità degli ambienti cloud. Inoltre, deve essere attentamente valutato l'approccio alla sicurezza in relazione al modello di servizio cloud (IaaS, PaaS o SaaS) e al modello di deployment prescelto (Private, Community, Public o HybridCloud). Infatti, a differenti modelli corrispondono differenti attività e responsabilità per i CSP e per i CSC sia nella fase di predisposizione degli ambienti che nello sviluppo che, infine, nell'esercizio.

Data la criticità di questo scenario, Cloud Security Alliance ha quindi destinato molta attenzionealla sicurezza applicativa nella propria "Security Guidance 3.0", dedicando al tema l'intero Dominio 10, uno dei più corposi di tutta la guidance.

Considerando il panorama italiano, in questo percorso di crescita di consapevolezza, si sconta un gap importante dovuto alla cronica mancanza di una "vision" sui temi dello sviluppo strategico dell'IT. Le contingenze legate, ad esempio, alla difficoltà nel rendere operativi piani di sviluppo della banda larga o all'assenza di una "Cybersecurity Strategy", rendono il percorso di diffusione del cloud maggiormente insidioso e difficoltoso. Inoltre, il nostro Paese, essendo caratterizzato da una forte presenza di PMI sarà, così come lo è adesso, rappresentato da un'estesa presenza di CSC a fronte di un ridotto numero di CSP nazionali.

Questo scenario complessivo, comporta un'ancora maggiore necessità di impegno nella proposizione di contributi, anche da parte di soggetti non istituzionali, che possano proporre apporti utili al consolidamento di pratiche virtuose nello strategico campo della sicurezza.

CSA-Italy e OWASP Italy hanno, quindi, deciso di fare propria questa sfida e di avviare una collaborazione sul tema della sicurezza applicativa in ambito cloud che vedrà nel corso del tempo il varo di iniziative verticali di approfondimento di temi critici, nell'ottica di una partecipazione attiva allo sviluppo e alla crescita del sistema paese.

2.2 I Progetti OWASP Top Ten e Cloud TOP Ten Security Risks

Il panorama delle minacce, in particolar modo quelle legate alle applicazioni software di tipo Web Based, è in costante mutamento. I fattori chiave di questa incessante evoluzione sono da ricercare nei continui progressi compiuti dagli attaccanti, nello sviluppo di nuove tecnologie e nell'utilizzo di sistemi sempre più complessi.

OWASP Top 10, uno dei documenti più noti sostenuti dal progetto OWASP (Open Web Application Security Project), nasce per rispondere in maniera efficace a questo rinnovamento designandosi come una classifica periodicamente aggiornata dei dieci maggiori rischi associati alle applicazioni *Web Based*.

Per completezza di informazione viene riportato di seguito l'elenco delle dieci categorie di rischio individuate ed analizzate nell'ambito del progetto: A1 - "Injection", A2 - "Cross-Site Scripting (XSS)", A3 - "Broken Authentication and Session Management", A4 - "Direct Object Reference", A5 - "Cross-Site Request Forgery (CSRF)", A6 - "Security Misconfiguration", A7 - "Insecure Cryptographic Storage", A8 - "Failure to Restrict URL Access", A9 - "Insufficient Transport Layer Protection", A10 - "Unvalidated Redirects and Forwards".

Il progetto OWASP Top Ten, preso come riferimento da importanti organizzazioni quali, ad esempio, MITRE, PCI DSS, DISA e FTC, rappresenta oramai uno standard *de-facto,* oltre che una guida preziosa, non solo nell'ambito del Penetration Testing *Web Based* bensì nel più vasto campo relativo al Penetration Testing applicativo.

Un ulteriore progetto OWASP di particolare interesse è il "Cloud Top 10 Security Risks".

Questo progetto affronta i dieci maggiori rischi inerenti alla sicurezza applicativa nel Cloud, in particolare nei modelli pubblici e ibridi in ambito "Software as a Service" (SaaS). Di seguito si riporta l'elenco dei rischi individuati dal progetto (sebbene non ancora considerato "stabile" dall'organizzazione): R1. Accountability and Data Ownership, R2. User Identity Federation, R3. Regulatory Compliance, R4. Business Continuity and Resiliency, R5. User Privacy and Secondary Usage of Data, R6. Service and Data Integration, R7. Multi Tenancy and Physical Security, R8. Incident Analysis and Forensic Support, R9. Infrastructure Security, R10. Non-production Environment Exposure.

