Guida alla sicurezza

per

Aree di criticità

nel

Cloud Computing V2.1

Redatta da
Cloud Security Alliance
Dicembre 2009

Traduzione in italiano redatta da
Cloud Security Alliance Capitolo Italiano
Settembre 2011

Premessa alla traduzione italiana

Come associazione CSA Italy siamo orgogliosi di annunciare come prima pubblicazione ufficiale la traduzione in italiano della Guidance di CSA, ovvero la "Security Guidance for Critical Areas of Focus in Cloud Computing" nella sua versione 2.1, una guida che, nella sua edizione originale, è stata oggetto di più di 100.000 download dalla data di pubblicazione (Dicembre 2009).
Non posso quindi che ringraziare per l'ottimo lavoro svolto i soci e fondatori del capitolo italiano Yvette Agostini, Moreno Carbone, Mauro Gris, Andrea Piazza e Valerio Vertua.
CSA Italy nasce contestualmente come Regional Chapter per l'Italia di Cloud Security Alliance (CSA) di cui eredita la missione, indirizzata al mercato italiano, ovvero "promuovere l'utilizzo di best practice al fine di garantire la sicurezza nell'ambito del Cloud Computing, e fornire la necessaria formazione e sensibilizzazione sull'utilizzo del Cloud, al fine di consentire di rendere sicure tutte le forme di computing".
Il 2011 rappresenta per molti aspetti l'anno di ripartenza del settore Information Technology dopo la crisi del 2009 e, in particolare, l'anno della maturità del mercato Cloud Computing in cui sono emerse numerose offerte, in particolare nell'area Public Cloud, ma anche una domanda crescente. In questo nuovo contesto si avverte, sia lato provider che consumer di servizi cloud. maggior consapevolezza dell'importanza del tema security nel nuovo paradigma. Il nostro lavoro si inserisce, quindi, in un momento in cui il mercato, in particolare quello italiano, inizia a cercare risposte e soluzioni sul tema. La Guidance italiana diventa, quindi, oggi un supporto fondamentale sia per facilitare la comprensione tecnico-organizzativa della sicurezza nel nuovo paradigma cloud computing che una base di conoscenza fondamentale per avviare un vero e proprio percorso di certificazione professionale specifico sulla sicurezza del cloud quale il CCSK (Certificate of Cloud Security Knowledge), gestito da CSA, o in generale nell'ambito della sicurezza informatica.
Non mi resta pertanto che invitarvi a continuare la lettura di questa guida ed a seguirci sulla "rete" (chapters.cloudsecurityalliance.org/italy/) per usufruire di altre importanti pubblicazioni sulla cloud security.

Alberto Manfredi
Presidente CSA Italy

Introduzione

La presente guida è la seconda versione del documento della Cloud Security Alliance "Guida alla sicurezza per le aree critiche di focus nel Cloud Computing", originariamente pubblicato nell'Aprile 2009. Gli archivi permanenti di questi documenti sono:
http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf (questo documento)
http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf (versione 1 della guida)

A differenza della prima versione della nostra guida, è stato deciso di separare la guida chiave dalla ricerca dei domini fondamentali. Ciascuna ricerca dei domini fondamentali sarà pubblicata come autonomo white paper. Questi, insieme alla programmazione delle uscite, sono disponibili all'indirizzo:
http://www.cloudsecurityalliance.org/guidance/domains
Un altro cambiamento rispetto alla prima versione consiste nel fatto che il Dominio 3: Aspetti legali e il Dominio 4: Electronic Discovery sono stati fusi in un unico dominio. Inoltre, il Dominio 6: gestione del ciclo di vita ed il Dominio 14: storage sono stati uniti in un unico dominio, denominato Gestione del Ciclo di vita. Questo ha comportato la rinumerazione dei 13 Domini.

Lettera degli autori

E' difficile credere che solo sette pochi mesi fa, abbiamo radunato un gruppo di individui da ogni angolo dell'industria tecnologica per pubblicare la prima "Guida...". Sin dal suo lancio, questa pubblicazione determinante ha continuato ad eccedere le nostre aspettative per l'aiuto fornito agli enti in tutto il mondo nel prendere decisioni consapevoli sull'opportunità, i modi ed i tempi per l'adozione di servizi e tecnologie del Cloud Computing. Ma in questi sette mesi la nostra conoscenza, e le tecnologie del Cloud Computing, sono evolute a gran velocità. Questa seconda versione è pensata per fornire sia nuovi elementi conoscitivi che un maggior approfondimento per supportare queste complesse sfide. L'adozione del Cloud Computing è una decisione complessa che coinvolge molteplici fattori. La nostra speranza è che la guida contenuta in questo lavoro sia di aiuto per meglio comprendere quali domanda porre, quali sono le prassi correntemente raccomandate, e le potenziali insidie da evitare.

Focalizzandosi sulle questioni centrali della sicurezza del Cloud Computing abbiamo tentato di portare maggiore chiarezza in un orizzonte piuttosto complesso, spesso affollato di informazioni incomplete o eccessivamente semplificate. Il focus sugli originari 15 Domini (ora consolidatisi in 13) serve a contestualizzare e dare specificità alla discussione sulla sicurezza del Cloud Computing: rendendo possibile il superamento delle generalizzazioni grezze ed il conseguimento di raccomandazioni più dense di contenuto e mirate. Nel nostro viaggio si è unita a noi una lista crescente di industrie, imprese, ed individui che credono nella nostra missione di sviluppo e promozione delle migliori prassi per assicurare la sicurezza nel Cloud Computing. Le loro prospettive e le loro intuizioni sono state essenziali nel creare un lavoro ben bilanciato, obiettivo, che continui a servire da eccellente fondamento sul quale continuare a costruire. Il Cloud Computing è tuttora uno scenario in rapida evoluzione e che richiede di essere seguito con attenzione pena il rimane indietro.

In questa seconda versione della guida ci siamo basati sull'esperienza e sulla professionalità collettiva della nostra grande e differenziata comunità di volontari per creare un lavoro più completo maggiormente dettagliato e preciso. Tuttavia, non dobbiamo compiacercene. Come i professionisti della sicurezza han fatto per anni, dobbiamo continuare ad evolvere i nostri processi, metodi e tecniche alla luce delle opportunità che il Cloud Computing porta alle nostre industrie. Questa evoluzione è critica per il nostro successo a lungo termine dovendo trovare nuovi modi per migliorare l'efficacia e l'efficienza dell'applicazione delle misure di sicurezza e di monitoraggio. Il Cloud Computing non è necessariamente più o meno sicuro del nostro ambiente abituale. Come ogni nuova tecnologia crea nuovi rischi e nuove opportunità. In alcuni casi la migrazione al Cloud Computing fornisce un'opportunità per riprogettare applicazioni ed infrastrutture obsolete in modo da rispettare o superare i moderni requisiti di sicurezza. In altri casi, il rischio connesso alla migrazione di dati sensibili ed applicazioni su un'infrastruttura emergente potrebbe superare il livello di rischio tollerabile. Il nostro obiettivo in questa guida non è dirvi esattamente cosa, dove, o come migrare nella nuvola, ma fornire raccomandazioni pratiche e argomenti chiave per rendere la transizione il più sicura possibile, per voi. Infine, in rappresentanza della Cloud Security Alliance e del Gruppo di Lavoro dei Autori, vorremmo ringraziare tutti i volontari per il tempo e l'impegno che hanno profuso nello sviluppo di questo nuovo documento guida. Siamo stati costantemente ispirati dalla dedizione dei gruppi nell'estendere e migliorare le rispettive aree, e crediamo che il loro impegno abbia aggiunto un significativo valore a questo lavoro. Questo documento non sarebbe ciò che è senza il loro contributo. Come sempre, siamo lieti di ricevere i vostri commenti dalla lettura di questa nuove versione della guida. Se trovate utile questa guida o vorreste vederla migliorata, considerate di unirvi alla Cloud Security Alliance come socio o contributore.

Glenn Brunette
Rich Mogull Editors

Indice dei contenuti

Premessa

Benvenuti alla seconda versione della "Guida alla sicurezza delle aree di criticità nel Cloud Computing" della Cloud Security Alliance. Mentre il cammino del Cloud Computing prosegue, porta con se' nuova opportunità e nuove sfide di sicurezza. Speriamo umilmente di fornire ai lettori sia guida che ispirazione per sostenere le necessità del business mentre si gestiscono nuovi rischi.

Mentre la Cloud Security Alliance potrebbe essere più nota per questa guida, nel corso dei prossimi mesi saranno visibili molte altre attività, inclusi capitoli internazionli, alleanze ed accordi, nuovi progetti di ricerca, e attività di conferenza volte a sostenere ulteriormente la nostra missione. E' possibile essere aggiornati sulle nostre attività al sito www.cloudsecurityallianche.org.

Il cammino per rendere sicuro il cloud computing è certamente lungo, e richiede la partecipazione di un vasto insieme di portatori di interesse su base globale. D'altro canto, dobbiamo riconoscere con soddisfazione i progressi cui stiamo assistendo: nuove soluzioni di sicurezza per il cloud computing appaiono regolarità, le aziende stanno utilizzando la nostra guida per relazionarsi con i fornitori di servizi cloud, e si sta svolgendo a livello mondiale un sano dialogo pubblico a proposito della conformità e degli aspetti di trust connessi al cloud computing.

La vittoria più importante che abbiamo conseguito è che i professionisti della sicurezza sono fortemente impegnati nel mettere in sicurezza il futuro e non semplicemente nella protezione del presente.

Rimanete impegnati su questo argomento e continuate a lavorare con noi per portare a compimento questa importante missione.

Distinti saluti

Jerry Archer Dave Cullinane Nils Puhlmann Alan Boehme Paul Kurtz Jim Reavis

The Cloud Security Alliance Board of Directors

Una nota degli autori sul rischio: decidere cosa, quando e come migrare al Cloud

Attraverso questa guida si fa esteso riferimento a raccomandazioni sulla riduzione del rischio nell'adozione del Cloud Computing, ma non tutte queste raccomandazioni sono necessarie o realistiche per tutti i tipi di implementazione di soluzioni Cloud. Mentre, durante il processo editoriale, compilavamo le informazioni dai differenti gruppi di lavoro, abbiamo rapidamente capito che semplicemente non vi era abbastanza spazio per fornire raccomandazioni sufficientemente dettagliate per tutti i possibili scenari di rischio. Così come un'applicazione critica potrebbe essere troppo importante perché sia migrata su un fornitore pubblico di Cloud, così potrebbe non essere giustificata l'applicazione di estesi controlli di sicurezza a dati di basso valore nella migrazione verso uno storage basato sul Cloud.

Essendovi così tante differenti scelte implementative – incluso il modello di servizio SPI (SPI è l'acronimo di Software as a Service, Platform as a Service, o Infrastructure as a Service, ed è dettagliatamente spiegato nel Dominio 1); le implementazioni pubblico/privato, l'hosting interno/esterno, e varie permutazioni ibride – nessuna lista di controlli può comprendere tutte le circostanze. Come in ogni area della sicurezza, gli enti dovrebbero adottare un approccio basato sul rischio nel migrare al Cloud e nella selezione delle scelte di sicurezza.

Quanto segue è un semplice inquadramento per aiutare a valutare i rischi iniziali connessi al Cloud e per guidare le decisioni riguardanti la sicurezza. Questo processo non è un quadro completo di determinazione del rischio, né una metodologia per determinare tutte le esigenze di sicurezza. E' un metodo rapido per valutare il livello di rischio nello spostamento di un asset verso vari modelli di Cloud Computing.

Identificazione dell'asset per l'implementazione del Cloud

In estrema sintesi, gli assets supportati dal Cloud ricadono in due categorie generali:

1. Dati
2. Applicazioni/Funzioni/Processi

Possono essere spostate nel Cloud o informazioni o transazioni/processi (da funzioni parziali sino alle intere applicazioni).

Con il Cloud Computing, dati e applicazioni non necessitano di risiedere nello stesso luogo, ed è possibile spostare nel Cloud anche solo parti di funzioni. Ad esempio, possiamo ospitare la nostra applicazione e i dati nel nostro data center, mentre affidiamo all'esterno nel Cloud una parte della sua funzionalità mediante il modello Platform as a Service.

Il primo passo nel valutare il rischio connesso al Cloud è determinare esattamente quali dati o funzioni vanno prese in considerazione per il Cloud. Ciò dovrebbe includere i potenziali utilizzi dell'asset una volta migrato nel Cloud per individuare eventuali falle. I volumi di dati e transazioni sono spesso più alti di quanto atteso.

Valutazione dell'asset

Il passo successivo è determinare quanto i dati o le funzioni sono importanti per l'ente. Non è necessario condurre una valutazione dettagliata salvo che l'ente sia già dotato di un processo in tal senso, ma è necessaria almeno una grossolana valutazione della sensibilità dell'asset e dell'importanza dell'applicazione/funzione/processo.

Per ogni asset, si pongono le seguenti domande:

1. in che modo l'impresa sarebbe danneggiata se l'asset divenisse di pubblico dominio e distribuito su vasta scala?
2. in che modo l'ente sarebbe danneggiato se un dipendente del fornitore di servizi Cloud avesse accesso all'asset?
3. in che modo l'impresa sarebbe danneggiata se il processo o funzione fossero manipolati da un'entità esterna?
4. in che modo l'ente sarebbe danneggiato se il processo o la funzione fallissero nel fornire i risultati attesi?
5. in che modo l'impresa sarebbe danneggiata se l'informazione o i dati fossero alterati in modo inatteso?
6. in che modo l'impresa sarebbe danneggiata se l'asset non fosse disponibile per un certo tempo?

Essenzialmente si valutano i requisiti di confidenzialità, integrità e disponibilità per l'asset; e come questi sarebbero interessati da una loro migrazione al Cloud totale o parziale. E' molto simile al valutare il potenziale affidamento in outsourcing di un progetto, eccetto che con il Cloud Computing vi sono una miriade di possibilità implementative, inclusi i modelli interni.

Mappatura dell'asset per i potenziali modelli implementativi del cloud

A questo punto si dovrebbe avere una certa comprensione dell'importanza dell'asset. Il prossimo passo è determinare qual è il modello implementativo adeguato. Prima di iniziare a cercare i potenziali fornitori, si dovrebbe capire se sono accettabili i rischi impliciti in ciascun modello implementativo - privato, pubblico, comunitario, o ibrido - e gli scenari di hosting - interno, esterno, o combinato -. Per quanto concerne l'asset, è necessario chiarire se si è disposti ad accettare le seguenti possibilità:

1. Pubblico
2. Privato, interno/on-premises
3. Privato, esterno (inclusa infrastruttura condivisa o dedicata)
4. Community, tenendo conto della localizzazione dell'hosting, del potenziale fornitore di servizi, e dell'identificazione di altri membri appartenenti alla community.
5. Ibrido. Per valutare efficacemente un'implementazione ibrida, è necessario partire almeno da una bozza architetturale di dove i componenti, i dati e le funzioni risiederanno.

A questo punto ci si dovrebbe essere fatti un'idea piuttosto buona di quale sia il livello accettabile di rischio nella migrazione, e quali siano i modelli implementativi e le localizzazioni che soddisfano i propri requisiti di sicurezza e di rischio.

Valutazione dei potenziali modelli di servizio e fornitori Cloud

A questo punto ci si deve focalizzare sul grado di controllo che si avrà con ciascun livello degli SPI (fornitori servizi internet) nell'implementazione della gestione del rischio richiesta. Se si sta valutando una specifica offerta, si potrebbe ora voler passare a una valutazione completa del rischio.

Ci si dovrà concentrare sul grado di controllo possibile nell'implementazione della riduzione dei rischi nei differenti livelli di SPI. Se si hanno già dei requisiti specifici (ad esempio, per gestire dati regolamentati) è possibile includerli nella valutazione.

Disegnare il possibile flusso dei dati

Se si sta valutando una specifica scelta implementativa, bisogna mappare il flusso dei dati tra l'impresa, il servizio Cloud, e ogni altro cliente o ogni altro nodo. Mentre la maggior parte di questi passaggi è di alto livello, prima di prendere una decisione definitiva è assolutamente essenziale capire se e come i dati possono entrare e uscire dal Cloud.

Se si deve ancora decidere per una particolare offerta, sarà opportuno tracciare un flusso dei dati per ogni possibilità tra quelle ritenute accettabili. Ciò al fine di assicurarsi che al momento di prendere la decisione definitiva, si sarà in grado di identificare i punti di esposizione al rischio.

Conclusioni

A questo punto dovrebbe essere chiara l'importanza di quel che si pensa di spostare nel Cloud, la propensione al rischio (almeno ad alto livello), e quali combinazioni di implementazione e modelli di servizio sono ritenute accettabili. Si dovrebbe pure avere un'idea approssimativa dei punti nei quali le informazioni e i trattamenti sensibili sono potenzialmente esposti.

Insieme, questi aspetti dovrebbero fornire un contesto sufficiente per valutare ogni altro controllo di sicurezza elencato in questa guida. Per gli asset di minor valore non è necessario lo stesso livello in termini di controlli di sicurezza ed è possibile evitare molte delle raccomandazioni, quali ispezioni in sito, e complessi schemi crittografici. Un asset di alto valore e regolamentato potrebbe comportare obblighi di audit e di data retention. Altri asset di alto valore ma non regolamentati potrebbero richiedere una maggiore attenzione sui controlli di sicurezza tecnica.

A causa dello spazio limitato, così come della vastità degli argomenti da trattare e da approfondire, questo documento contiene estese elencazioni di raccomandazioni di sicurezza. Non tutte le implementazioni Cloud richiedono tutti i possibili controlli di rischio e di sicurezza. L'impiego di un po' di tempo per una valutazione della propensione al rischio e della potenziale esposizione fornirà l’ambiente necessario per

selezionare e scegliere le migliori opzioni per l'impresa e per l'implementazione del Cloud.

Sezione I. Architetture del Cloud

Dominio 1: Aspetti architetturali del Cloud Computing

Questo dominio, aspetti architetturali del Cloud Computing, fornisce un base concettuale per tutto il resto della guida CSA. I contenuti di questo dominio sono concentrati sulla descrizione del Cloud Computing specificamente nella prospettiva del professionista di reti IT e sicurezza. Le seguenti tre sezioni definiscono questa prospettiva in termini di:

- La terminologia utilizzata in questa guida, per fornire un lessico congruente
- I requisiti architetturali e le sfide per la messa in sicurezza delle applicazioni e servizi del Cloud
- Un modello di riferimento che descriva una tassonomia delle architetture e dei servizi Cloud.

La sezione finale di questo dominio fornisce una breve introduzione a ognuno degli altri domini nella guida stessa.

La comprensione dell'aspetto architetturale descritto in questo dominio è un primo passo importante nella comprensione del resto della Guida CSA. Questo aspetto definisce molti dei concetti e termini utilizzati negli altri domini.

Che cosa è il Cloud Computing?

Cloud Computing ('Cloud') è un termine in evoluzione che descrive lo sviluppo di molte tecnologie esistenti e che si pone nei confronti del Computing in modo differente. Il Cloud separa le applicazioni e le risorse informative dalla sottostante infrastruttura, e dai meccanismi utilizzati per la fornitura del servizio.

Il Cloud aumenta la collaborazione, l'agilità, la scalabilità e la disponibilità, fornendo il potenziale per ridurre i costi mediante l'utilizzo ottimizzato ed efficiente delle risorse computazionali.

Più specificamente, il Cloud descrive l'uso di una quantità di servizi, applicazioni, informazioni e infrastrutture comprendenti aggregati di risorse di potenza di calcolo, di rete, di informazioni e di storage.
Questi componenti possono essere orchestrati rapidamente, messi a disposizione, implementati e dismessi, incrementati o decrementati, fornendo un modello di allocazione e consumo risorse simile a quello on-demand adottato dalle utilities.