Le tematiche affrontate dai rischi sopra elencati coprono buona parte degli argomenti trattati nei maggiori standard di riferimento sulla sicurezza informatica ed evidenziano l'esigenza di una chiara distinzione delle responsabilità dei CSC e dei CSP. Da quest'ultimo aspetto si evince, inoltre, la necessità di stabilire "solidi" accordi contrattuali fra le parti, anche in termini di livelli di servizio.

In merito al contesto italiano (e non solo) vale la pena citare, poiché particolarmente critico, il rischio R3 (Regulatory Compliance), ovvero la difficoltà da parte dei CSP nel dimostrare la conformità alle normative applicabili, con particolare riferimento alla normativa europea e nazionale in tema di protezione dei dati personali.

Degno di nota risulta essere anche il rischio R8 (Incident Analysis and Forensic Support) che evidenzia la necessità di poter acquisire informazioni, a fronte di un incidente informatico, in un'ottica di analisi forense. Tali informazioni potrebbero essere presenti su diversi sistemi, in parte gestiti dai CSP (eventualmente ubicati in paesi diversi e quindi disciplinati da leggi diverse) ed in parte gestiti dai CSC, comportando quindi una maggiore complessità nella raccolta ed analisi.

Il progetto "Cloud Top 10 Security Risks" è pertanto da considerarsi un punto di riferimento per i Cloud Service Provider (CSP), un utile strumento per il Risk Management dei CSC ed una guida per quelle organizzazioni che intendono realizzare delle cloud basate su modelli alternativi di deployment (private e community cloud).

In conclusione, il progetto "Cloud Top 10 Security Risks", è in grado di portare concreti contributi alla risoluzione delle citate criticità di sicurezza e quindi mitigare l'attuale resistenza dei CSC verso l'adozione di soluzioni cloud. Una volta ritenuto maturo questo progetto, potrebbe seguire il successo ottenuto dal fratello maggiore "Top 10 Web Application Security Risks", diventando anch'esso uno standard "de facto" nella sicurezza del Cloud.

2.3 Modelli per lo sviluppo di software sicuro

L'acronimo inglese SSDLC (Secure Software Development Life Cycle) definisce un ciclo di vita del software ottimizzato ed arricchito, nel corso di tutte le sue tipiche fasi (analisi, progettazione, sviluppo, test e manutenzione), di opportune attività legate specificatamente alla sicurezza delle informazioni.

Abuse Case, *Secure Code Review* e *Penetration Testing* sono soltanto alcune di queste.

Il noto esperto di sicurezza applicativa Gary McGraw, all'interno del libro "*Software Security: Building Security In*" traccia sapientemente un chiaro esempio di integrazione di tali attività all'interno di un tipico ciclo di vita del software.

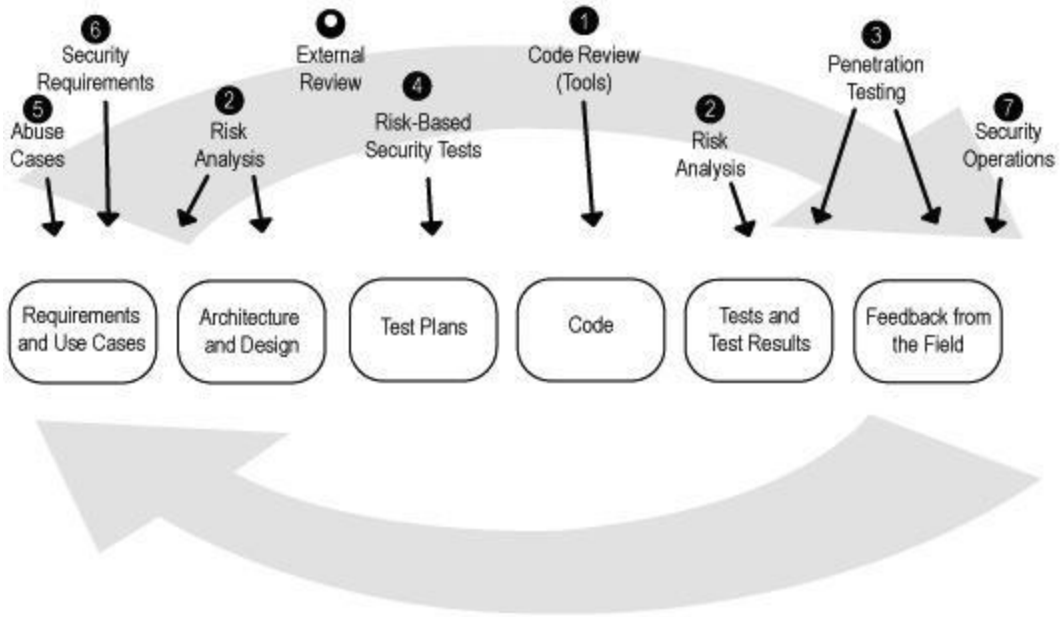

Figura 3: Ciclo di vita del software sicuro

Una loro corretta e completa attuazione contribuirebbe, infatti, ad incrementare sensibilmente il livello di protezione di ogni singola fase.