Da un punto di vista architetturale vi è molta confusione intorno alle similitudini e differenze rispetto ai modelli di Computing tradizionali, e riguardo a come queste similitudini e differenze impattano sull'approccio organizzativo, operativo e tecnologico alle prassi di sicurezza di rete e delle informazioni.

In questo periodo ci sono molte definizioni che tentano di definire il Cloud dalla prospettiva degli accademici, degli architetti, degli ingegneri, degli sviluppatori, dei manager e degli utilizzatori finali.
Questo documento si concentra su una definizione che è specificamente concepita dalla prospettiva unica dei professionisti della sicurezza IT e di rete.

Le chiavi per comprendere come le architetture Cloud impattino l'architettura di sicurezza sono un lessico comune e conciso, insieme a una consistente (consistent) tassonomia delle offerte mediante la quale le architetture e i servizi Cloud possono essere decostruiti, mappati nei confronti di un modello di controlli compensativi di sicurezza e operativi, base di stima e gestione del rischio, e di conformità agli standard.

Che cosa include il Cloud Computing?

La prima versione della guida della Cloud Security Alliance riportava definizioni che erano state redatte prima che fosse stato pubblicato il lavoro degli scienziati dell'U.S. National Institute of Standards and Technology (NIST) frutto dei loro sforzi per la definizione del Cloud Computing.

La pubblicazione del NIST è generalmente ben accetta, e si è scelto di allineare la definizione di Cloud Computing con la Working Definition che ne da il NIST (al momento della redazione della versione inglese di questa guida, alla versione 15) per portare coerenza e consenso intorno ad un linguaggio comune così che ci si possa concentrare sui casi d'utilizzo piuttosto che intorno alle sfumature semantiche.

E' importante notare che questa guida è intesa per essere utilizzabile in modo diffuso e applicabile a enti a livello globale. Mentre il NIST è un organismo del governo americano, la scelta di questo modello di riferimento non dovrebbe essere interpretata in senso di escludere altri punti di vista o località geografiche.

Il NIST definisce il Cloud Computing descrivendo 5 caratteristiche essenziali, 3 modelli di servizio Cloud, e 4 modelli implementativi del Cloud. Questi sono illustrati in figura 1 e spiegati in dettaglio nel seguito.

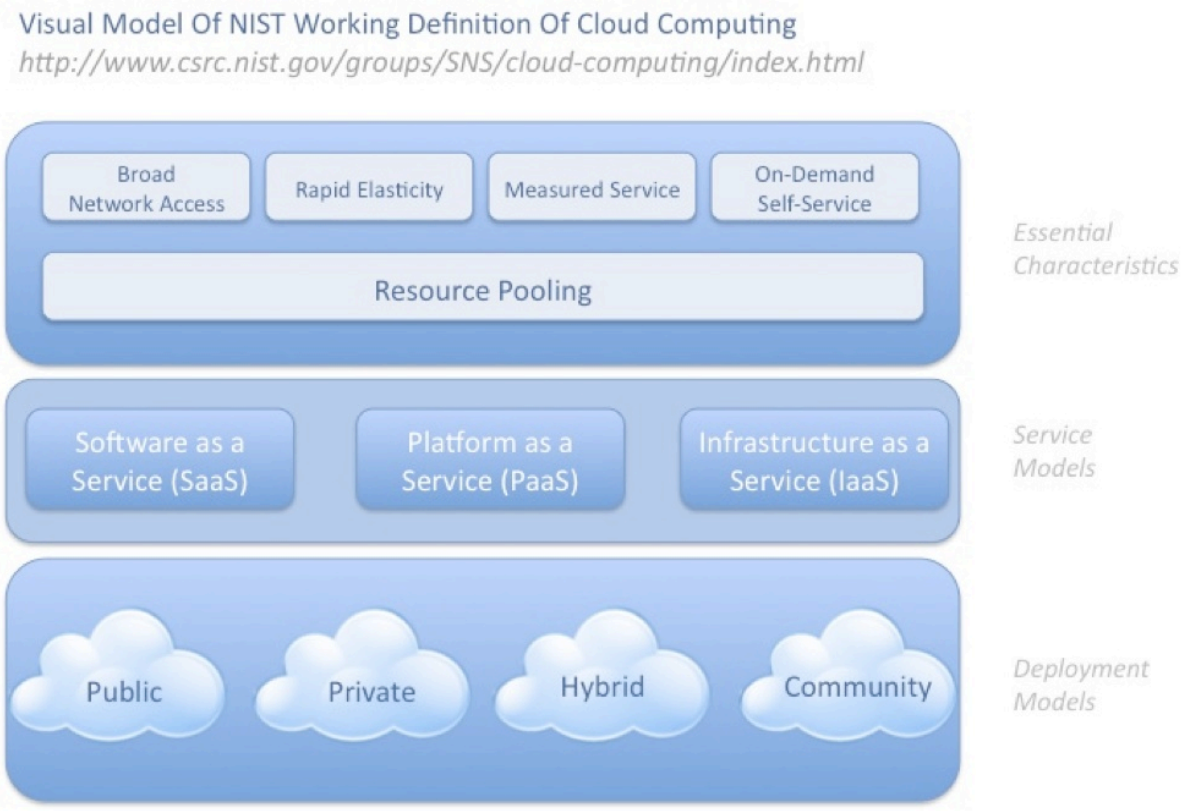

Figura 1: Schema della definizione del Cloud Computing secondo il NIST

Caratteristiche essenziali del Cloud Computing

I servizi Cloud mostrano 5 caratteristiche essenziali che dimostrano la loro relazione con, e le differenze da, gli approcci tradizionali al Computing:

- **On-demand self-service**. Un utilizzatore può unilateralmente fornire capacità di calcolo quali tempo processore e storage di rete quando necessario in modo automatico, senza la necessità di interazione umana con un fornitore di servizi.
- **Ampio accesso di rete**. Le capacità di calcolo sono rese disponibili in rete e sono accessibili tramite meccanismi standard che ne promuovono l'uso da parte di piattaforme eterogenee e di diverse dimensioni (ad esempio, telefoni cellulari, computer portatili e PDA) così come avviene per altri servizi software basati sul Cloud o meno.
- **Resource pooling**. Le risorse computazionali del fornitore di servizi sono messe a disposizione per servire molteplici utenti finali utilizzando un modello multi-tenant, con differenti risorse fisiche e virtuali assegnate e riassegnate dinamicamente secondo la domanda dell'utilizzatore. C'è un certo grado di indipendenza dalla localizzazione nel senso che il cliente generalmente non ha controllo sull'esatta posizione delle risorse che gli sono fornite, ma può essere in grado di specificarne, ad un livello più alto di astrazione (ad esempio, nazione, regione, data center), la localizzazione. Esempi di risorse sono: lo storage (spazio disco), processori, memoria, banda di rete, macchine virtuali. Anche le Cloud private tendono a mettere in comune le risorse tra parti differenti della stessa impresa.
- **Elasticità rapida**. Le capacità di calcolo possono essere fornite rapidamente ed elasticamente – in alcuni casi in modo automatico – incrementandole velocemente; e rilasciate rapidamente decrementandole in modo altrettanto veloce. Per l'utilizzatore, le capacità disponibili spesso appaiono illimitate e possono essere acquistate in qualsiasi quantità e in ogni momento.
- **Servizio misurato**. I sistemi Cloud controllano e ottimizzano automaticamente l'utilizzo delle risorse mediante misurazioni effettuate a un livello di astrazione adeguato al tipo di servizio (ad esempio, storage, processore, banda, o utenti attivi). L'utilizzo delle risorse può essere monitorato, controllato e relazionato – aggiungendo trasparenza sia per il fornitore di servizio che per l'utilizzatore dello stesso. E' importante riconoscere che i servizi Cloud sono spesso, ma non sempre, utilizzati in congiunzione con, e abilitati da, tecnologie di virtualizzazione. Non ci sono requisiti, però, che legano l'astrazione delle risorse alle tecnologie di virtualizzazione e in molte offerte la virtualizzazione attraverso hypervisor o sistema operativo contenitore non è utilizzata. Inoltre, dovrebbe essere tenuto conto del fatto che la multi-tenancy non è indicata dal NIST come caratteristica essenziale del Cloud, ma spesso è trattata come se lo fosse. Per una trattazione più approfondita, si faccia riferimento alla sezione che si riferisce alla multi-tenancy che si trova dopo la descrizione dei modelli di implementazione del Cloud.

Modelli di servizio del Cloud

La fornitura dei servizi Cloud è divisa fra tre modelli archetipici e varie combinazioni derivate da questi. Alle tre classificazioni fondamentali si fa spesso riferimento come "Modello SPI", dove SPI sta per Software, Piattaforma o Infrastruttura (in forma di servizio), rispettivamente; perciò:

- **Cloud Software as a Service (SaaS)**. All'utente è fornita la possibilità di utilizzare le applicazioni del provider che riesiedono in un'infrastruttura Cloud. Le applicazioni sono accessibili da diversi dispositivi client attraverso un'interfaccia client leggera, quale un browser web (ad esempio, posta elettronica web based). L'utente non gestisce o controlla l'infrastruttura Cloud sottostante, comprendente rete, server, sistemi operativi, storage, applicazioni individuali, con la possibile eccezione di insiemi di istruzioni di configurazione dell'applicazione limitati all'ambito utente.
- **Cloud Platform as a Service (PaaS)**. All'utente è fornita la possibilità di implementare nell'infrastruttura Cloud applicazioni da egli create o acquisite, utilizzando linguaggi di programmazione e strumenti supportati dal fornitore Cloud. L'utente non gestisce o controlla l'infrastruttura Cloud sottostante, comprendente rete, server, sistemi operativi, storage, ma ha controllo sulle applicazioni implementate e sulle possibili configurazioni dell'ambiente che ospita le applicazioni.
- **Cloud Infrastructure as a Service (IaaS)**. È fornita all'utente la possibilità di utilizzare potenza di calcolo, storage, rete e altre risorse computazionali fondamentali e l'utente può implementare e far funzionare software arbitrario, che può includere sistemi operativi e applicazioni. L'utente non gestisce o controlla la sottostante infrastruttura Cloud, ma ha controllo sui sistemi operativi, lo storage, le applicazioni installate, e un controllo limitato di alcuni componenti di rete (ad esempio, il firewall sull'host).

Sia il modello del NIST che questo documento non trattano direttamente le definizioni emergenti dei modelli di servizio associate con i mediatori di servizi Cloud, cioè di quei fornitori Cloud che offrono intermediazioni, monitoraggio, trasformazione/portabilità, governo, provisioning, e integrazione di servizi e che negoziano relazioni tra vari fornitori di servizi Cloud e utenti.

Nel breve termine, poiché l'innovazione porta allo sviluppo rapido si soluzioni, gli utenti e i fornitori di servizi Cloud potranno avere una varietà di metodi di interazione con i servizi Cloud, sotto forma di API e interfacce e così i mediatori di servizi Cloud emergeranno come un importante componente nell'ecosistema complessivo del Cloud.

I mediatori di servizi Cloud astrarranno quelle capacità potenzialmente incompatibili e quelle interfacce per conto degli utenti per fornire dei proxy in attesa dell'arrivo di modi standardizzati e aperti per risolvere il problema di più lungo termine con una capacità semantica che consente agilità e fluidità così che l'utente possa trarre vantaggio dal modello che meglio si attagli alle sue necessità.

E' pure importante notare l'emergere di molti sforzi centrati sullo sviluppo di API, sia aperte che proprietarie, che cercando di rendere possibile la gestione, la sicurezza e l'interoperabilità per il Cloud. Tra questi sforzi si annoverano l'Open Cloud Computing Interface Working Group, le API di Amazon EC2, le API vCloud DMTF-submitted di VMware, le API Open Cloud di Sun, le API di Rackspace, e quelle di GoGrid's, solo per nominarne alcune. Le API aperte e standard giocheranno un ruolo chiave nella portabilità ed interoperabilità del Cloud, così come i formati del comune contenitore quali l'Open Virtualization Format (OVF) del DMTF.

Mentre ci sono molti gruppi di lavoro, specifiche in bozza e pubblicate in esame in questo momento, è naturale che il consolidamento avverrà quando le forze di

mercato, la domanda degli utenti e i parametri economici ridurranno questo panorama ad un più gestibile ed interoperabile insieme di attori.

Modelli di implementazione del Cloud

Oltre ai modelli di servizio utilizzati (SaaS, PaaS, o IaaS) ci sono quattro modelli di implementazione dei servizi Cloud, con varianti da questi derivati che soddisfano specifiche necessità:

- **Cloud Pubblico:** L'infrastruttura Cloud è resa disponibile al pubblico generico o a un grosso gruppo industriale ed è di proprietà di un'ente che vende servizi Cloud.
- **Cloud Privato:** L'infrastruttura Cloud è gestita totalmente da una singola impresa. Può essere gestita dall'impresa o da una terza parte, e può esistere all'interno dell'infrastruttura o all'esterno di essa.
- **Cloud Comunitario:** L'infrastruttura Cloud è condivisa tra differenti imprese e supporta una specifica comunità con necessità simili (ad esempio: mission, requisiti di sicurezza, politiche, o considerazioni relative alla conformità).Può essere gestita dalle imprese o da una terza parte e può esistere all'interno dell'infrastruttura o all'esterno di essa.
- **Cloud ibrido:** L'infrastruttura Cloud è una combinazione di due o più Cloud (del tipo privato, pubblico, comunitario) che rimangono entità uniche ma che sono tenute insieme da tecnologia standardizzata o proprietaria che abilita la portabilità dei dati e delle applicazioni (ad esempio, bursting del Cloud per il bilanciamento di carico tra "nuvole").

E' importante notare che ci sono modelli implementativi derivati che emergono in seguito alla maturazione delle offerte sul mercato e della domanda dei clienti. Un esempio sono le Cloud private virtuali – un modo di utilizzare infrastrutture Cloud pubbliche in modo privato o semi-privato e di interconnettere queste risorse alle risorse interne ad un data center del cliente, di solito mediante connettività VPN (Virtual Private Network).

Il contesto architetturale usato nella progettazione di soluzioni ha chiare implicazioni sulle future flessibilità, sicurezza e mobilità del risultato, così come sulle sue capacità in termini di collaborazione. Come regola di massima, le soluzioni perimetrate sono meno efficaci di quelle de-perimetrate in ognuna delle quattro aree. Per ragioni simili, particolare attenzione dovrebbe pure essere data alla scelta tra soluzioni aperte e proprietarie.

Multi-Tenancy

Sebbene, nel modello del NIST, non sia considerata una caratteristica essenziale del Cloud Computing, CSA ha identificato la multi-tenancy come un elemento importante del Cloud.

La multi-tenancy nei modelli di servizio cloud implica la necessità di applicazioni guidate da policy, di segmentazione, di isolamento, di governance, di livelli di servizi e di modelli di riaddebito/di fatturazione per diverse categorie di utilizzatori. Gli utilizzatori potrebbero impiegare le offerte di servizi di un fornitore di cloud pubblico o

addiritura essere la medesima impresa, come il caso di diverse unità produttive invece di diverse entita organizzative, ma condividerebbero ancora l'infrastruttura.

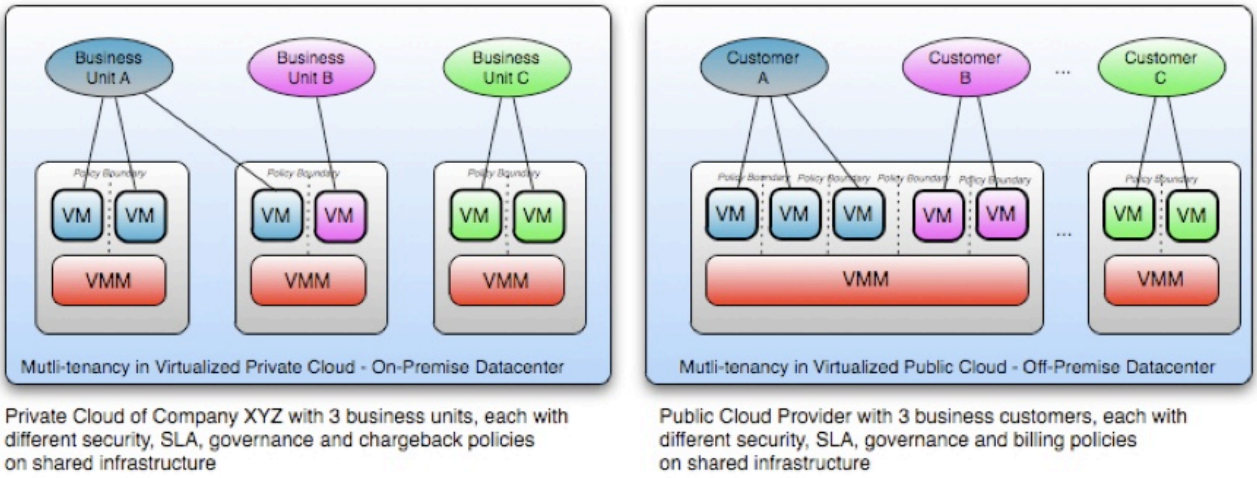

Figura 2: Schema della multi-tenancy

Dalla prospettiva di un fornitore di servizi, la multi-tenancy suggerisce un approccio architetturale e di progetto che abilita le economie di scala, la disponibilità, la gestione, la segmentazione, l'isolamento e l'efficienza operativa sfruttando l'infrastruttura condivisa, i data, i metadati, i servizi e le applicazioni tra molti clienti diversi.

La multi-tenancy può anche avere definizioni diverse a seconda del modello di servizio Cloud adottato dal fornitore; in quanto può aver effetto sulle capacità sopra descritte a livello di infrastrutture, di database o di applicazione. Un esempio potrebbe essere la differenza tra una implementazione multi-tenant IaaS e una SaaS.

I modelli implementativi del Cloud danno differente importanza alla multi-tenancy. Tuttavia, pure nel caso del Cloud privato, una singola impresa può avere una moltitudine di consulenti e collaboratori esterni, così come il desiderio di un maggior grado di separazione tra business unit. Perciò, le preoccupazioni relative alla multi-tenancy dovrebbero essere sempre prese in considerazione.

Il modello di riferimento del Cloud

La comprensione delle relazioni e dipendenze tra i modelli di Cloud Computing è critica per la comprensione dei rischi di sicurezza del Cloud Computing stesso. IaaS è il fondamento di tutti i servizi Cloud, con il PaaS costruito sull'IaaS, ed il SaaS sul PaaS, come descritto nel diagramma del modello di riferimento del Cloud. In questo modo, proprio come vengono ereditate le capacità, così lo sono le questioni relative alla sicurezza delle informazioni e del rischio. E' importante notare che i fornitori commerciali di Cloud potrebbero non rientrare strettamente in modelli di servizio stratificati. Pur tuttavia, il modello di riferimento è importante per mettere in relazione i servizi reali con un base architetturale e per comprendere quali risorse e servizi richiedono analisi della sicurezza.

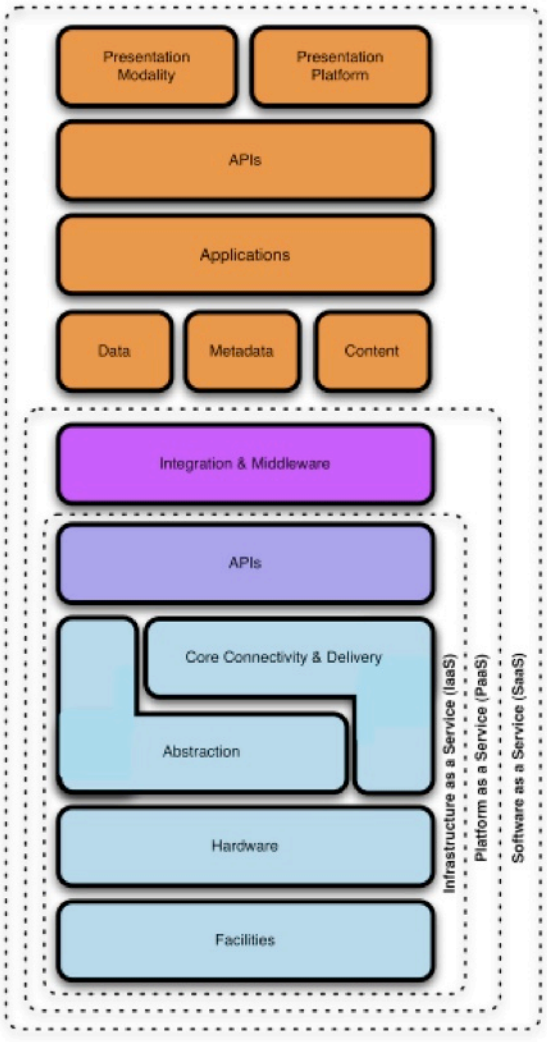

Figura 3: Il modello di implementazione del Cloud

IaaS include l'intera pila delle risorse infrastrutturali, dalle facilities alle piattaforme hardware che in esse risiedono. Incorpora la capacità di astrarre le risorse (o no), così come dispiega la connettività fisica e logica di queste risorse.
Infine, IaaS fornisce un insieme di API che consentono la gestione e altre forme di interazione con l'infrastruttura da parte dei clienti.

Il PaaS si situa sopra l'IaaS ed aggiunge uno strato di integrazione ulteriore con il quadro di sviluppo applicativo; le capacità middleware, e funzioni quali basi di dati, messaggistica, accodamento che permettono agli sviluppatori di costruire applicazioni sulla piattaforma; ed i cui linguaggi di programmazione e strumenti sono supportati dallo stack.

Il SaaS, a sua volta, è costruito sulle sottostanti pile IaaS e PaaS; e fornisce un ambiente operativo autocontenuto utilizzato per fornire l'intera esperienza utente, inclusi i contenuti, la loro presentazione, le applicazioni, e le capacità di gestione.

Dovrebbe quindi essere chiaro che ci sono significativi compromessi per ognuno dei modelli in termini di caratteristiche integrate, complessità rispetto ad apertura (estendibilità), e sicurezza. I compromessi tra i tre modelli di implementazione del Cloud includono:

- in genere il SaaS fornisce la maggior parte delle funzionalità integrate direttamente nell'offerta, con la minore estendibilità per l'utente, e un livello relativamente elevato di sicurezza integrata (quanto meno il fornitore ha la responsabilità della sicurezza).
- PaaS è pensato per abilitare gli sviluppatori a costruire le proprie applicazioni sulla piattaforma. Come risultato, tende ad essere maggiormente estendibile del SaaS, a spese delle caratteristiche già approntate per l'utente. Questo compromesso estende le caratteristiche di sicurezza e le capacità, dove le capacità integrate sono meno complete, ma c'è maggior flessibilità per aggiungere ulteriori caratteristiche di sicurezza.
- IaaS fornisce poche o nessuna caratteristica del tipo applicazione, ma un'enorme estendibilità. Questo significa, in genere, minori capacità e funzionalità di sicurezza integrate oltre la protezione dell'infrastruttura stessa. Questo modello richiede che i sistemi operativi, le applicazioni e i contenuti siano gestiti e posti in sicurezza dall'utente del Cloud.

Il concetto chiave in termini di sicurezza in questo caso è che più il fornitore limita in basso nello stack le caratteristiche di sicurezza, tanto più sono le caratteristiche di

sicurezza e di gestione di cui l'utente del Cloud è responsabile in termini di implementazione e gestione.

Nel caso del SaaS, questo significa che i livelli di servizio, la sicurezza, la governance, la conformità e la responsabilità del fornitore di servizi sono contrattualmente stipulate, gestite in modo da essere conformi ed implementate.
Nel caso del PaaS o dell'IaaS è responsabilità degli amministratori di sistema del cliente l'efficace gestione degli stessi con qualche compensazione atteso dal fornitore per la messa in sicurezza della piattaforma sottostante e dei componenti infrastrutturali per fornire la disponibilità del servizio e la sicurezza a livello base. Dovrebbe essere chiaro che in entrambi i casi è possibile assegnare/trasferire la responsabilità, ma non necessariamente la competenza.

Restringendo l'oggetto o le specifiche capacità e funzionalità in ciascuno dei modelli implemetativi del Cloud, o impiegando l'accoppiamento funzionale di servizi e capacità tra essi, ne possono derivare classificazioni ulteriori. Ad esempio “Storage as a Service” è una sub-offerta specifica della famiglia IaaS.

Mentre una più ampia panoramica del crescente insieme di soluzioni di Cloud Computing è al di fuori degli scopi di questo documento, la tassonomia delle soluzioni Cloud redatta da OpenCrowd e riportata nella figura seguente, fornisce un eccellente punto di partenza. Essa dimostra il grande aumento di soluzioni disponibili attualmente attraverso ciascuno dei modelli definiti in precedenza.

Dovrebbe essere notato che CSA non appoggia in modo specifico alcune delle soluzioni proposte e delle aziende menzionate nella figura della tassonomia, ma fornisce il diagramma a dimostrazione della varietà di offerte disponibili oggi.

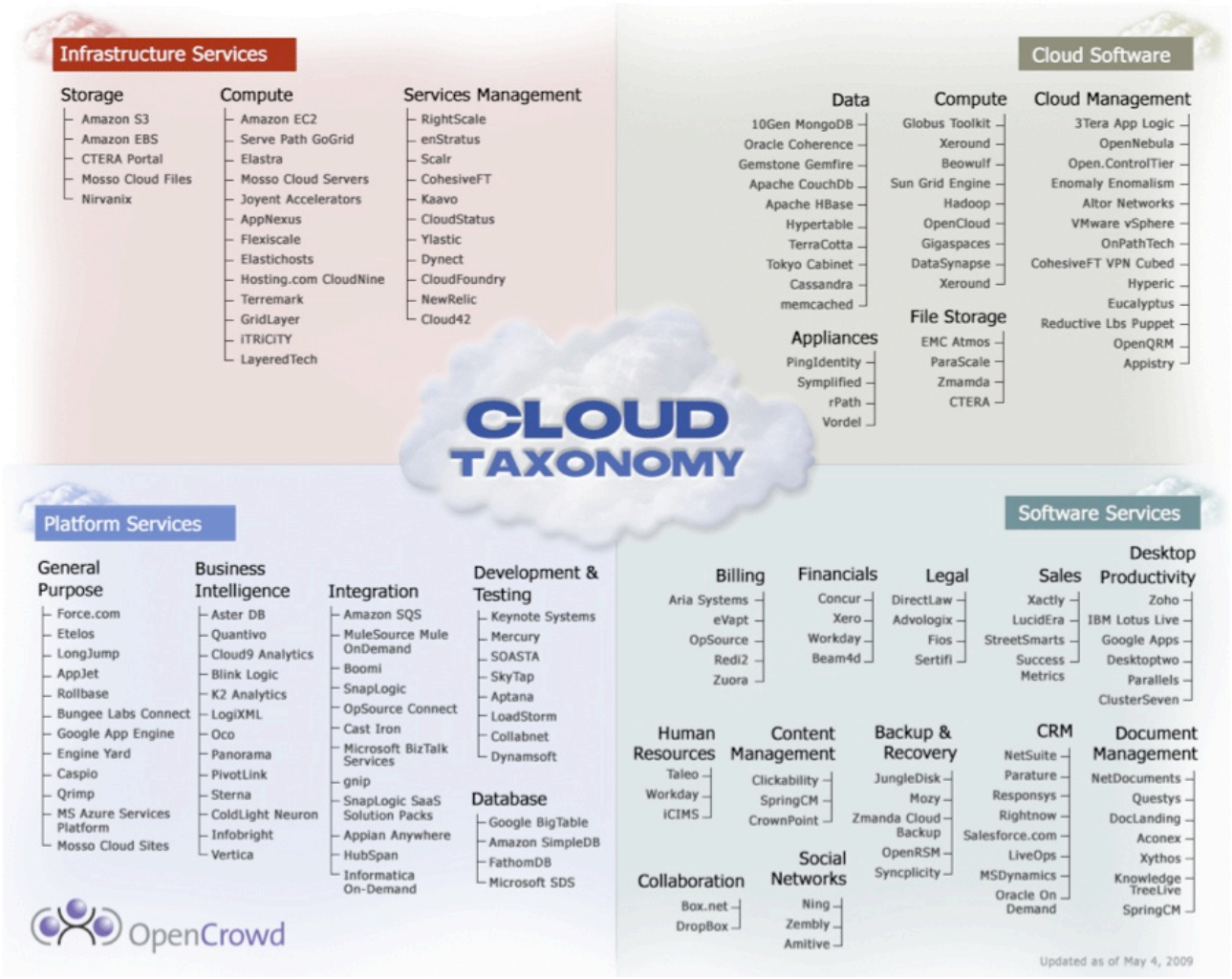

Figura 4: La tassonomia del Cloud secondo OpenCrowd

Per una eccellente panoramica di molteplici casi di utilizzo del Cloud Computing, il Gruppo CSA "Cloud Computing Use Case" ha prodotto un lavoro collaborativo per descrivere e definire i casi comuni e dimostrare i benefici del Cloud, essendo il loro obiettivo quello di "...riunire i clienti ed i fornitori del Cloud per definire casi di utilizzo comuni del Cloud Computing...e far luce sulle capacità e possibilità che devono essere standardizzate in un ambiente Cloud per assicurare l'interoperabilità, la facilità di integrazione e la portabilità."

Modello di riferimento del Cloud per la sicurezza

Il modello di riferimento del Cloud per la sicurezza tratta le relazioni di queste classi e le contestualizza con le pertinenti riflessioni e controlli di sicurezza. Per le imprese e gli individui che hanno a che fare con il Cloud Computing per la prima volta, è importante notare ciò che segue per evitare potenziali insidie e confusioni:

1. La nozione del come i servizi Cloud sono implementati è spesso utilizzata in modo intercambiabile con il dove essi sono forniti, il che potrebbe ingenerare confusione. Per esempio, Cloud pubbliche o private possono essere descritte come Cloud esterna ed interna rispettivamente il che potrebbe essere accurato o meno in tutte le situazioni.
2. Il modo in cui i servizi Cloud sono fruiti è spesso descritto in relazione alla

posizione del management di una impresa o al perimetro di sicurezza (di solito definito dalla presenza di un firewall). Mentre è importante capire dove si trovano i confini della sicurezza in termini di Cloud Computing, la nozione di perimetro ben demarcato è un concetto anacronistico.

3. La riperimetrazione e l'erosione della fiducia nei confini che già si stanno verificando nelle imprese sono amplificate ed accelerate dal Cloud Computing. La connettività onnipresente, la natura amorfa dello scambio di informazioni, e l'inefficacia dei controlli di sicurezza statici che non possono competere con la natura dinamica dei servizi Cloud, richiedono un nuovo modo di pensare in relazione al Cloud Computing. Il Jericho Forum ha prodotto una considerevole quantità di materiale sulla riperimetrazione delle reti aziendali, inclusi molti studi basati sui casi d'uso.

L'implementazione e le modalità di utilizzo del Cloud dovrebbero essere pensate non solo nel contesto di "interno" rispetto ad "esterno", perché esse hanno a che fare con la localizzazione fisica degli asset, delle risorse e delle informazioni; ma pure da chi li utilizza e da chi ne è responsabile per il loro controllo, sicurezza e conformità con le policies e gli standard.

Ciò, non per suggerire che la localizzazione di un asset internamente od esternamente, di una risorsa o di una informazione non riguardi la sicurezza e l'atteggiamento nei confronti del rischio di una impresa, perché essi influenzano questi fattori – ma per sottolineare che il rischio dipende pure da:

- i tipi degli asset, risorse ed informazioni che sono gestiti
- chi e come gestisce gli asset
- quali controlli sono selezionati e come essi sono integrati
- questioni di conformità

Ad esempio, un'installazione LAMP implementata su AWS WC2 di Amazon sarebbe classificata come soluzione IaaS pubblica, delocalizzata e gestita da terzi; anche se le istanze e le applicazioni/i dati in esse contenuti sono gestiti dall'utente o da una terza parte. Uno stack di applicazioni personalizzate che servono multiple business unit, implementate su Eucalyptus sotto il controllo, gestione e proprietà di una società, potrebbe essere descritto come soluzione SaaS privata, interna ed autogestita. Entrambi gli esempi utilizzano la scalabilità elastica e le funzionalità self service del Cloud.

La tabella seguente riassume questi punti:

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

Tabella 1: sintesi dei modelli implementativi del Cloud

Un altro modo per visualizzare le combinazioni di modelli di servizio Cloud, modelli di implementazione, localizzazione fisica delle risorse, ed attribuzione di gestione e proprietà, è il modello cubico del Cloud del Jericho Forum (http://www.jerichoforum.org) mostrato nella figura seguente:

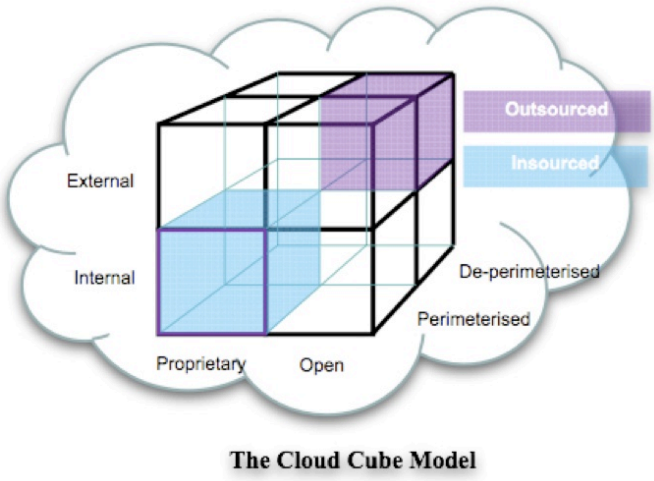

Figura 5: Modello cubico del Cloud secondo il Jericho Forum

Il modello cubico del Cloud illustra le molte permutazioni disponibili nell'offerta Cloud odierna e presenta quattro criteri/dimensioni in modo da distinguere l'una dall'altra le "formazioni" Cloud ed il modo in cui sono implementate, così da comprendere come il Cloud Computing modifichi il modo in cui potrebbe essere approcciata la sicurezza.

Esso mette pure in luce le sfide insite nella comprensione e mappatura dei modelli Cloud per controllare le strutture e gli standard quali l'ISO/IEC 27002, che fornisce "...una serie di linee guida e principi generali per iniziare, implementare, mantenere e migliorare la gestione della sicurezza delle informazioni in un'impresa."

L'obiettivo di controllo menzionato nella ISO/IEC 27002, sezione 6.2, "Soggetti esterni" recita: "...la sicurezza delle informazioni dell'imprese e le strutture per il trattamento delle informazioni non dovrebbero essere diminuite dall'introduzione di prodotti o servizi di soggetti esterni...".

Come tale, le differenze nei metodi e responsabilità per la messa in sicurezza dei tre modelli di servizio del Cloud indicano che gli utenti dei servizi Cloud si trovano a confrontarsi con uno sforzo impegnativo.
A meno che il fornitore di servizi possa prontamente rivelare al cliente i controlli di sicurezza adottati e l'estensione con la quale sono implementati, e che il cliente sappia quali controlli sono necessari per mantenere la sicurezza delle proprie informazioni, vi è ampio margine per decisioni sbagliate ed esiti dannosi.

Questo è un aspetto critico. Prima si classifica un servizio Cloud in relazione al modello architetturale. Poi, è possibile mappare la sua architettura di sicurezza; così come i requisiti di business, regolamentari ed in genere di conformità, nei confronti di questa con un esercizio di gap analysis. Il risultato determina l'atteggiamento generale nei confronti della sicurezza di un servizio e come ciò si relazioni ai requisiti di garanzia e protezione di un asset.

La figura seguente mostra un esempio di come la mappatura di un servizio Cloud può essere comparata con un catalogo di controlli compensativi per determinare quali controlli esistono e quali no – così come riportato dal cliente, dal fornitore di servizi Cloud, o da una terza parte. Questo può essere a sua volta comparato con un quadro di conformità o con un insieme di requisiti, quali PCI-DSS, come mostrato.

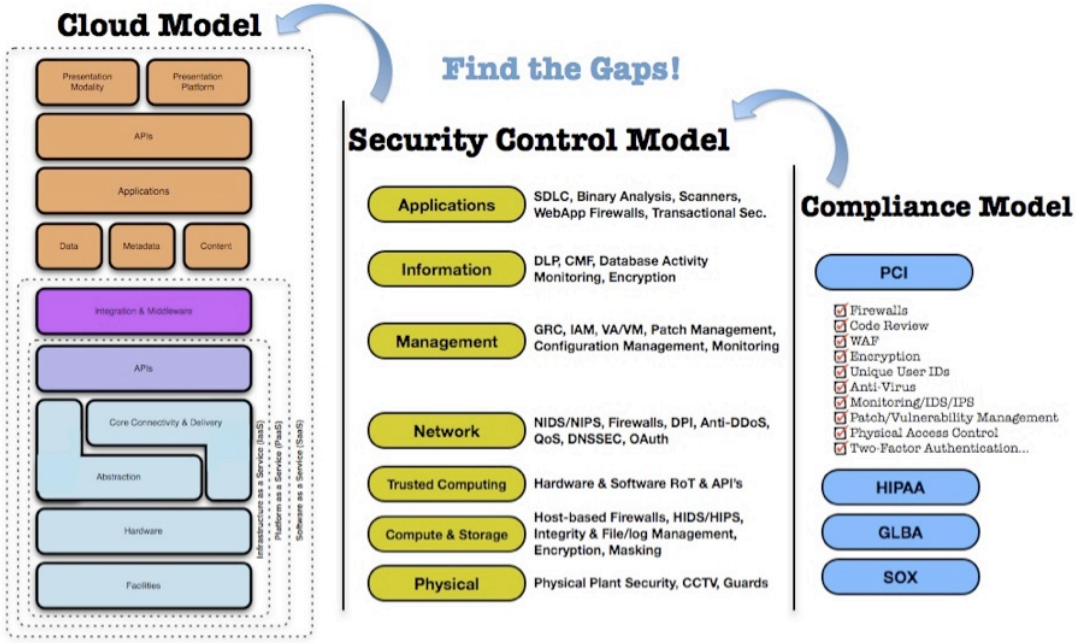

Figura 6: mappatura del modello del Cloud nei confronti dei modelli di controllo di sicurezza e di conformità

Una volta che la gap analysis è completa, come richiesto dai mandati regolamentari o di conformità, diventa molto più semplice determinare cosa dev'essere fatto per alimentare di nuovo il quadro di valutazione del rischio; questo, a sua volta, è di aiuto nel determinare come le difformità ed in ultima battuta i rischi dovrebbero essere affrontati: accettati, trasferiti, o mitigati.

E' importante rilevare che l'utilizzo del Cloud Computing come modello operativo per sua natura non procura né previene il conseguimento della conformità. L'abilità di conformarsi con qualsiasi requisito è risultato diretto del modello di servizio e di implementazione utilizzato e del progetto, della realizzazione e della gestione delle risorse disponibili.

Per una eccellente panoramica del quadro di controllo che fornisca una buona illustrazione di questo cui si è accennato più sopra, si veda la documentazione prodotta dal Gruppo Open Security Architecture, panoramica degli schemi di sicurezza, o il sempre utile e recentemente aggiornato catalogo dei controlli di sicurezza NIST 800-53 revision 3 Recommended Security Controls for Federal Information Systems and Organizations.

Cos'è la sicurezza per il Cloud Computing?

I controlli di sicurezza nel Cloud Computing sono, per la maggior parte, non differenti dai controlli di sicurezza in ogni ambiente IT. Tuttavia, per via dei modelli di servizio Cloud utilizzati, dei modelli operativi, e delle tecnologie utilizzate per abilitare i servizi Cloud, il Cloud Computing può presentare per un ente rischi differenti rispetto alle tradizionali soluzioni IT.

Il Cloud Computing è inerente alla garbata perdita del controllo pur mantenendone il controllo nonostante le responsabilità operative ricadano su una o più terze parti.

L'atteggiamento di un'impresa nei confronti della sicurezza è caratterizzata dalla maturità, efficacia e completezza dei controlli di sicurezza adeguati al rischio che essa implementa. Questi controlli sono implementati in uno o più strati, partendo dalle facilities (sicurezza fisica), all'infrastruttura di rete (network security), ai sistemi IT (sicurezza dei sistemi), sino alle informazioni ed alle applicazioni (sicurezza delle applicazioni). Controlli aggiuntivi sono implementati a livello delle persone e dei processi, quali, rispettivamente, la separazione dei compiti e la gestione del cambiamento.

Come descritto precedentemente in questo documento, le responsabilità in termini di sicurezza del fornitore e dell'utilizzatore sono molto differenti tra modelli di servizio Cloud. L'offerta IaaS AWS EC2 di Amazon, ad esempio, include responsabilità della sicurezza a carico del fornitore sino all'hypervisor, ciò significa che essi possono offrire solo controlli di sicurezza inerenti alla sicurezza fisica, ambientale e di virtualizzazione. A sua volta, l'utilizzatore è responsabile per i controlli di sicurezza connessi al sistema IT (anzitutto) inclusi il sistema operativo, le applicazioni ed i dati.

L'inverso è vero per l'offerta SaaS del CRM di Saleforce.com. Poiché l'intero stack è fornito da Saleforce.com, il fornitore non è responsabile solo dei controlli di sicurezza fisica ed ambientale, ma deve pure occuparsi dei controlli di sicurezza per

l'infrastruttura, le applicazioni ed i dati. Ciò alleggerisce molto la responsabilità operativa diretta del cliente.

Uno degli aspetti attraenti del Cloud Computing sono le efficienze di costi rese possibili dalle economie di scala, il riutilizzo, e la standardizzazione. Per mettere in campo queste efficienze i fornitori Cloud devono fornire servizi sufficientemente flessibili da soddisfare la più larga base di clienti possibile, massimizzando i mercati raggiungibili. Sfortunatamente, integrare la sicurezza in queste soluzioni è spesso percepito come un loro irrigidimento.

Questa rigidità spesso si manifesta nell'incapacità di pareggiare i controlli di sicurezza implementati nel Cloud con quelli dell'IT tradizionale. Questo deriva in larga parte dall'astrazione dell'infrastruttura, e dalla scarsa visibilità e capacità di integrare molti controlli di sicurezza noti, specie a livello di rete.

La figura sottostante illustra questo problema: negli ambienti SaaS i controlli di sicurezza ed i loro ambiti sono negoziati all'interno di contratti di servizio; livelli di servizio, privacy, e conformità sono tutti argomenti che vanno affrontati dal punto di vista legale nei contratti. In un'offerta IaaS, mentre la responsabilità di mettere in sicurezza l'infrastruttura ed il livello di astrazione sottostante è del fornitore, il rimanente dello stack ricade nelle responsabilità del cliente. Il PaaS offre un bilanciamento intermedio, laddove la messa in sicurezza della piattaforma stessa ricade sul fornitore, mentre la messa in sicurezza delle applicazioni sviluppate su di essa e il loro sviluppo sicuro rientrano entrambi nelle responsabilità del cliente.

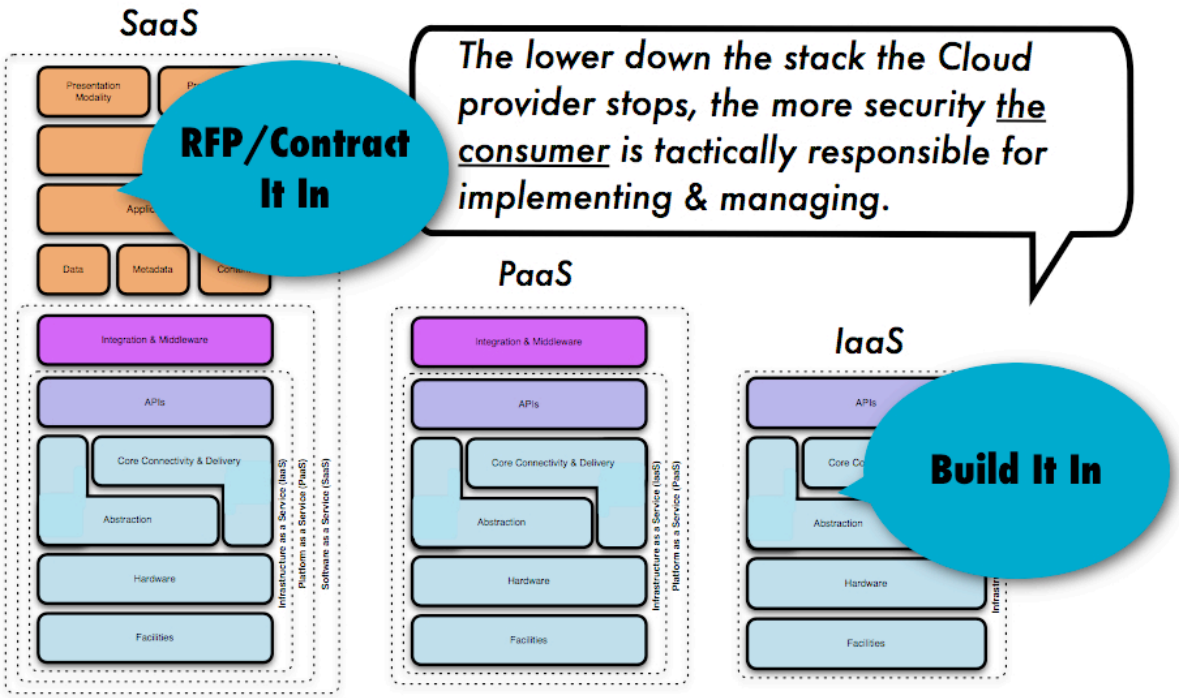

Figura 7: Come viene integrata la sicurezza sul modello del Cloud

La comprensione dell'impatto di queste differenze tra modelli di servizio e come essi sono implementati è critico per gestire l'atteggiamento nei confronti del rischio di una impresa.

Oltre l'architettura: le aree critiche

I rimanenti 12 domini compresi nel seguito della guida CSA, fanno luce sulle aree di interesse per il Cloud Computing e sono concepiti per trattare i "punti dolenti" sia della sicurezza strategica che di quella tattica, e possono essere applicati ad ogni combinazione di servizio Cloud e di modelli di implementazione.

I domini sono divisi in due grandi categorie: governance ed operatività. I domini appartenenti all'area governance sono ampi e trattano gli argomenti di politiche e di strategie in ambito Cloud Computing, mentre i domini operativi si focalizzano maggiormente sugli argomenti di sicurezza tattica e l'implementazione nell'architettura.

Domini della governance

Dominio	**Argomenti**
Governance and Enterprise Risk Management	L'abilità di una impresa nel governare e misurare il rischio d'impresa introdotto dal Cloud Computing. Argomenti quali le priorità legali per le violazioni di accordo, l'abilità delle imprese utilizzatrici di stimare adeguatamente il rischio connesso ad un fornitore Cloud, la responsabilità di proteggere i dati sensibili quando sia l'utente che il fornitore potrebbero essere in difetto, e come i confini internazionali possono condizionare questi temi, sono alcune delle materie trattate.
Legal and Electronic Discovery	Potenziali aspetti legali connessi all'utilizzo del Cloud Computing. Gli argomenti toccati in questa sezione includono i requisiti di protezione per le informazioni ed i computer, leggi concernenti la pubblicizzazione di eventuali brecce di sicurezza, requisiti regolamentari, requisiti di privacy, legislazione internazionale, ecc.
Compliance and audit	Giungere alla conformità e mantenere questa condizione, utilizzando il Cloud Computing. Gli argomenti discussi qui riguardano la valutazione degli effetti del Cloud Computing sulla conformità alle politiche interne di sicurezza, così come ai vari requisiti di conformità (regolamentari, legislativi, ed altri). Questo dominio comprende alcune indicazioni sulle modalità per comprovare la conformità in occasione di attività di audit.
Information Lifecycle Management	Gestione dei dati posti nel Cloud. Vengono trattati in quest'ambito gli argomenti inerenti l'identificazione ed il controllo dei

	dati nel Cloud, così come i controlli compensativi che possono essere utilizzati per controbilanciare la perdita del controllo fisico sui dati quando essi vengono spostati nel Cloud. Sono pure menzionati altri argomenti, quali chi è responsabile della confidenzialità, integrità e disponibilità dei dati.
Portability and Interoperability	La capacità di spostare dati/servizi da un fornitore ad un altro, o riportarli all'interno dell'impresa. Vengono discussi pure argomenti inerenti l'interoperabilità tra fornitori.

Domini Operativi

Dominio	**Argomenti**
Traditional Security, Business Continuity and Disaster Recovery	Come il Cloud Computing agisce sui processi e le procedure operative correntemente utilizzate per implementare la sicurezza, la business continuity ed il disaster recovery. Il punto centrale è la discussione e la disamina dei possibili rischi connessi al Cloud Computing, nella speranza di aumentare il dialogo ed il dibattito intorno alla schiacciante richiesta di migliori modelli per la gestione del rischio. Inoltre, la sezione tenta di indicare le aree in cui il Cloud Computing potrebbe esser d'aiuto nel ridurre certi rischi di sicurezza, oppure in quali aree potrebbe comportare un aumento del rischio stesso.
Data Center Operations	Come valutare l'architettura di data center e l'operatività di un fornitore. Questa sezione vuol fornire un aiuto agli utenti nell'identificare le caratteristiche comuni dei data center che potrebbero essere di detrimento per i servizi, e quelle che sono fondamentali per la stabilità a lungo termine.
Incident Response, Notification and Remediation	Corretto ed adeguato rilevamento, notifica e ripristino degli incidenti. Questa sezione tenta la trattazione dei dispositivi che dovrebbero essere messi in atto sia presso il fornitore che presso l'utente per rendere possibile una corretta gestione degli incidenti e delle attività forensi.
Application Security	La messa in sicurezza del software applicativo eseguito nel Cloud o che in

Dominio	Argomenti
	esso debba essere sviluppato. Questo include argomenti quali l'opportunità della migrazione o del progetto di una applicazione da eseguire nel Cloud, e in caso ciò avvenisse, che tipo di piattaforma Cloud (SaaS, PaaS, or IaaS) sia la più adeguata. Sono pure discussi alcuni specifici argomenti di sicurezza correlati al Cloud.
Encryption and Key Management	Identificazione del corretto utilizzo della cifratura e gestione scalabile delle chiavi. Questa sezione non è prescrittiva, ma è più informativa, trattando il perché ciò sia necessario ed identificando i problemi che potrebbero sorgere durante l'adozione, sia nella protezione dell'accesso alle risorse che per la protezione dei dati.
Identity and Access Management	Gestire le identità e sfruttare i servizi di directory per il controllo accessi. Il focus è sui problemi rilevabili quando si estende l'identità di un'impresa nel Cloud. Questa sezione fornisce informazioni sul come valutare la disponibilità di un ente ad adottare la gestione dell'identità e degli accessi (IAM) basato sul Cloud.
Virtualization	L'uso della tecnologia di virtualizzazione nel Cloud Computing. Questo dominio tratta argomenti quali i rischi connessi con la multi-tenancy, l'isolamento delle VM, la co-residenza delle VM, le vulnerabilità degli hypervisor, ecc. Particolare attenzione viene data ai problemi di sicurezza connessi alla virtualizzazione dei sistemi/hardware, piuttosto che una panoramica più generale di tutte le forme di virtualizzazione.

Sommario

Le chiavi per comprendere come l'architettura Cloud impatta l'architettura della sicurezza sono un comune e conciso lessico, unito ad una consistente tassonomia delle offerte, mediante i quali i servizi Cloud e l'architettura possono essere decostruiti, mappati nei confronti di un modello di controlli di sicurezza compensativi ed operativi, quadri di stima del rischio, e quadri di gestione, ed a sua volta nei confronti degli standard di conformità.

Comprendere se e come cambiano l'architettura, la tecnologia, il processo, ed i requisiti del capitale umano, quando si implementa il Cloud Computing è cruciale.

Senza una chiara comprensione delle implicazioni architetturali di più alto livello, è impossibile trattare le problematiche più dettagliate in modo razionale.

Questa panoramica architetturale, insieme con le dodici aree di attenzione, forniranno al lettore un solido fondamento per la valutazione, la messa in esercizio, la gestione ed il governo della sicurezza in ambienti di Cloud Computing.

Hanno contribuito: Glenn Brunette, Phil Cox, Carlo Espiritu, Christofer Hoff, Mike Kavis, Sitaraman Lakshminarayanan, Kathleen Lossau, Erik Peterson, Scott Matsumoto, Adrian Seccombe, Vern Williams, Richard Zhou

Sezione II. Governare il Cloud

Dominio 2: Governance e Gestione del rischio d'impresa

Un'efficace governance e una gestione del rischio d'impresa negli ambienti Cloud Computing derivano da processi di information security governance ben sviluppati, come parte dei complessivi obblighi di diligenza nella corporate governance dell'impresa. Processi di information security governance ben sviluppati dovrebbero sfociare in programmi di gestione del rischio d'impresa che risultino scalabili con il business, ripetibili all'interno dell'impresa, misurabili, sostenibili, difendibili, in continuo miglioramento ed efficaci dal punto di vista dei costi, in modo continuo.

I problemi fondamentali di governance e di gestione del rischio d'impresa nel Cloud Computing riguardano l'identificazione e l'implementazione di strutture organizzative, processi e controlli appropriati al fine di mantenere l'efficacia della governance della sicurezza dell'informazione, della gestione del rischio e della compliance. Le imprese dovrebbero inoltre assicurare una sicurezza dell'informazione ragionevole lungo l'intera catena di approvvigionamento dell'informazione, che comprende i fornitori e i clienti dei servizi di Cloud Computing e i fornitori terzi a supporto, in qualsiasi modello di sviluppo del Cloud.

Raccomandazioni di governance

- ✓ Una porzione dei risparmi ottenuti dai servizi di Cloud Computing deve essere investita in un maggiore esame delle capacità di sicurezza del provider, nell'applicazione di controlli di sicurezza e in periodiche valutazioni dettagliate e in audit, per garantire che i requisiti siano continuamente soddisfatti.

- ✓ Sia i fornitori che i clienti del servizio di Cloud Computing dovrebbero sviluppare una robusta governance della sicurezza delle informazioni, indipendentemente dal modello di servizio o di sviluppo. La governance della sicurezza delle informazioni dovrebbe essere frutto di una collaborazione tra clienti e fornitori per raggiungere obiettivi concordati che sostengano gli obiettivi di business e il programma di sicurezza delle informazioni. In una gestione collaborativa della governance della sicurezza informazioni e del rischio, il modello di servizio può tarare i ruoli definiti e le responsabilità (sulla base dei rispettivi ambiti di controllo di utente e provider), mentre il modello di sviluppo può definire responsabilità e aspettative (sulla base della valutazione del rischio).

- ✓ Le imprese utenti dovrebbero includere la revisione di specifiche strutture e processi di governance della sicurezza delle informazioni delle potenziali imprese fornitrici, come pure quella di specifici controlli di sicurezza. I processi e le capacità di Governance della sicurezza del provider devono essere sottoposti a valutazione della sufficienza, maturità e coerenza coi processi di gestione di sicurezza dell'informazione dell'impresa utente. I controlli di sicurezza delle informazioni del provider dovrebbero essere basati sul rischio in modo dimostrabile e supportare chiaramente questi processi di gestione.

- ✓ Strutture e processi di governo collaborativi tra clienti e fornitori devono essere identificati come necessari, sia come parte della progettazione e sviluppo dell'erogazione del servizio, sia come protocolli di valutazione dei rischi e gestione del rischio del servizio, e poi incorporati negli accordi di servizio.

- ✓ I reparti di sicurezza dovrebbero essere coinvolti durante la creazione degli accordi sul livello di servizio e degli obblighi contrattuali, per garantire che i requisiti di sicurezza possano essere imposti contrattualmente.

- ✓ Metriche e standard per la misurazione delle prestazioni e dell'efficacia delle gestione della sicurezza delle informazioni dovrebbero essere istituite prima del passaggio al Cloud. Come minimo, le imprese dovrebbero capire e documentare le loro attuali metriche e come queste cambieranno nel momento in cui l'operatività sarà spostata nel Cloud, dove un provider potrebbe utilizzare metriche diverse (potenzialmente non compatibili).

- ✓ Ovunque possibile, le metriche e gli standard di sicurezza (in particolare quelle legate ai requisiti legali e di conformità) dovrebbero essere incluse in ogni Accordo sul Livello di Servizio e in qualsiasi contratto. Questi standard e metriche dovrebbero essere documentati e dimostrabili (sottoponibili ad audit).

Raccomandazioni sulla gestione del rischio d'impresa

Come per ogni nuovo processo aziendale, è importante seguire le best practices di gestione del rischio. Queste pratiche devono essere proporzionate al vostro specifico uso dei servizi nel Cloud, che possono spaziare da innocue e temporanee elaborazioni di dati a processi aziendali mission critical riguardanti informazioni altamente sensibili. Una discussione completa sulla gestione del rischio d'impresa e della gestione del rischio dell'informazione va oltre gli scopi di questa guida, ma qui sono raccolte alcune raccomandazioni specifiche per il Cloud che si possono incorporare nei vostri processi esistenti di gestione del rischio.

- ✓ A causa della mancanza di controllo fisico sull'infrastruttura in molte implementazioni del Cloud Computing, gli Accordi sul Livello del Servizio, i requisiti contrattuali e la documentazione del provider giocano un ruolo più importante nella gestione del rischio rispetto alle tradizionali infrastrutture detenute dalle aziende.

- ✓ A causa degli aspetti di approvvigionamento on-demand e del multi-tenancy del Cloud Computing, forme tradizionali di audit e di valutazione potrebbero non essere disponibili, o potrebbero essere modificate. Per esempio, alcuni provider limitano le valutazione di vulnerabilità e i penetration test, mentre altri limitano la disponibilità degli audit log e il monitoraggio delle attività. Se questi aspetti sono ritenuti necessari dalle vostre politiche interne, potrebbe essere necessario ricercare opzioni di valutazioni alternative, o un provider alternativo meglio allineato ai vostri requisiti di gestione del rischio.

- ✓ Relativamente all'uso dei servizi nel Cloud per funzioni critiche per l'impresa, l'approccio basato sulla gestione del rischio dovrebbe includere l'identificazione e la valutazione degli asset, l'identificazione e l'analisi delle minacce e delle vulnerabilità, e il loro potenziale impatto sugli asset (scenari di rischio e di incidente), l'analisi delle probabilità degli eventi/scenari, dei livelli e criteri di accettazione del rischio approvati dal Management, e lo sviluppo di piani di trattamento del rischio con opzioni multiple (controllare, evitare, trasferire, accettare). I risultati dei piani di trattamento del rischio dovrebbero essere incorporati negli Accordi di Servizio.

- ✓ Gli approcci alla valutazione del rischio da parte di provider e utenti dovrebbero essere costanti, con coerenza dei criteri di analisi degli impatti e di definizione delle probabilità. L'utente e il provider dovrebbero sviluppare congiuntamente gli scenari di rischio per il servizio nel Cloud; questo dovrebbe essere intrinseco al disegno del servizio del provider per l'utente, e alla valutazione del rischio del servizio cloud da parte dell'utente.

- ✓ L'inventario degli asset dovrebbe tenere conto degli assets che supportano i servizi nel cloud e che sono sotto il controllo del provider. Gli schemi di classificazione e valutazione degli Asset dovrebbero essere costanti tra provider e utente.

- ✓ Il servizio e non solo il fornitore dovrebbe essere soggetto alla valutazione del rischio. L'uso dei servizi nel Cloud, ed in particolare i modelli di servizio e di implementazione utilizzati, dovrebbero essere costanti sia con gli obiettivi di gestione del rischio dell'impresa sia con gli obiettivi di business.

- ✓ Quando un provider non è in grado di dimostrare processi di gestione del rischio onnicomprensivi ed efficaci in associazione ai suoi servizi, i clienti dovrebbero valutare attentamente se avvalersi del fornitore così come le proprie eventuali capacità di compensare le potenziali lacune nella gestione del rischio.

- ✓ I clienti dei servizi Cloud dovrebbero chiedere se il loro management ha definito le tolleranze al rischio rispetto ai servizi Cloud ed accettato ogni rischio residuo legato all'utilizzo dei servizi Cloud.

Raccomandazioni di Information Risk Management

L'Information Risk Management (IRM) è l'atto di allineare l'esposizione al rischio alla capacità di gestirlo con la propensione al rischio del proprietario dei dati. In questo modo, risulta essere il mezzo primario di supporto decisionale per le risorse informative disegnate per proteggere la confidenzialità, integrità e disponibilità degli asset informativi.

- ✓ Adottare un modello strutturato di gestione del rischio per valutare l'IRM, e un modello di maturità per valutare l'efficacia del vostro modello di IRM.

- ✓ Stabilire requisiti contrattuali e controlli tecnologici appropriati per raccogliere i dati necessari a prendere decisioni legate al rischio delle informazioni (per esempio, uso delle informazioni, controllo degli accessi, controlli di sicurezza, ubicazioni, ecc.)

- ✓ Adottare un processo per determinare l'esposizione al rischio prima di sviluppare i requisiti per un progetto di Cloud Computing. Nonostante le categorie di informazioni richieste per capire l'esposizione al rischio e le capacità di gestione siano generali, le effettive metriche probatorie raccolte sono connaturate alla natura del modello SPI del Cloud Computing e a ciò che può essere concretamente raccolto in termini di servizio.

- ✓ Quando si utilizza SaaS, la stragrande maggioranza delle informazioni dovrà essere fornita dal service provider. Le imprese dovranno strutturare processi analitici di raccolta delle informazioni all'interno degli obblighi contrattuali del servizio SaaS.

- ✓ Quando si utilizza PaaS, strutturare la raccolta delle informazioni come sopra per il SaaS, ma quando possibile includetre la possibilità di distribuire e raccogliere le informazioni dai controlli e di creare le disposizioni contrattuali per verificare l'efficacia di quei controlli.

- ✓ Quando si utilizza un provider di servizi IaaS service, costruire la trasparenza delle informazioni all'interno di un linguaggio contrattuale per le informazioni richieste dall'analisi del rischio.

- ✓ I provider di servizi Cloud dovrebbero includere metriche e controlli per assistere i clienti nell'implementazione dei loro requisiti di Information Risk Management.

Raccomandazioni sulla gestione delle terze parti

- ✓ I clienti dovrebbero vedere i servizi e la sicurezza del Cloud come problemi di sicurezza nella catena di approvvigionamento. Ciò significa esaminare e valutare la catena di approvvigionamento del provider (relazioni e dipendenze) per quanto possibile. Questo significa anche esaminare la gestione delle terze parti del provider.

- ✓ La valutazione dei service providers di terze parti dovrebbe riguardare in modo specifico le politiche, i processi e le procedure di gestione dell'incidente, business continuity e disaster recovery; e dovrebbe includere la revisione delle strutture di co-ubicazioni e di backup. Ciò dovrebbe comprendere la revisione della valutazione interna di conformità del provider alle proprie politiche e procedure, e la valutazione delle metriche del provider per fornire informazioni ragionevoli riguardanti le prestazioni e l'efficacia dei suoi controlli in queste aree.

- ✓ I piani di Business Continuity e Disaster Recovery dell'utente dovrebbero includere scenari riguardanti l'interruzione dei servizi del provider, e l'interruzione dei servizi o delle capacità dipendenti da terze parti di cui il provider si avvale. IL test di questa parte del piano dovrebbe essere coordinata con il cloud provider.

- ✓ Le strutture e i processi di information security governance, gestione del rischio, e compliance del provider dovrebbero essere sottoposti ad una valutazione globale:

    - Richiedere documentazione chiara su come vengono svolte le valutazioni del rischio delle strutture e dei servizi, l'auditing delle debolezze nei controlli, la frequenza delle valutazioni, e su come vengono mitigate le debolezze dei controlli in modo tempestivo.
    - Richiedere la definizione di ciò che il provider considera un servizio critico, i fattori di successo per l'information security, gli indicatori principali di performance, e come questi sono misurati nell'ambito dei servizi IT e dell'Information Security Management.
    - Rivedere la completezza dei processi di raccolta, la valutazione e la comunicazione dei requisiti del provider in ambito legale, normativo, contrattuale e dell'industria di riferimento.

- Investigare in modo approfondito (due diligence) i contratti e i termini d'uso per determinare ruoli, compiti e responsabilità. Assicuratevi di compiere una revisione legale, inclusiva di una valutazione dell'applicabilità delle disposizioni contrattuali e delle leggi locali in giurisdizioni straniere o di un altro stato.
- Determinare se i requisiti di due diligence comprendono tutti gli aspetti materiali della relazione con il cloud provider, come le condizioni finanziarie del provider, la reputazione (ad esempio col controllo delle referenze), i controlli, i piani e i test di disaster recovery, le assicurazioni, le capacità di comunicazione, e l'uso di subappalti.

Hanno contribuito: Jim Arlen, Don Blumenthal, Nadeem Bukhari, Alex Hutton, Michael Johnson, MS Prasad, Patrick Sullivan

Dominio 3: Indagine Legale ed Elettronica

Il Cloud Computing crea nuove dinamiche nella relazione tra un'impresa e le sue informazioni, dovute alla presenza di una terza parte: il cloud provider. Ciò porta alla creazione di nuove sfide nella comprensione di come le leggi si applichino a un'ampia varietà di scenari di gestione delle informazioni.

Un'analisi completa degli aspetti legali legati al Cloud Computing richiede di considerare le dimensioni funzionali, giurisdizionali e contrattuali.

- La dimensione funzionale implica la necessità di determinare quali funzioni e servizi nel Cloud Computing hanno implicazione legali per i partecipanti e le parti interessate (stakeholders).

- La dimensione giurisdizionale riguarda il modo in cui i governi amministrano le leggi e le normative che impattano sui servizi di Cloud Computing, le parti interessate e il patrimonio di dati coinvolti.

- La dimensione contrattale riguarda le strutture, i termini e le condizioni contrattuali, e i meccanismi di attuazione tramite cui le parti interessate in ambienti Cloud Computing possono indirizzare e gestire le problematiche legali e di sicurezza.

Il Cloud Computing in generale si può distinguere dal tradizionale outsourcing in tre modi: i tempi del servizio (on-demand e intermittente), l'anonimità dell'identità del/dei service provider e l'anonimità della ubicazione del/dei server coinvolto/i. Prendendo in considerazione nello specifico IaaS e PaaS, buona parte dell'orchestrazione, configurazione e sviluppo software è svolto dal cliente – quindi molta della responsabilità non può essere trasferita al cloud provider.

La conformità con i recenti requisiti amministrativi e legislativi nelle diverse parti del mondo forzano una maggiore collaborazione tra i professionisti legali e di tecnologia. Ciò risulta particolarmente vero nel Cloud Computing, a causa delle potenziali nuove aree di rischio legale create dalla natura distribuita del cloud, rispetto alle infrastrutture tradizionali o in outsourcing.

Numerose leggi e normative di conformità negli Stati Uniti e nell'Unione Europea imputano la responsabilità legale ai subappaltatori o richiedono alle entità aziendali di imporre su di essi contrattualmente la responsabilità legale.

I tribunali ora stanno realizzando che i servizi di information security management sono critici per decidere se le informazioni digitali possono essere accettate come prova. Se questo è un problema per le infrastrutture IT tradizionali, lo è in modo ancor più preoccupante per il Cloud Computing a causa della mancanza di storia del diritto nel Cloud.

Raccomandazioni

- ✓ I clienti e i cloud provider devono possedere una mutua comprensione dei rispettivi ruoli e responsabilità legate all'indagine elettronica, incluse quelle attività come la conduzione della controversia, le ricerche investigative, chi fornirà la testimonianza di esperti, ecc.

- ✓ Si consiglia ai Cloud provider di assicurarsi che i propri sistemi di sicurezza informatica rispondano ai requisiti dei clienti riguardo la conservazione dei dati in modo da garantirne l'autenticità e affidabilità, includendo sia le informazioni primarie che secondarie, come metadata e file di log.

- ✓ I dati custoditi dal provider del servizio cloud devono essere sottoposti a una tutela equivalente a quella dei dati posseduti dal proprietario o custode originale.

- ✓ Pianificare la conclusione attesa o inattesa del rapporto di servizio nella fase di negoziazione del contratto, e la riconsegna ordinaria o la cancellazione sicura degli asset.

- ✓ Due diligence pre-contrattuale, negoziazione dei termini contrattuali, monitoraggio post-contrattuale, e conclusione del contratto, e la transizione della custodia dei dati sono elementi che il cliente di un servizio cloud deve richiedere.

- ✓ Conoscere dove il provider dei servizi cloud ospiterà i dati è un prerequisitio all'implementazione delle misure richieste per assicurare la compliance con le leggi locali che limitano il flusso oltreconfine dei dati.

- ✓ Come custode dei dati personali dei suoi impiegati o dei clienti, e delle altre proprietà intellettuali aziendali, un'azienda che utilizza i servizi di Cloud Computing dovrebbe assicurarsi di mantenere il possesso dei propri dati nel loro formato originale e autenticabile.

- ✓ Numerosi problemi di sicurezza, come sospette violazioni dei dati, devono essere indirizzati in specifiche disposizioni dell'accordo di servizio, che chiariscano i rispettivi impegni del provider del servizio cloud e del cliente.

- ✓ Il provider del servizio cloud e il cliente dovrebbero avere un processo unificato per rispondere alle citazioni in giudizio e ad altre richieste legali.

- ✓ L'accordo sui servizi cloud deve permettere al cliente dei servizi cloud o a una terza parte designata di monitorare le performance del provider del servizio e di verificare la presenza di vulnerabilità del sistema.

- ✓ Le parti di un accordo di servizio cloud dovrebbero assicurare che l'accordo stesso anticipi i problemi relativi al recupero dei dati del cliente dopo il termine della relazione contrattuale.

Hanno contribuito: Tanya Forsheit, Scott Giordano, Francoise Gilbert, David Jackson, Peter McLaughlin, Jean Pawluk, Jeffrey Ritter

Dominio 4: Compliance e Audit

Con lo sviluppo da parte del Cloud Computing di un mezzo fattibile e redditizio di mettere in outsourcing interi sistemi o interi processi di business, il mantenimento della conformità (compliance) con le vostre policy di sicurezza e i vari requisiti normativi e legislativi a cui è soggetta la vostra impresa può divenire più difficile da ottenere e ancora più complicato da dimostrare ai revisori ed ai verificatori.

Delle molte normative che riguardano l'information technology a cui le imprese devono essere conformi, poche sono state scritte avendo in mente il Cloud Computing. I revisori ed i verificatori potrebbero non avere familiarità con il Cloud Computing in generale o con un dato servizio cloud in particolare. Se questo è il caso, è compito del cliente capire:

- L'applicabilità delle normative in merito all'uso di una dato servizio cloud.
- La suddivisione delle responsabilità di conformità tra il cloud provider e il cliente.
- La capacità del Cloud provider di fornire le evidenze richieste per la conformità.
- Il ruolo del cliente del servizio cloud nel colmare le distanze tra il cloud provider e chi esegue la revisione/verifica.

Raccomandazioni

- ✓ Coinvolgere i gruppi legali e contrattuali. I termini di servizio standard del cloud provider potrebbero non essere adatti alle vostre esigenze di conformità; per questo è utile avere sia personale legale che contrattuale coinvolto sin dall'inizio per assicurarsi che le disposizioni contrattuali del servizio cloud siano adeguate agli obblighi di conformità e di revisione.

- ✓ Clausola sul diritto di Revisione. I clienti avranno spesso la necessità di sottoporre a revisione il cloud provider, data la natura dinamica del cloud e dell'ambiente normativo. Una clausola contrattuale di diritto alla revisione dovrebbe essere ottenuta ogni qualvolta sia possibile, particolarmente quando si usa il cloud provider per un servizio per il quale il cliente ha delle responsabilità di conformità alla normativa. Con l'andar del tempo, il bisogno di questo diritto dovrebbe essere ridotto e in molti casi sostituito da appropriate certificazioni del cloud provider, collegate alle nostre raccomandazioni per la certificazione ISO/IEC 27001 trattate successivamente in questa sezione.

- ✓ Analizzare l'ambito della conformità. Determinare se le normative di conformità a cui l'impresa è soggetta saranno impattate dall'uso dei servizi cloud, per un dato insieme di applicazioni e dati.

- ✓ Analizzare l'impatto delle normative sulla sicurezza dei dati. I potenziali utenti finali dei servizi di Cloud Computing dovrebbero considerare quali applicazioni e dati stanno pensando di spostare sui servizi cloud, e con che portata questi saranno soggetti a normative di conformità.

- ✓ Revisionare i Partner e i Service Provider rilevanti. Questa è un'indicazione generale per assicurare che la relazione coi service provider non impatti negativamente con la conformità. Valutare quali service provider stanno elaborando dati che sono soggetti a normative di conformità e poi valutare i

controlli di sicurezza forniti da quei service provider è fondamentale. Molte normative di compliance adottano un linguaggio specifico riguardo la valutazione e gestione del rischio legato a terze parti fornitrici. Come per i servizi IT e di business non legati al cloud, le imprese devono capire quali dei loro business partner sul cloud stanno elaborando dati soggetti a normative di conformità.

- ✓ Capire le responsabilità contrattuali legate alla protezione dei dati e i relativi contratti. Il modello di servizi nel cloud in una certa misura impone se il cliente o il fornitore di servizi nel cloud è responsabile per l'implementazione dei controlli di sicurezza. In uno scenario di implementazione IaaS, il cliente ha un livello di controllo e di responsabilità più alto che in uno scenario SaaS. Da un punto di vista dei controlli di sicurezza, questo significa che i clienti IaaS avranno il compito di implementare molti dei controlli di sicurezza ai fini della conformità alla normativa. In uno scenario SaaS, il fornitore di servizi Cloud deve fornire i controlli necessari. Da un punto di vista contrattuale, capire gli specifici requisiti e assicurare che il contratto e gli accordi di servizio nel cloud li indirizzano in modo adeguato, è fondamentale.

- ✓ Analizzare gli impatti delle normative sull'infrastruttura del provider. Nell'area infrastrutturale, il passaggio ai servizi nel cloud richiede una altrettanto accurata analisi. Alcuni requisiti di normativa specificano dei controlli che sono difficili o impossibili da raggiungere in certe tipologie di servizi cloud.

- ✓ Analizzare l'impatto delle normative su policy e procedure. Spostare dati ed applicazioni sui servizi nel cloud avrà probabilmente un impatto su policy e procedure. I clienti dovrebbero valutare quali policy e procedure in relazione alle normative dovranno subire modifiche. Esempi di policy e procedure includono i report sulle attività, logging, conservazione dei dati, risposta agli incidenti, verifica dei controlli e policy sulla privacy.

- ✓ Preparare evidenze di come ogni requisito viene soddisfatto. Raccogliere evidenze di conformità attraverso la moltitudine di normative di compliance e di requisiti rappresenta una sfida. I clienti dei servizi cloud dovrebbero sviluppare processi di raccolta e memorizzazione delle evidenze di conformità inclusive di audit log e report sulle attività, copie delle configurazioni dei sistemi, report sulla gestione dei cambiamenti, e il risultato di altre procedure di test. A seconda del modello di servizio cloud, il cloud provider potrebbe dover fornire gran parte di queste informazioni.

- ✓ Qualifica e selezione del Revisore. In molti casi l'impresa non ha voce in capitolo nella scelta dei revisori o degli ispettori di sicurezza. Se un'impresa può dare input alla selezione, è altamente consigliabile scegliere un revisore "cloud aware" poiché molti potrebbero non avere familiarità con le sfide del cloud e della virtualizzazione. Richiedere familiarità con la nomenclatura IaaS, PaaS, e SaaS è un buon punto di partenza.

- ✓ Cloud Provider SAS 70 Type II. I provider dovrebbero possedere come minimo questa relazione del revisore, in quanto esso fornisce un punto di riferimento riconoscibile per chi effettua revisione e verifica. Poiché una revisione SAS 70 Type II assicura solo che i controlli sono implementati come documentato, è ugualmente importante capire l'ambito della revisione SAS 70 e se questi controlli soddisfano i vostri requisiti.

- ✓ Roadmap del cloud provider sulla certificazione ISO/IEC 27001/27002. I cloud provider che desiderano fornire servizi mission critical dovrebbero adottare lo standard ISO/IEC 27001 per i sistemi di information security management. Se il provider non ha ottenuto la certificazione ISO/IEC 27001, dovrebbe dimostrare allineamento alle pratiche ISO 27002.

- ✓ ISO/IEC 27001/27002 Scoping. La Cloud Security Alliance invia un appello all'industria al fine di allineare i cloud provider alla certificazione ISO/IEC 27001, per assicurare che l'analisi non trascuri criteri di certificazione critici.

Hanno contribuito: Nadeem Bukhari, Anton Chuvakin, Peter Gregory, Jim Hietala, Greg Kane, Patrick Sullivan

Dominio 5: Gestione del ciclo di vita dell'informazione

Uno degli obiettivi principali dell'Information Security è quello di proteggere i dati fondamentali che alimentano i nostri sistemi e le nostre applicazioni. Nella transizione verso il Cloud Computing, i nostri metodi tradizionali di mettere in sicurezza i dati devono raccogliere la sfida delle architetture basate sul Cloud. Elasticità, contratti multipli, nuove architetture fisiche e logiche e controlli astratti, richiedono nuove strategie di protezione dei dati. Con i molti modelli di Cloud disponibili, stiamo trasferendo i dati in ambienti esterni – o in ambienti pubblici – in modi impensabili solo fino a pochi anni fa.

Gestione del Ciclo di vita dell'informazione

Il ciclo di vita della sicurezza dei dati differisce dalla gestione del ciclo di vita dell'informazione, in quanto riflette i diversi bisogni dell'audience della security. Il Ciclo di vita della sicurezza dei dati consiste di sei fasi:

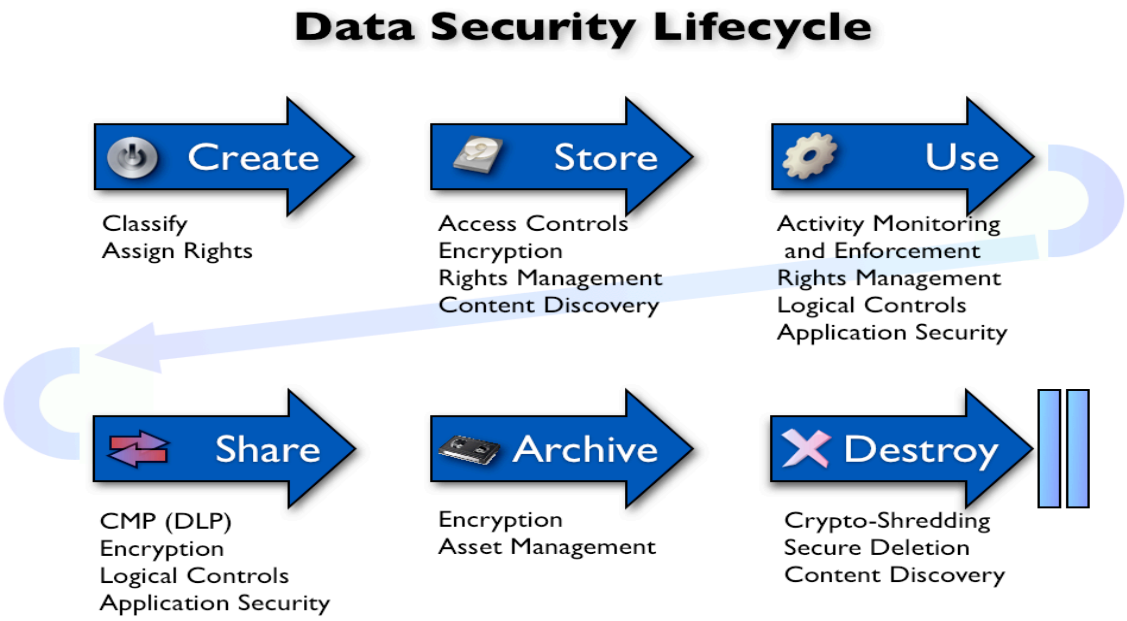

Figura 8: Schematizzazione del ciclo di vita sicuro dei dati

Le sfide chiave che riguardano il ciclo di vita della sicurezza dei dati nel Cloud, includono i seguenti aspetti:

Sicurezza dei dati. Confidenzialità, Integrità, Disponibilità, Autenticità, Autorizzazione, Autenticazione, e Non-Rifiuto (*Non-Repudiation*)

Ubicazione dei dati. Deve essere assicurato che i dati, incluse tutte le copie e i backup, siano conservati solo in zone geografiche consentite dal contratto, dagli SLA, e/o da normative. Per esempio l'uso di "storage conforme" reso obbligatorio dall'Unione Europea per la conservazione di informazioni sulla sanità in formato

elettronico, può essere una sfida aggiuntiva per il proprietario dei dati e per il fornitore di servizi Cloud.

Rimanenza o persistenza dei dati. I dati devono essere efficacemente e completamente rimossi per essere ritenuti "distrutti". Di conseguenza devono essere disponibili, e usate quando richiesto, delle tecniche per localizzare completamente ed efficacemente i dati nel Cloud, per cancellare/distruggere i dati, e per assicurare che i dati siano completamente rimossi o resi irrecuperabili.

Commistione dei dati con altri clienti del Cloud. I dati specialmente quelli classificati/sensibili – non devono essere commistionati con i dati di altri clienti senza che vi siano i necessari controlli di compensazione durante l'uso, la conservazione o il transito. Mischiare o commistionare i dati rappresenta una sfida al sorgere di preoccupazioni riguardo la sicurezza dei dati e alla loro ubicazione geografica.

Backup dei dati e schemi di ripristino per recovery e restoration. I dati devono essere disponibili e gli schemi di backup e recovery per il Cloud devono essere presenti ed efficaci al fine di prevenire la perdita di dati, la sovrascrittura involontaria di dati e la distruzione. Non date per assunto che venga effettuato il backup dei dati nel Cloud e che siano recuperabili.

Data discovery. Il continuo interesse dei sistemi legali verso la reperibilità elettronica, deve portare i fornitori di servizi Cloud e i proprietari dei dati a focalizzarsi sulla ricerca dei dati e sull'assicurare alle autorità legali e normative che tutti i dati richiesti siano stati recuperati. Nel Cloud è estremamente difficile rispondere a questa domanda e sono richiesti controlli amministrativi, tecnici e legali quando necessario.

Aggregazione e inferenza dei dati. Con i dati nel Cloud ci sono preoccupazioni ulteriori sull'aggregazione e sull'inferenza dei dati che possono portare a violare la confidenzialità di informazioni ritenute sensibili e confidenziali. Di conseguenza è necessario che siano messe in atto pratiche per assicurare al proprietario dei dati e a tutte le figure coinvolte, che i dati siano sempre protetti da ingegnose violazioni, quando gli stessi sono commistionati e/o aggregati, al fine di non rivelare le informazioni protette (per es. file medici contenenti nomi e informazioni mediche miste a dati anonimi ma contenenti lo stesso "campo incrociato")

Raccomandazioni

- ✓ Capire come l'integrità viene mantenuta e come una sua compromissione viene individuata e segnalata ai clienti. La stessa raccomandazione si applica, quando appropriato, alla confidenzialità.

- ✓ Il Cloud Computing Provider deve assicurare al proprietario dei dati che gli sarà garantita la piena apertura (nota come 'trasparenza') riguardo pratiche e procedure di sicurezza così come stabilito nei loro SLA.

- ✓ Accertare l'identificazione specifica di tutti i controlli utilizzati durante il ciclo di vita dei dati. Garantire le specifiche di cui l'entità è responsabile per ciascun controllo fra il proprietario dei dati e i Cloud Services Provider.

- ✓ Mantenere una filosofia di base: sapere dove sono i propri dati. Accertare la conoscenza della posizione geografica dello storage. Definire tutto questo negli

SLA e nei contratti stipulati. Assicurarsi che controlli circa le restrizioni sul paese di ubicazione dello storage siano definiti e applicati.

- ✓ Capire le circostanze in cui lo storage possa essere sequestrato da terze parti o da autorità governative. Accertarsi che la SLA definita con il Cloud Provider includa il preavviso al proprietario dei dati (dove possibile) che le proprie informazioni sono state o saranno sequestrate.

- ✓ In alcuni casi, un mandato o un'ordinanza di accesso ai dati può essere avanzata nei confronti del Cloud Computing Services Provider. In questo caso, quando il provider ha la custodia dei dati del cliente, al Cloud Services Provider dovrebbe essere richiesto di informare il proprietario dei dati del fatto che il Cloud Services Provider è obbligato a rivelare i dati alle autorità.

- ✓ Un sistema sanzionatorio dovrebbe essere incluso nel contratto fra il proprietario dei dati e il Cloud Services Provider. In particolare, i dati che possono essere soggetti a leggi locali o internazionali sulla violazione dei dati (ad esempio, la California Senate Bill 1386 o il nuovo HIPAA), dovrebbero essere protetti dal Cloud Services Provider.

- ✓ E' responsabilità del proprietario dei dati determinare chi debba accedervi, quali sono i loro permessi e privilegi e sotto quali condizioni questi permessi di accesso vengono forniti. Il proprietario dei dati deve mantenere una policy predefinita di tipo restrittivo ("Default Deny All"), sia per i dipendenti del Cloud Services Provider, sia per i dipendenti del proprietario dei dati.

- ✓ I Cloud Services Provider dovrebbero offrire contratti che garantiscano il divieto di accesso ai dati come filosofia fondamentale (Accesso di tipo restrittivo). Questo si applica specificatamente ai dipendenti del Cloud Services Provider e ai loro clienti, oltre che ai dipendenti del proprietario dei dati e al personale autorizzato.

- ✓ E' responsabilità del proprietario dei dati definire e identificare la classificazione dei dati. E' invece responsabilità del Cloud Services Provider di applicare i requisiti di accesso definiti dal proprietario dei dati e basati sulla classificazione degli stessi. Tali responsabilità dovrebbero essere definite nel contratto,rispettate e verificate per conformità.

- ✓ Quando un cliente è costretto a divulgare informazioni, non deve avvenire contaminazione dei dati. Non solo il proprietario dei dati deve assicurarsi che tutti i dati richiesti da mandati, sentenze etc. siano intatti e forniti in maniera opportuna; il proprietario dei dati deve anche assicurare che nessun altro dato sia divulgato.

- ✓ Crittografare i dati a riposo e in transito

- ✓ Identificare i confini di fiducia (trust boudaries) per tutta l'architettura IT e gli strati di astrazione. Assicurarsi che i sottosistemi attraversino i trust boundaries solo all'occorrenza e con l'accortezza di prevenire la divulgazione dei dati non autorizzata, la loro alterazione o la loro distruzione.

- ✓ Capire quali tecniche di compartimentazione sono impiegate dal provider per isolare i suoi clienti l'uno dall'altro. Un provider può usare una varietà di metodi in base al tipo e numero di servizi offerti.

- ✓ Capire le capacità di ricerca dei dati del Cloud provider e le limitazioni quando tenta di vedere "dentro" il dataset per una data discovery

- ✓ Capire come viene gestita la crittografia in uno storage rivolto a più destinatari (muti-tenant). C'è una singola chiave per tutti i proprietario dei dati, una chiave per proprietario dei dati o chiavi multiple per proprietario dei dati? C'è un sistema per prevenire che diversi proprietari dei dati abbiano le stesse chiavi di crittografia?

- ✓ I proprietari dei dati devono richiedere al fornitore di servizi Cloud di assicurare che i loro dati di backup non siano mischiati con i dati di altri clienti

- ✓ Capire i processi di dismissione dello storage del Cloud provider. La distruzione dei dati è estremamente difficile in un ambiente con molti utenti e il Cloud provider deve usare una forte crittografia dello storage al fine di rendere illeggibili i dati quando lo storage viene riciclato, dismesso, o vi si acceda con qualsiasi mezzo, al di fuori di applicazioni, processi e entità autorizzati.

- ✓ E' responsabilità del proprietario dei dati la conservazione dei dati e la schedulazione della distruzione,. E' responsabilità del fornitore di servizi Cloud distruggere i dati quando richiesto, con particolare enfasi nella distruzione di tutti i dati in tutti i posti, inclusi quelli in strutture dati e sui media. Il proprietario dei dati dovrebbe fare rispettare e controllare questa pratica, se possibile.

- ✓ Capire la segregazione logica dell'informazione e i controlli protettivi implementati

- ✓ Capire le restrizioni dovute alla privacy inerenti ai dati affidati alla tua azienda; potrebbe essere necessario designare il proprio Cloud provider come un particolare tipo di partner prima di affidargli il trattamento di queste informazioni.

- ✓ Capire le policy e procedure del Cloud provider per la conservazione dei dati, la distruzione e come si raffrontano con le policy organizzative interne. Fare attenzione che l'assicurazione della conservazione dei dati può essere facilmente dimostrabile dal Cloud provider, mentre la distruzione può essere molto difficile.

- ✓ Negoziare penali pagabili dal Cloud provider per perdita di dati per assicurarsi che il problema venga preso seriamente. Se praticabile, il cliente dovrebbe cercare di recuperare tutti i costi per perdita di dati, come parte del proprio contratto con il provider. Se impraticabile, il cliente dovrebbe verificare altre strade di trasferimento del rischio, come le assicurazioni, per recuperare costi dovuti a perdite di dati

- ✓ Eseguire test periodici di backup e recovery per assicurarsi che la segregazione logica e i controlli siano efficaci.

- ✓ Assicurarsi che siano in atto controlli sul personale del Cloud provider al fine di garantire una separazione logica dei doveri

- ✓ Capire come venga gestita la crittografia per storage multi-utente. C'è una sola chiave per tutti i clienti, una chiave per cliente o chiavi multiple per cliente?

Raccomandazioni per la sicurezza dei dati dalla fase di ILM (Incident LifeCycle Management)

Alcune delle nostre raccomandazioni generiche, così come altri controlli specifici, sono elencati all'interno del contesti di ogni fase del ciclo di vita. Tenete in mente che sulla base del modello di Cloud service (Saas, PaaS o IaaS) alcune raccomandazioni devono essere implementate dal cliente e altre devono essere implementate dal Cloud provider.

Creare

- ✓ Identificare le capacità di etichettatura dei dati e di classificazione disponibili

- ✓ L'Enterprise Digital Rights Management può essere un'opzione

- ✓ L'abitudine di taggare i dati è diventata di uso comune nel Web 2.0 e può essere di aiuto per classificare i dati

Immagazzinare

- ✓ Identificare i controlli di accesso disponibili per file system, DBMS, sistemi di document management, ecc.

- ✓ Soluzioni di crittografia quali quelle per email, network transport, database, file e filesystem

- ✓ Strumenti di Content discovery (spesso DLP, o Data Loss Prevention) possono essere d'aiuto nell'identificazione e nell'auditing dei dati che richiedono controllo

Usare

- ✓ Attività di monitoraggio e di esecuzione, tramite file di log e/o strumenti basati su agenti.

- ✓ Logica per applicazione

- ✓ Controlli a livello oggetto entro soluzioni DBMS.

Condividere

- ✓ Attività di monitoraggio e di esecuzione, tramite file di log e/o strumenti basati su agenti.

- ✓ Logica per applicazione

- ✓ Controlli a livello oggetto entro soluzioni DBMS.
- ✓ Identificare i controlli di accesso disponibili per il file system, DBMS, sistemi di document management, ecc.
- ✓ Soluzioni di crittografia quali quelle per email, network transport, database, file e filesystem
- ✓ Data Loss Prevention per la protezione dei dati basata sul contenuto

Archiviare

- ✓ Crittografia, quale quella per nastri di backup e altri media di storage a lungo termine
- ✓ Gestione e tracciatura degli assets

Distruggere

- ✓ Crypto-shredding: la distruzione di tutto il materiale chiave legato ai dati crittografati
- ✓ Cancellazione sicura tramite pulizia del disco e tecniche collegate
- ✓ Distruzione fisica, quali smagnetizzazione (degaussing) di media fisici
- ✓ Scoperta dei contenuti a conferma del processo di distruzione

Contributors: Richard Austin, Ernie Hayden, Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna Garcia, Rich Mogull, Jeff Reich

Dominio 6: Portabilità e Interoperabilità

Le aziende devono rivolgersi al Cloud sapendo che potrebbero dover cambiare il provider in futuro. La portabilità e l'interoperabilità devono essere considerate come una parte primaria del risk management e dell'assicurazione di sicurezza di un qualsiasi programma di Cloud.

I grandi Cloud provider possono offrire ridondanza geografica nel Cloud, con la speranza di abilitare un'alta disponibilità con un singolo provider. Tuttavia, è consigliabile attivare un piano di continuità operativa di base, per aiutare a ridurre l'impatto di uno scenario del caso-peggiore. Diverse compagnie si troveranno in futuro a dovere affrontare improvvisamente e con urgenza un cambio di Cloud provider per varie ragioni, tra cui:

- Un inaccettabile aumento dei costi al momento del rinnovo contrattuale
- Una cessazione dell'attività da parte del provider
- Una chiusura improvvisa da parte del provider di uno o più servizi in uso, senza un piano di migrazione accettabile
- Un inaccettabile degrado della qualità del servizio, come l'incapacità di raggiungere le richieste di performance o garantire gli SLA prestabiliti.
- Una discussione d'affari tra provider e cliente

Alcune semplici considerazioni architetturali possono aiutare a ridurre il danno nel caso in cui questo genere di scenari dovesse accadere. Ad ogni modo, i mezzi per rispondere a questi problemi dipende dal tipo di Cloud service.

Nel caso del Software as a Service (SaaS), il cliente per definizione dovrà sostituire le vecchie applicazioni software con nuove. Di conseguenza il punto centrale non è la portabilità delle applicazioni, quanto il preservare o migliorare le funzionalità di sicurezza fornite dall'applicazione precedente e ottenere una migrazione dall'esito positivo.

Nel caso del Platform as a Service (PaaS), l'aspettativa è che sia necessario un certo livello di modifiche applicative per garantire la portabilità. Il punto centrale è minimizzare la quantità di riscrittura dell'applicazione, e nel contempo preservare o migliorare i controlli di sicurezza, al fine di ottenere una migrazione di successo.

Nel caso dell'Infrastructure as a Service (IaaS), il punto fondamentale e le aspettative sono che sia le applicazioni che i dati possano migrare e girare su un nuovo Cloud provider.

A causa di una generale mancanza di standard di interoperabilità, e alla mancanza di una adeguata pressione da parte del mercato su questi standard, la transizione tra Cloud provider può tradursi in un faticoso processo manuale. Dal punto di vista della sicurezza, le nostre preoccupazioni principali sono quelle di garantire la consistenza dei controlli durante il cambio di ambiente.

Raccomandazioni

Per tutte le soluzioni Cloud:

- ✓ La sostituzione del Cloud provider è vista praticamente in tutti i casi come una transizione negativa per almeno una delle parti coinvolte, e questo può causare

reazioni negative inaspettate da parte del precedente Cloud provider. Questo deve essere pianificato nel processo contrattuale come sottolineato nel Dominio 3, nel programma di Business Continuity come sottolineato nel Domino 7, e come parte della governance generale nel Dominio 2.

- ✓ Valutare la dimensione dei dati ospitati dal Cloud provider. La sola dimensione dei dati può causare una interruzione di servizio durante una transizione, o anche un periodo di transizione più lungo del previsto. Molti clienti hanno trovato che usare un corriere per spedire hard drive è più veloce che trasmettere grandi quantità di dati per via elettronica.

- ✓ Documentare l'architettura di sicurezza e la configurazione dei componenti individuali dei controlli di sicurezza in modo che possano essere usati per supportare audit interni, come anche facilitare la migrazione a nuovi provider.

Per le soluzioni Cloud IaaS:

- ✓ Capire come le immagini delle macchine virtuali possano essere catturate e portate sul nuovo Cloud provider, chi può usare diverse tecnologie di virtualizzazione

- ✓ Identificare ed eliminare (o almeno documentare) qualunque estensione specifica del provider per l'ambiente delle macchine virtuali

- ✓ Capire quali pratiche sono in atto per essere sicuri che il deprovisioning delle immagini delle macchine virtuali sia appropriato e che avvenga effettivamente dopo che un'applicazione viene trasferita dal Cloud provider

- ✓ Capire le pratiche usate per la dismissione di dischi e dispositivi di storage

- ✓ Capire dipendenze basate su hardware/piattaforma che necessitano di essere identificate prima della migrazione dell'applicazione o dei dati

- ✓ Chiedere l'accesso ai log e trace di sistema, e l'accesso e i dati di fatturazione dal precedente Cloud provider

- ✓ Identificare le opzioni per ripristinare o estendere il servizio con il precedente service provider in parte o del tutto, nel caso in cui il nuovo service provider si dimostrasse inferiore

- ✓ Determinare se c'è una qualsiasi funzione a livello di gestione, interfaccia o API che viene usata che è incompatibile o non può essere implementata con il nuovo provider

Per le soluzioni Cloud PaaS:

- ✓ Quando possibile usare componenti di piattaforma con una sintassi standard, open API e open standard

- ✓ Capire quali strumenti sono a disposizione per trasferimento di dati, backup e restore

- ✓ Capire e documentare componenti di applicazione e moduli specifici del PaaS provider, e sviluppare un'architettura di applicazione con strati di astrazione per minimizzare l'accesso diretto a moduli proprietari

- ✓ Capire come servizi di base come monitoraggio, logging, a auditing si trasferiranno a un nuovo vendor.

- ✓ Capire i controlli di funzione forniti dal Cloud provider precedente e come verranno trasferiti al nuovo provider

- ✓ Quando si migra verso una nuova piattaforma, capire l'impatto sulle performance e disponibilità dell'applicazione, e come questo impatto possa essere misurato

- ✓ Capire come i test possano essere prima e dopo la migrazione, per verificare che i servizi o le applicazioni stanno operando correttamente. Assicurarsi che le responsabilità del test sia per il provider che per l'utente siano ben note e documentate.

Per le soluzioni Cloud SaaS:

- ✓ Compiere backup ed estrazione di dati con regolarità, a un formato utilizzabile senza SaaS provider

- ✓ Capire se i metadati possono essere preservati e migrati

- ✓ Capire se tutti gli strumenti personalizzati implementati devono essere sviluppati di nuovo o se il nuovo fornitore deve fornirli

- ✓ Assicurare la consistenza dell'efficacia dei controlli dal vecchio al nuovo provider

- ✓ Assicurarsi della possibilità di migrazione dei backup e altre copie dei log, record di accesso, a ogni altra informazione pertinente che possa essere richiesta per ragioni legali o di conformità

- ✓ Capire le interfacce di gestione, monitoraggio, e reportistica e la loro integrazione fra gli ambienti

- ✓ fornitore

Contributors: Warren Axelrod, Aradhna Chetal, Arthur Hedge, Dennis Hurst, Sam Johnston, Scott Morrison, Adam Munter, Michael Sutton, Joe Wallace

Sezione III. Operare nel Cloud

Dominio 7: Sicurezza tradizionale, Business Continuity, e Disaster Recovery

L'insieme di conoscenze accumulate nella sicurezza fisica tradizionale, nella business continuity e nel disaster recovery, rimane rilevante allo stesso modo per il Cloud Computing. Il rapido cambio di passo e perdita di trasparenza del Cloud Computing richiede che i professionisti della sicurezza tradizionale, della Business Continuity (BCP) e del Disaster Recovery (DR) siano continuamente impegnati in controlli e monitoraggio dei Cloud provider scelti.

La nostra sfida è collaborare sull'identificazione dei rischi, riconoscere interdipendenze, integrare e influenzare risorse in maniera dinamica e convincente. Il Cloud Computing con la sua infrastruttura che lo accompagna, aiuta nel ridurre certi problemi di sicurezza, ma può farne aumentare altri e non potrà mai eliminare il bisogno di sicurezza. Così mentre continueranno a esserci grossi cambiamenti nel business e nella tecnologia, i principi tradizionali della sicurezza rimarranno dei punti fermi.

Raccomandazioni

- ✓ Tenere in mente che la centralizzazione dei dati significa correre il rischio di un abuso dall'interno, dal Cloud provider, generando una fonte di preoccupazione significante.

- ✓ I fornitori di servizi Cloud dovrebbero considerare di adottare le richieste più stringenti di ogni cliente come livello base della sicurezza. Possibilmente tali pratiche di sicurezza non devono impattare negativamente l'esperienza del cliente, pratiche di sicurezza più rigide devono dimostrare di fare risparmiare nel lungo periodo, riducendo il rischio così come fa l'esame del cliente, nelle diverse aree che gli destano preoccupazione.

- ✓ I fornitori devono avere una forte compartimentazione dei compiti, attuare controlli di background, richiedere/applicare accordi di non divulgazione agli impiegati, e limitare la conoscenza dei clienti agli impiegati a ciò che è strettamente necessario per svolgere le proprie mansioni

- ✓ I clienti dovrebbero fare ispezioni on-site delle strutture del fornitore Cloud quando possibile

- ✓ I clienti dovrebbero ispezionare i piani di disaster recovery e business continuity dei fornitori Cloud

- ✓ I clienti dovrebbero identificare interdipendenze fisiche nell'infrastruttura del provider

- ✓ Assicurarsi che vi sia una classificazione autoritativa nel contratto per definire chiaramente gli obblighi contrattuali legati a sicurezza, ripristino e accesso ai dati

- ✓ I clienti dovrebbero chiedere la documentazione dei controlli di sicurezza interni ed esterni del provider, e l'adesione agli standard industriali.

- ✓ Assicurarsi che i Recovery Time Objective (RTO) dei clienti siano pienamente compresi e definiti in relazioni contrattuali e inseriti nei processi di pianificazione tecnologici.

- ✓ Assicurarsi che le roadmap tecnologiche, le policy, e le capacità operative siano in grado di soddisfare queste richieste.

- ✓ I clienti hanno bisogno di conferma che il provider ha una policy di BCP approvata dal proprio consiglio direttivo

- ✓ I clienti dovrebbero ricercare l'evidenza di un supporto gestionale in atto e di una revisione periodica del programma di BCP per assicurarsi che il programma di BCP sia in funzione

- ✓ I clienti dovrebbero controllare che il programma di BCP sia certificato e/o mappato secondo standard riconosciuti a livello internazionale come BS 25999

- ✓ I clienti dovrebbero assicurarsi che il fornitore abbia ogni risorsa on line dedicata alla sicurezza e al BCP, e dove sono disponibili per consultazione il documento panoramico e quelli informativi

- ✓ Assicurarsi che i fornitori di servizi Cloud siano esaminati dal Vendor Security Process (VSP) di modo che vi sia una chiara comprensione di quali dati devono essere condivisi e quali devono essere utilizzati. La decisione del VSP dovrebbe alimentare il processo decisionale e la valutazione dell'accettazione del rischio

- ✓ La natura dinamica del Cloud Computing e la sua relativa giovinezza, giustificano cicli più frequenti di tutte le attività di cui sopra, per scoprire cambiamenti non comunicati ai clienti.

Contributors: Randolph Barr, Luis Morales, Jeff Spivey, David Tyson

Dominio 8: Operazioni di Data Center

Il numero di Cloud provider continua a crescere tanto più il business e gli utilizzatori di servizi IT si muovono verso il Cloud. C'è stata una simile crescita dei data center nell'alimentare l'offerta di servizi di Cloud Computing. Cloud provider di tutti i tipi e di ogni dimensione, inclusi leader tecnologici ben noti e migliaia di aziende emergenti in crescita o agli esordi, stanno facendo grossi investimenti in questo nuovo promettente approccio alla fornitura di servizi IT.

La condivisione di risorse IT per creare efficienza ed economia di scala non è un concetto nuovo. Tuttavia il modello di business del Cloud funziona meglio se i tradizionali enormi investimenti in operazioni di data center vengono spalmate su un vasto numero di utilizzatori. Storicamente le architetture dei data center sono state volutamente sovradimensionate per superare i picchi di carico, il che significa che durante i normali o i bassi periodi di domanda, le risorse dei data center sono spesso inattive o sottoutilizzate per lunghi periodi di tempo. I Cloud provider, d'altra parte, cercano di ottimizzare l'uso delle risorse, sia umane che tecnologiche, per ottenere un vantaggio competitivo e massimizzare i margini di profitto.

La sfida per gli utenti dei servizi Cloud è come valutare al meglio le capacità dei fornitore nel fornire servizi appropriati, efficienti ed economici e che allo stesso tempo proteggano i dati e gli interessi dei clienti. Non presumete che il fornitore abbia gli interessi dei suoi clienti come propria massima priorità. Con il modello comune di fornitura di servizi, di cui il Cluod Computing ne è una forma, il service fornitore normalmente ha poco o nullo accesso o controllo sui dati o sistemi del cliente, oltre al livello di gestione contrattato. Certamente questo è l'approccio corretto da seguire, ma alcune architetture Cloud potrebbero prendersi delle libertà con l'integrità e la sicurezza dei dati del cliente con cui il cliente non sarebbe a suo agio se ne venisse a conoscenza.
I clienti devono educare se stessi circa i servizi che stanno considerando, facendosi domande opportune e divenendo familiari con le architetture di base e le potenziali aree di vulnerabilità della sicurezza.

Nel prendere la decisione di muovere tutte o parte delle operazioni dell'IT sul Cloud il primo aiuto è capire come il Cloud provider ha implementato le "Cinque Principali Caratteristiche del Cloud Computing" del Dominio 1, e come quelle architetture e infrastrutture tecnologiche impattano sulla sua abilità di raggiungere gli SLA e di rispondere alle preoccupazioni sulla sicurezza. L'architettura tecnologica specifica del fornitore potrebbe essere una combinazione di prodotti IT e altri servizi Cloud, come per esempio approfittare di un servizio di storage di un altro fornitore IaaS.

L'architettura e l'infrastruttura tecnologica dei Cloud provider può essere diversa, ma per rispondere agli obiettivi di sicurezza tutti devono essere in grado di dimostrare una completa compartimentalizzazione dei sistemi, dei dati, delle reti, della gestione, della fornitura e del personale. I controlli che separano ogni strato dell'infrastruttura devono essere integrati in modo appropriato in modo tale che non interferiscano gli uni con gli altri. Per esempio, investigare se la compartimentalizzazione dello storage possa essere facilmente aggirata dagli strumenti di gestione o da deboli chiavi di gestione.

Infine, capire come il Cloud provider usi le risorse in modo democratico e dinamico per meglio prevedere i giusti livelli di disponibilità e performance dei sistemi attraverso le normali fluttuazioni del business. Bisogna ricordare che la teoria del Cloud Computing

a volte ancora supera la pratica: molti clienti fanno assunzioni sbagliate circa il livello di automazione in realtà implicato. Non appena viene raggiunta la capacità delle risorse che vengono fornite, il fornitore è responsabile del garantire che risorse aggiuntive vengano immediatamente rese disponibili al cliente.

Raccomandazioni

E' fondamentale che un'azienda che sta valutando di acquistare servizi Cloud, di qualsiasi genere, sia pienamente consapevole esattamente di quali servizi sta contrattando e cosa non è incluso. Sotto è riportato un sommario di informazioni che devono essere riviste come parte del processo di selezione del vendor, e altre domande per aiutare a qualificare i fornitore e meglio fare combaciare i loro servizi con le richieste aziendali.

- ✓ A prescindere da quali certificazioni il Cloud provider abbia, è importante ottenere un accordo o un permesso per condurre un audit fatto dal cliente stesso o da terze parti

- ✓ I clienti del Cloud dovrebbero capire come i Cloud provider implementano le "Cinque Principali Caratteristiche del Cloud Computing" del Dominio 1 e come quelle architetture e infrastrutture tecnologiche impattano sulla loro abilità di raggiungere gli SLA

- ✓ L'architettura e l'infrastruttura tecnologica dei Cloud provider può essere diversa, ma tutti devono essere in grado di dimostrare una completa compartimentalizzazione dei sistemi, dei dati, delle reti, della gestione, della fornitura e del personale

- ✓ Capire come il proprio Cloud provider usi le risorse in modo democratico e dinamico per meglio prevedere i giusti livelli di disponibilità e performance dei sistemi attraverso le normali fluttuazioni del proprio business. Se possibile, scoprire gli altri clienti del Cloud provider per valutare l'impatto che le loro fluttuazioni di business può avere con la propria customer experience nei confronti del Cloud provider. Tuttavia questo non sostituisce il dovere di assicurarsi che gli SLA siano chiaramente definiti, misurabili, applicabili e adeguati per le proprie richieste.

- ✓ I clienti dovrebbero capire le policy e le procedure di patch management dei Cloud provider e come queste vadano a impattare i loro ambienti. Questa comprensione dovrebbe riflettersi in linguaggio contrattuale.

- ✓ Il miglioramento continuo è particolarmente importante in un ambiente Cloud perché ogni miglioramento nelle policy, nei processi, nelle procedure, o strumenti per un singolo cliente , potrebbe portare ad un miglioramento dei servizi per tutti i clienti. Cercare Cloud provider con processi standard di miglioramento continuo in atto.

- ✓ Il supporto tecnico o il service desk è spesso una finestra del cliente sulle operazioni del fornitore. Per ottenere un supporto cliente omogeneo e uniforme per gli utenti finali è essenziale assicurarsi che i processi, le procedure, gli strumenti e gli orari di supporto al cliente del fornitore siano compatibili con i propri.

- ✓ Come nel Domino 7, rivedere i paini di business continuity e disaster recovery da una prospettiva IT, e come questi si relazionano con il personale e i processi. L'architettura tecnologica di un Cloud provider può fare uso di nuovi e mai usati metodi di failover, per esempio. Anche i piani di business continuity del cliente dovrebbero affrontare gli impatti e le limitazioni del Cloud Computing.

Contributors: Randolph Barr, Luis Morales, Jeff Spivey, David Tyson

Dominio 9: Risposta a un incidente, notifica, e rimedio

La natura del Cloud Computing rende più difficile determinare chi contattare in caso di un incidente di sicurezza, perdita di data, o altri eventi che richiedono investigazione e reazione. I meccanismi standard di risposta agli incidenti di sicurezza possono essere usati con modifiche al fine di rispondere ai cambiamenti richiesti dalle responsabilità di resoconto condivise. Questo dominio fornisce la guida su come gestire questi incidenti.

Il problema del cliente del Cloud è che le applicazioni dispiegate per la struttura del Cloud non sono sempre progettate avendo in mente l'integrità dei dati e la sicurezza. Questo può portare ad avere applicazioni vulnerabili in ambienti Cloud che fanno da innesco a incidenti di sicurezza. Inoltre, imperfezioni nell'architettura dell'infrastruttura, errori commessi durante le procedure di irrobustimento e semplice distrazione, presentano un rischio significante per le operazioni nel Cloud. Chiaramente, simili vulnerabilità mettono anche in pericolo operazioni di data center tradizionali.

Nella gestione degli incidenti è ovviamente richiesta competenza tecnica, ma esperti di privacy e legali possono contribuire molto alla sicurezza del Cloud. Giocano anche un ruolo nella risposta agli incidenti riguardo a notifiche, rimedi, e possibili azioni legali conseguenti. Un'organizzazione che considera di usare i servizi del Cloud ha bisogno di rivedere quali meccanismi sono stati implementati per rispondere a questioni circa l'accesso ai dati dei dipendenti che non è governato da accordi utente e policy di privacy. I dati non gestiti dalle applicazioni proprie del Cloud provider, come nelle architetture IaaS e PaaS, generalmente hanno controlli diversi dai dati gestiti da un'applicazione di un fornitore SaaS.

Le complessità di grandi Cloud provider di servizi SaaS, PaaS e IaaS, creano significativi problemi di *incident response* che i potenziali clienti devono stimare per valutare gli accettabili livelli di servizio. Quando si valuta un fornitore è importante stare attenti al fatto che il fornitore possa ospitare centinaia di migliaia di istanze applicative. Da una prospettiva di monitoraggio degli incidenti, ogni applicazione esterna aumenta la responsabilità del *security operations center* (SOC). Normalmente un SOC monitorizza allarmi e altri indicatori di incidenti, come quelli forniti da sistemi di intrusion detection e firewall, ma il numero di sorgenti che devono essere monitorate e il volume delle notifiche può crescere esponenzialmente in un ambiente Cloud aperto, dal momento che il SOC può avere bisogno di monitorare attività fra clienti e anche incidenti esterni.

Un'organizzazione dovrà avere bisogno di capire la strategia di *incident response* del Cloud provider scelto. La strategia dovrà rispondere all'identificazione e alla notifica, così come alle opzioni di rimedio verso l'accesso non autorizzato ai dati applicativi. Per rendere le cose ancora più complicate, la gestione dei dati applicativi e l'accesso hanno diversi significati e regolamentazioni in base alla posizione in cui si trovano. Per esempio, potrebbe avvenire un incidente che coinvolge dati in Germania, mentre se gli stessi dati fossero negli USA potrebbe non essere considerato un problema. Questa complicazione rende l'identificazione degli incidenti una sfida particolarmente impegnativa.

Raccomandazioni

- ✓ I clienti del Cloud hanno bisogno di definire e comunicare con chiarezza al Cloud provider cosa considerano essere un incidente (come per es. una fuga di dati) rispetto a semplici eventi (come un sospetto allarme di intrusion detection) prima della fornitura del servizio.

- ✓ I clienti del Cloud possono avere un limitato coinvolgimento con le attività di risposta agli incidenti del fornitore. Perciò per i clienti è critico capire i percorsi di comunicazione predefiniti al gruppo di risposta agli incidenti del fornitore.

- ✓ I clienti del Cloud dovrebbero studiare attentamente quali strumenti di individuazione degli incidenti e di analisi i fornitore usano per essere sicuri che siano compatibili con i propri sistemi. Un formato di log del fornitore proprietario o inusuale potrebbe rappresentare un grosso ostacolo in un'investigazione comune, in particolare in quelle che coinvolgono aspetti legali o interventi governativi.

- ✓ Applicazioni e sistemi male progettati e protetti possono facilmente sopraffare le capacità di incident response di chiunque. Condurre un corretto risk management sui sistemi e utilizzare pratiche di difesa-in-profondità sono essenziali per ridurre le probabilità di un incidente di sicurezza al primo posto.

- ✓ I Security Operations Center (SOC) spesso usano un solo modello di governance riguardo l'incident response, che è inappropriato per i Cloud provider con più destinatari. Un processo di Security Information and Event Management (SIEM) robusto e ben strutturato che identifichi sorgenti di dati disponibili (application log, firewall log, IDS log, ecc.) e li metta in correlazione in un'unica piattaforma di analisi e allarmi può aiutare il SOC nell'individuazione di incidenti nella piattaforma di Cloud Computing.

- ✓ Per facilitare enormemente dettagliate analisi offline, è bene cercare Cloud provider con l'abilità di fornire snapshot dell'intero ambiente virtuale del cliente – firewall, rete (switch), sistemi, applicazioni e dati.

- ✓ Il contenimento è una gara fra il controllo del danno e la raccolta dell'evidenza. Gli approcci al contenimento che si focalizzano sulla triade confidenzialità-integrità-disponibilità (confidentiality-integrity-availability, CIA), possono risultare efficaci

- ✓ Il rimedio fa risaltare l'importanza di essere in grado di ripristinare i sistemi a loro stati precedenti, e anche un bisogno di tornare indietro dai sei ai dodici mesi a una valida configurazione conosciuta. Tenendo in mente le opzioni legali e le richieste, il rimedio può anche avere bisogno di supportare registrazioni forensi di incidenti di dati.

- ✓ Qualsiasi dato classificato come privato per le regole della perdita di dati, dovrebbe essere sempre cifrato per ridurre le conseguenze di una perdita di dati. I clienti dovrebbero stipulare delle richieste di crittografia per contratto, come da Dominio 11.

- ✓ Alcuni Cloud provider possono ospitare un numero significante di clienti con applicazioni uniche. Questi Cloud provider dovrebbero considerare strutture di log a livello applicativo per fornire un granulare restringimento di incidenti per uno specifico cliente. Questi Cloud provider dovrebbero anche costruire un

registro di proprietari di applicazioni, per interfaccia applicativa (URL, servizio SOA, ecc.)

- ✓ Firewall a livello applicativo, proxy e altri strumenti di log di applicazioni sono capacità chiave attualmente disponibili per aiutare nella risposta agli incidenti in ambienti con più destinatari.

Contributors: John Arnold, Richard Austin, Ralph Broom, Beth Cohen, Wing Ko, Hadass Harel, David Lingenfelter, Beau Monday, Lee Newcombe, Jeff Reich, Tajeshwar Singh, Alexander Windel, Richard Zhao

Dominio 10: Sicurezza delle applicazioni

Gli ambienti Cloud – in virtù della loro flessibilità, apertura, e spesso pubblica disponibilità – rappresentano una sfida a molte assunzioni fondamentali riguardo alla sicurezza delle applicazioni. Alcune di queste assunzioni son ben comprese, mentre alcune non lo sono. Questa sezione intende documentare come il Cloud Computing influenzi la sicurezza per tutto il ciclo di vita di un'applicazione – dal progetto, alle operazioni per completare la dismissione. Questa guida è per tutti quelli coinvolti - inclusi progettisti di applicazioni, professionisti della sicurezza, personale operativo, e management tecnico – su come meglio mitigare il rischio e gestire la sicurezza nelle applicazioni nel Cloud Computing.

Il Cloud Computing è una sfida particolare per le applicazioni attraverso gli strati di Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS). Le applicazioni software basate sul Cloud richiedono un rigore di progetto simile alle applicazioni che risiedono in un classico DMZ. Ciò include una profonda analisi diretta che copra tutti gli aspetti tradizionali della gestione della confidenzialità, integrità e disponibilità dell'informazione.

Le applicazioni nell'ambiente del Cloud vanno sia a impattare che a subire l'impatto dei seguenti aspetti principali:

- **Architettura della sicurezza delle applicazioni** – Vanno fatte considerazioni sulla realtà che molte applicazioni dipendono da vari altri sistemi. Con il Cloud Computing, le dipendenze delle applicazioni possono essere altamente dinamiche, anche al punto che ogni dipendenza rappresenti un separato fornitore di servizi di terze parti. Le caratteristiche del Cloud rendono significativamente più complesse la gestione della configurazione e la fornitura continua, rispetto al metodo tradizionale. L'ambiente fa da guida dei bisogni di modifiche architetturali per assicurare la sicurezza delle applicazioni.