Tra i più noti e rigorosi processi di programmazione sicura ci sembra doveroso citare: SDL (Secure Software Development Lifecycle) uno dei programmi di maggiore successo nato dall'iniziativa Trustworthy Computing di Microsoft e CLASP (Comprehensive Lightweight Application Security Process), originariamente sviluppato da SecureSoftware ed in seguito devoluto al progetto OWASP (Open Web Application Security Project).

Tale processo è definito attraverso cinque prospettive di alto livello chiamate viste. Le viste sono a loro volta suddivise in attività contenenti componenti di processo.

3.0 Principi di Software Security

La seguente sezione si pone l'obiettivo dipresentare brevemente, ma con completezza di informazioni, alcuni dei principi fondamentali relativi alla sicurezza del software.

3.1 Least Privilege

Il principio di Least Privilege nasce dalla necessità di limitare i potenziali danni derivanti, ad esempio, da condizioni di errore, incidenti di sicurezza piuttosto che da un utilizzo non autorizzato o non convenzionale di un'applicazione software.

La raccomandazione che si ritrova all'interno del postulato è che gli utenti – così come le stesse applicazioni software – siano in possesso di un subset minimo di privilegi necessari per la sola esecuzione delle proprie attività lavorative inibendo così tutti gli eventuali accessi, seppur involontari, a funzionalità critiche dell'applicativo, file system e/o base di dati.

3.2 Secure By Default

L'applicazione software dovrebbe essere dotata, già in configurazione standard, di opportune caratteristiche di sicurezza quali, ad esempio, l'abilitazione automatica di meccanismi di costruzione di password complesse piuttosto che dalla presenza di procedure di rinnovo delle stesse secondo una scadenza di natura temporale.

3.3 Defence In Depth

Secondo questo approccio, la protezione di una data componente non è più incentrata su un unico meccanismo difensivo bensì su una pluralità di fattori, tutti finalizzati all'aumento del livello di robustezza globale dell'applicativo.

Appare, infatti, evidente che un eventuale tentativo di compromissione della componente - e conseguentemente dell'applicazione - sarebbe perseguibile soltanto dopo l'elusione di più layer di sicurezza.

3.4 Separation Of Duties

Il principio di *Separation Of Duties* attesta, infine, che la sicurezza globale di una qualsiasi infrastruttura può accrescere qualora ci sia la possibilità di assegnare, ad utenti diversi, parti distinte di un processo ritenuto critico. Infatti, in una simile prospettiva è assai raro che l'errato operato di un singolo individuo causi la compromissione dell'intera infrastruttura.

4.0 CSA Italy: processo di gestione

Così come già visto all'interno del paragrafo dedicato alle implicazioni e alla portata del tema, l'orientamento consigliato per un'efficace gestione della sicurezza delle applicazioni Webin ambiente Cloud prevede anche un richiamo agli approcci canonici dello sviluppo software sicuro (SSDLC) tenendo conto, ovviamente, delle peculiarità dei nuovi ambienti.

Quello che viene, in breve, proposto è un efficiente processo di gestione, strutturato in quattro fasi, suggerito per riuscire a progettare, sviluppare e mantenere software sicuro e di qualità all'interno di un'organizzazione.

La prima fase, denominata "**Strategia di Governance**" rimarca: l'indispensabile definizione dei diversi ruoli (quali, ad esempio, Developer, Project Manager, e Security Auditor) coinvolti nel processo di gestione, l'importanza dell'acquisizione di *knowhow* mediante attività di formazione specialistica oltre che la necessaria acquisizione, mediante una serie di interviste, delle informazioni inerenti ai processi e alle eventuali metodologie in essere all'interno dell'azienda.

La fase successiva è quella definita di "**Implementazione**" termine che racchiude, così come peraltro avviene all'interno delle metodologie di sviluppo agili, non solo la mera attività di produzione del codice sorgente bensì tutti quei metodi e criteri adottati per la realizzazione di un'architettura software sicura.

Vengono introdotte, pertanto, in questa fase, le attività di Secure Code Review" ovvero l'analisi manuale del codice dell'applicazione al fine di identificarne eventuali vulnerabilità di sicurezza e l'attività di "Threat Modeling" (modellazione delle minacce), ossia la valutazione e la documentazione dei rischi associati alla sicurezza di un particolare sistema e/o applicazione software.