- **Sviluppo del ciclo di vita del software (SDLC)** – Il Cloud Computing influenza tutti gli aspetti del SDLC, dall'architettura dell'applicazione, al progetto, allo sviluppo, alla garanzia della qualità, alla documentazione, alla messa in opera, alla gestione, al supporto, e alla dismissione

- **Conformità** – La conformità chiaramente influenza i dati, ma influenza anche le applicazioni (per esempio, regolando come un programma implementa una particolare funzione crittografica), le piattaforme (magari prescrivendo controlli e impostazioni di sistemi operativi) e i processi (come richieste di report per incidenti di sicurezza)

- **Strumenti e servizi** – Il Cloud Computing introduce un numero di nuove sfide riguardo gli strumenti e i servizi richiesti per costruire e mantenere applicazioni d'uso corrente. Ciò include sviluppo e strumenti di test, utilities di gestione delle applicazioni, l'accoppiamento con servizi esterni, e dipendenze da librerie e servizi di sistemi operativi, che possono avere origine dai Cloud provider. E' fondamentale capire le ramificazioni di chi fornisce, possiede, opera, e assume le responsabilità per ciascuno di essi.

- **Vulnerabilità** – Le vulnerabilità non includono solo quelle ben documentate – e in continua evoluzione – associate con applicazioni web, ma anche quelle

associate con architetture *Service-Oriented Architecture* (SOA) macchina-macchina, la cui espansione nel Cloud è in crescita.

Raccomandazioni

- ✓ La sicurezza del Software Development Lifecycle (SDLC) è importante, e dovrebbe a un alto livello, rispondere alle seguenti tre aree di differenziazione con lo sviluppo basato sul Cloud: 1) modelli aggiornati di minacce e fiducia, 2) strumenti aggiornati di valutazione delle applicazioni per gli ambienti Cloud, e 3) processi e controlli di qualità del SDLC per rendere conto di cambi architetturali di sicurezza delle applicazioni

- ✓ IaaS, PaaS e SaaS creano confini di fiducia differenti per il ciclo di vita di sviluppo del software, di cui va tenuto conto durante lo sviluppo, il test, e la messa in produzione delle applicazioni.

- ✓ Per i fornitori IaaS un fattore chiave di successo è la presenza di immagini di macchine virtuali fidate. L'alternativa migliore è l'abilità di fornire la propria immagine di macchina virtuale conforme alle policy interne

- ✓ Alle macchine virtuali andrebbero applicate le migliori pratiche disponibili per l'hardening dei sistemi in DMZ. E' conveniente limitare i servizi disponibili a solo quelli necessari per supportare l'insieme di applicazioni.

- ✓ Mettere in sicurezza le comunicazioni inter-host deve essere la regola, non ci può essere l'assunzione di un canale sicuro fra host, anche se in uno stesso data center o perfino sullo stesso dispositivo hardware

- ✓ Gestire e proteggere le credenziali delle applicazioni e il materiale chiave è critico

- ✓ Una cura particolare dovrebbe essere posta con la gestione di file usati per il log e il debug delle applicazioni, dato che l'ubicazione di questi file potrebbe essere remota o sconosciuta e l'informazione potrebbe essere sensibile.

- ✓ Tenere conto nel modello di minacce dell'applicazione per l'amministrazione esterna e l'utilizzo da parte di molti

- ✓ Le applicazioni sufficientemente complesse da fare uso di un Enterprise Service Bus (ESB) hanno bisogno di rendere sicuro l'ESB direttamente, con un protocollo come il WS-Security. L'abilità di segmentare l'ESB non è disponibile in ambienti PaaS.

- ✓ Per valutare l'efficacia dei programmi di sicurezza delle applicazioni si dovrebbero applicare delle metriche. Tra le metriche specifiche disponibili per la sicurezza diretta delle applicazioni ci sono i punteggi di vulnerabilità e la copertura delle patch. Queste metriche possono indicare la qualità del codice dell'applicazione. Metriche indirette di gestione dei dati ,come la percentuale di dati cifrati, posso indicare che sono state prese delle decisioni responsabili dal punto di vista dell'architettura dell'applicazione.

- ✓ I Cloud provider devono supportare strumenti dinamici di sicurezza di applicazioni web nei confronti di applicazioni ospitate nei loro ambienti

- ✓ Bisogna prestare attenzione a come potenziali malintenzionati reagiranno alle nuove architetture di applicazioni Cloud che oscurano le componenti dell'applicazione alla loro vista. Gli hacker attaccano con probabilità codice visibile, incluso, ma non solo, il codice in un contesto utente. E' probabile che attacchino infrastrutture ed eseguano test di tipo black box in modo estensivo.

- ✓ I clienti dovrebbero ottenere permessi contrattuali per compiere dei vulnerability assessment remoti, incluso vunerability assessment tradizionali (network/host) e di applicazione. Molti Cloud provider limitano i vulnerability assessment a causa della loro incapacità di distinguere tali test da un reale attacco, e per evitare un potenziale impatto su altri clienti.

Contributors: John Arnold, Warren Axelrod, Aradhna Chetal, Justin Foster, Arthur J. Hedge III, Georg Hess, Dennis Hurst, Jesus Luna Garcia, Scott Matsumoto, Alexander Meisel, Anish Mohammed, Scott Morrison, Joe Stein, Michael Sutton, James Tiller, Joe Wallace, Colin Watson

Dominio 11: Crittografia e gestione delle chiavi

Clienti e Cloud provider devono guardarsi da perdita e furti di dati. Oggigiorno la crittografia di dati personali e aziendali è fortemente raccomandata e in certi casi obbligatoria per legge e regolamentazioni, in varie parti del mondo. I clienti vogliono che i loro Cloud provider crittografino i loro dati per assicurare che siano protetti a prescindere da dove i dati siano fisicamente localizzati. Allo stesso modo, il Cloud provider ha bisogno di proteggere i dati sensibili dei suoi clienti.

Uno dei meccanismi centrali che i sistemi di Cloud Computing usano per proteggere i dati è una crittografia forte con gestione della chiave. Sebbene la crittografia in sé non prevenga la perdita di dati, gli statuti previsti da leggi e regolamentazioni considerano la perdita di dati cifrati, come se non fossero mai andati persi. La crittografia garantisce la protezione delle risorse, mentre la gestione delle chiavi abilita l'accesso alle risorse protette.

La crittografia per la confidenzialità e l'integrità

Gli ambienti Cloud sono condivisi tra molti utenti e i fornitori di servizi in quegli ambienti hanno un accesso privilegiato ai dati. E' per questo che i dati ospitati nel Cloud devono essere protetti usando una combinazione di controllo degli accessi (ved. Dominio 12), responsabilità contrattuali (ved. Dominio 2, 3 e 4), e crittografia, che descriviamo in questa sezione. Di questi, la crittografia offre i benefici di una minima dipendenza dal fornitore di servizi Cloud e di una perdita di dipendenza dalla scoperta di insuccessi operativi.

Crittografia dei dati in transito sulla rete. C'è il bisogno più importante di crittografare credenziali multiuso, come numeri di carte di credito, password, e chiavi private, che transitano su Internet. Sebbene le reti dei Cloud provider possano essere più sicure di Internet, sono fatte per la loro stessa architettura di molti componenti disparati, e le più disparate organizzazioni condividono il Cloud. Perciò è importante proteggere questa informazione sensibile e regolata in transito anche entro la rete del Cloud provider. Tipicamente questo può essere fatto con eguale facilità in ambienti SaaS, PaaS e IaaS.

Crittografia dei dati a riposo. La crittografia dei dati su disco o su un database di produzione ha valore, in quanto può proteggere contro un malintenzionato fornitore di servizi Cloud o da un malintenzionato utilizzatore del Cloud, così come da alcuni tipi di abusi di applicazione. Per l'archiviazione a lungo termine alcuni clienti crittografano i propri dati e poi li mandano come testo cifrato a un vendor di data storage nel Cloud. Il cliente poi detiene e controlla le chiavi crittografiche e decrittografa i dati, se necessario, con il suo stesso permesso.
La crittografia di dati a riposo è comune entro ambienti IaaS, usando una varietà di provider e strumenti di terze parti. La crittografia di dati a riposo in ambienti PaaS è generalmente più complessa, dovendo richiedere strumenti che il provider offre o una personalizzazione speciale. La crittografia di dati a riposo in ambienti SaaS è una caratteristica che i clienti del coud non possono implementare direttamente, e che hanno bisogno di richiedere ai loro provider.

Crittografia dei dati sui media di backup. Questa può proteggere da un uso improprio di media persi o rubati. Idealmente il clod service provider lo implementa in modo trasparente. Tuttavia, è responsabilità del cliente, in qualità di fornitore dei dati,

verificare che tale crittografia avvenga. Una considerazione per l'infrastruttura di crittografia è il rapporto con la longevità dei dati. Al di là degli usi comuni della crittografia, la possibilità di attacchi contro i Cloud provider garantisce anche un'ulteriore esplorazione dei mezzi per crittografare dati dinamici, inclusi i dati che risiedono in memoria.

Gestione delle chiavi

I fornitori di servizi Cloud esistenti possono fornire degli schemi di base di chiavi di crittografia per mettere in sicurezza sviluppo di applicazioni e servizi basati sul Cloud, oppure possono lasciare tutte queste misure protettive ai loro clienti. Mentre i fornitori di servizi Cloud stanno progredendo verso il supporto di robusti schemi di gestione delle chiavi, c'è ancora bisogno di lavoro per superare le barriere per l'adozione. Standard emergenti dovrebbero risolvere questo problema in un futuro vicino, ma il lavoro è ancora in corso. Ci sono diversi problemi e sfide nel Cloud Computing a proposito della gestione delle chiavi.

Secure key stores. Lo store stesso delle chiavi deve essere protetto, così come un qualsiasi altro dato sensibile. Deve essere protetto nello storage, in transito e in backup. Un cattivo uso dello storage delle chiavi potrebbe portare alla compromissione di tutti i dati crittografati.

Access to key stores. L'accesso allo store delle chiavi deve essere limitato a quelle entità che hanno bisogno specificatamente delle chiavi individuali. Ci dovrebbero anche essere delle policy che governano lo store delle chiavi, che usino la separazione dei ruoli per aiutare il controllo degli accessi; un'entità che usa una certa chiave non dovrebbe essere la stessa entità che detiene quella chiave.

Key backup and recoverability. La perdita delle chiavi inevitabilmente significa la perdita dei dati che quelle chiavi proteggono. Mentre si può dire che questo sarebbe un modo efficace per distruggere i dati, la perdita accidentale delle chiavi che proteggono dati critici sarebbe devastante per il business, per cui vanno implementate soluzioni di backup e recovery.

C'è un numero di standard e linee guida applicabili alla gestione delle chiavi nel Cloud. Il OASIS Key Management Interoperability Protocol (KMIP) è uno standard emergente per la gestione interfunzionale delle chiavi nel Cloud. Gli standard IEEE 1619.3 coprono la crittografia dello storage e la gestione delle chiavi, specialmente di pertinenza allo storage IaaS.

Raccomandazioni

- ✓ Usare la crittografia per separare i dati in possesso dai dati in uso
- ✓ Separare la gestione delle chiavi dal Cloud provider che ospita i dati, creando una catena di separazione. Questo protegge il Cloud provider e il cliente da conflitti nel caso in cui debbano fornire i dati per un mandato legale.
- ✓ Quando si stipula una crittografia in linguaggio contrattuale, assicurarsi che la crittografia aderisca agli standard dell'industria e a quelli governamentali, se applicabile.

- ✓ Capire se e come i mezzi del Cloud provider garantiscono la gestione dei ruoli e la separazione dei doveri.

- ✓ Nei casi in cui il Cloud provider deve gestire le chiavi, capire se il provider ha definito dei processi per un ciclo di vita della gestione delle chiavi: come le chiavi vengono generate, usate, immagazzinate, come viene fatto il backup, recuperate, ruotate e cancellate. Inoltre, capire se la stessa chiave è usata per ogni cliente o se ogni cliente ha il proprio set di chiavi.

- ✓ Assicurarsi che i dati sensibili o regolamentati del cliente, oltre che ad essere crittografati a riposo, siano crittografati quando in transito nella rete interna del provider. Questo deve essere compito del cliente del Cloud in un ambiente IaaS, una responsabilità condivisa fra cliente e provider in ambienti PaaS, e responsabilità del Cloud provider in ambienti SaaS.

- ✓ In ambienti SaaS, capire come le informazioni sensibili e il materiale chiave, altrimenti protetti da crittografia tradizionale, possano essere esposti durante l'uso. Per esempio, file di swap di macchine virtuali e altri data storage temporanei possono avere bisogno di essere crittografati.

Contributors: John Arnold, Girish Bhat, Jon Callas, Sergio Loureiro, Jean Pawluk, Michael Reiter, Joel Weise

Dominio 12: Identità e gestione degli accessi

La gestione dell'identità e del controllo degli accessi per le applicazioni aziendali rimane una delle maggiori sfide dell'IT di oggi. Mentre un'azienda può essere in grado di usare abilmente diversi servizi di Cloud Computing senza una buona strategia di gestione delle identità e degli accessi, nel lungo periodo estendere i servizi di identità di un'azienda nel Cloud è un precursore necessario verso un uso strategico di servizi di Computing on-demand. Supportare l'adozione aggressiva del giorno d'oggi di un ecosistema di Cloud dichiaratamente immaturo, richiede un'onesta valutazione della preparazione a condurre *Identity and Access Management (IAM)* basato sul Cloud, così come capire le capacità del Cloud Computer provider di quell'azienda.

Discuteremo le principali funzioni di IAM che sono essenziali per una gestione efficace e di successo delle identità nel Cloud:

- Fornitura e dismissione di identità
- Autenticazione
- Federazione
- Autorizzazione e gestione del profilo utente

In tutto questo la conformità è una considerazione chiave.

Gestione delle identità: Una delle sfide principali per le organizzazioni che adottano i servizi del Cloud Computing è la gestione sicura e tempestiva della creazione e dismissione di utenti nel Cloud. Inoltre, le organizzazioni che hanno investito in processi di gestione degli utenti dentro un'azienda, cercheranno di estendere quei processi e quelle pratiche ai servizi nel Cloud.

Autenticazione: Quando le organizzazioni iniziano a usare i servizi del Cloud l'autenticazione degli utenti in un modo gestibile e affidabile è un requisito vitale. Le organizzazioni devono rispondere alle sfide legate all'autenticazione quali la gestione delle credenziali, strong authentication (tipicamente definita come autenticazione multi-fattore), autenticazione delegata, e gestione della fiducia attraverso tutti i tipi di servizi del Cloud.

Federazione: In un ambiente di Cloud Computing, la *Federated Identity Management* gioca un ruolo cruciale nell'abilitare le organizzazioni ad autenticare i loro utenti dei servizi Cloud usando *l'identity provider* (IdP) scelto dall'organizzazione. In quel contesto, scambiare attributi di identità tra service provider (SP) e l'IdP in un modo sicuro è un altro prerequisito importante. Le organizzazioni che considerano la *Federated Identity Management* nel Cloud dovrebbero capire le varie sfide e le possibili soluzioni per rispondere a quelle sfide nel rispetto al ciclo di vita dell'*identity management*, ai metodi di autenticazione disponibili per proteggere la confidenzialità e l'integrità, supportando nel contempo la *non-repudiation*

Gestione delle autorizzazioni e dei profili utente: I requisiti di policy per i profili utente e per il controllo degli accessi variano in base al fatto che l'utente stia agendo in prima persona (come un utente) o come un membro di un'organizzazione (come un impiegato, università, ospedale o un'altra impresa). I requisiti di controllo degli accessi in ambienti SPI includono lo stabilire profili utente fidati e policy di informazione, per usarli per il controllo degli accessi all'interno dei servizi Cloud, e facendolo in un modo controllabile da audit.

Gestione delle identità – Raccomandazioni

- ✓ Le capacità offerte dai Cloud provider al momento non sono adeguate a rispondere alle richieste delle imprese. I clienti dovrebbero evitare soluzioni proprietarie quali creare connettori personalizzati unici per Cloud provider, così come esasperare la complessità gestionale.

- ✓ I clienti dovrebbero fare leva su connettori standard forniti dai Cloud provider per una misura pratica, preferibilmente costruito su schemi SPML. Se il Cloud provider al momento non offre SPML, bisognerebbe richiederlo

- ✓ I clienti Cloud dovrebbero modificare o estendere le loro raccolte autorevoli dei dati di identità in modo da includere applicazioni e processi nel Cloud

Autenticazione – Raccomandazioni

Sia i Cloud provider che i clienti dovrebbero considerare le sfide associate con la gestione delle credenziali e la strong authentication, e implementare soluzioni efficaci dal punto di vista dei costi che riducano il rischio in modo appropriato.

Tipicamente i provider SaaS e PaaS danno le opzioni di servizi di autenticazione incorporati per le loro applicazioni o piattaforme, oppure delegano l'autenticazione alle imprese.
I client hanno le seguenti opzioni:

- ✓ Autenticazione per le imprese. Le imprese dovrebbero considerare di autenticare gli utenti attraverso i loro Identity Provider (IdP) e di stabilire una fiducia per federazione con il vendor SaaS.

- ✓ Autenticazione per utenti individuali che agiscono per conto proprio. Le imprese dovrebbero considerare di usare autenticazione utente-centrica, quali Google, Yahoo, OpenID, Live ID, ecc. per permettere l'uso di un solo insieme di credenziali valide su siti multipli.

- ✓ Qualunque provider SaaS che richiede metodi proprietari per delegare l'autenticazione (per es. gestire la fiducia per mezzo di un cookie crittografato condiviso o altri mezzi) dovrebbe essere attentamente valutato con una valutazione di sicurezza appropriata prima di proseguire. La preferenza generale dovrebbe andare per l'uso di standard aperti.

Per IaaS le strategie di autenticazione dovrebbero forzare l'uso delle capacità esistenti dell'impresa.

- ✓ Per il personale IT, stabilire una VPN dedicata sarebbe un'opzione migliore, dal momento che possono fare uso di sistemi e processi esistenti.

- ✓ Fra le soluzioni possibili vi è la creazione di un tunnel PN dedicato per la rete aziendale o la federazione. Un tunnel VPN dedicato funziona meglio quando l'applicazione sfrutta i sistemi di gestione dell'identità esistenti (come soluzioni SSO o autenticazione basata su LDAP che garantisce una sorgente autoritativa dell'identità dei dati)

- ✓ Nei casi in cui un tunnel VPN dedicato non è fattibile, le applicazioni dovrebbero essere progettate per accettare affermazioni di autenticazione in diversi formati (SAML, WS_Federation, ecc.), in combinazione con reti di crittografia standard come l'SSL. Questo approccio permette alle organizzazioni di fornire SSO federate non solo entro un'impresa, ma anche per applicazioni Cloud.

- ✓ L'OpenID è un'altra opzione quando l'applicazione è prevista al di là degli utenti aziendali. Tuttavia, siccome il controllo delle credenziali OpenID è al di fuori dell'azienda, i privilegi di accesso estesi a tali utenti dovrebbero essere limitati in modo opportuno.

- ✓ Un qualunque servizio di autenticazione locale implementato dal Cloud provider dovrebbe essere conforme all'OATH. Con una soluzione conforme all'OATH, le aziende sono in grado di evitare di trovarsi bloccate all'interno delle credenziali di autenticazione di un vendor.

- ✓ Per potere abilitare la strong authentication (a prescindere dalla tecnologia) le applicazioni Cloud dovrebbero supportare la capacità di delegare l'autenticazione all'azienda che sta utilizzando i servizi, per esempio attraverso il SAML

- ✓ I Cloud provider dovrebbero considerare di supportare varie opzioni di strong authentication tra cui One-Time