Mediante l'applicazione di un processo di Threat Modeling è possibile, infatti, determinare un elemento denominato "Threat Profile" associato all'applicazione, ossia lo scenario non fidato in cui l'applicativo dovrà essere eseguito.

L'adozione di opportune tecniche quali, ad esempio, l'identificazione degli Entry Point, ovvero i punti di accesso all'applicazione, dei Privilege Boundaries e del Threat Tree saranno fondamentali per l'identificazione e l'applicazione di strategie di mitigazione utili per contrastare potenziali minacce a cui potrebbe essere soggetta l'applicazione.

La terza fase del processo, definita con il termine "**Collaudi di Sicurezza**" suggerisce l'adozione di attività di "Penetration Testing" ovvero l'insieme dei collaudi di sicurezza atti ad analizzare, da una prospettiva tipica dell'attaccante, la robustezza di un' applicazione software.

Tali verifiche hanno l'obiettivo di indurre gli applicativi in condizione di errore e/o scenari non canonici al fine di verificarne il possibile sfruttamento per l'esecuzione di azioni non autorizzate.

Rientrano in tale categoria tutte le azioni che violano uno, o più, dei tre elementi del paradigma cardine della sicurezza informatica: la riservatezza, l'integrità e la disponibilità del dato.

Soprattutto in questa terza fase del processo di gestione proposto, l'importanza rivestita dall'adozione di una metodologia è indubbia. "OWASP Top 10" ed "OSSTMM" rappresentano oggi le metodologie di riferimento per la realizzazione di attività di testing.

La loro combinata applicazione esprime quanto c'è di meglio nel campo della metodica applicata al Penetration Testing.

L'ultima fase dedicata alle "**Contromisure e continuità d'esercizio**" prevede tipicamente la gestione di due attività. La prima di "Code Mitigation" legata alla mitigazione delle eventuali problematiche di sicurezza rilevate all'interno del codice sorgente degli applicativi esaminati e la seconda denominata "Progettazione difensiva" ovvero il processo di definizione sicuro dei componenti software.

Alcuni tipici principi adottati nella progettazione difensiva sono rappresentati dallo sviluppo di componenti dedicati alla validazione di tutti i caratteri di input e di output, piuttosto che all'assegnazione di privilegi minimi.

5.0 Conclusioni e iniziative future

Come ampiamente illustrato nel documento si evince che queste tematiche sono punti chiave per lo sviluppo del cloud in Italia.

Sui temi di interoperabilità e portabilità, CSA Italy intende svolgere un ruolo attivo in Italia proponendosi in tutte le sedi opportune come interlocutore esperto per aziende ed enti, pubblici e privati, interessati sia alla definizione dell'offerta di servizi cloud che all'identificazione e selezione dei Cloud Provider secondo processi ispirati alle migliori “best practice” a livello internazionale. L'Italia, infatti, è tra i paesi che, in termini di crescita e di aumento della propria competitività, potrebbero ottenere i maggiori risultati dall'adozione del cloud computing; CSA-Italy, quindi, intende dare il proprio attivo contributo con l'obiettivo di sostenere lo sviluppo del nostro mercato interno di servizi cloud basati sulla trasparenza, sulla fiducia e, in ultima analisi sulla sicurezza.

Con tali presupposti CSA Italy seguirà con particolare attenzione gli attori del mercato ICT ritenuti fondamentali per lo sviluppo del mercato cloud, ovvero la Pubblica Amministrazione e gli operatori di telecomunicazione, che rappresentano i Cloud Carrier presenti e futuri.

In merito alla sicurezza delle applicazioni in ambito cloud, le prossime iniziative di CSA Italy avranno come obiettivo la produzione di documenti finalizzati all’approfondimento e alla contestualizzazione verticale delle tematiche precedentemente trattate.

In particolare CSA Italy si propone di avviare una ricerca finalizzata alla realizzazione di un documento di indirizzo e linee guida per l’applicazione del modelli SSDLC e SDL rispetto alle attuali soluzioni Cloud ed ai relativi modelli di deployment. Questo documento costituirà un punto di riferimento per i CSC per la determinazione delle responsabilità in tema di sicurezza delle applicazioni softwarenei vari modelli di cloud.

Tale iniziativa avrà, inoltre, come obiettivo quello di delineare il campo di azione (in termini di sviluppo di applicazione sicure) dei CSC e conseguentemente proporre soluzioni per far fronte alle criticità indotte dalla tecnologia Cloud.

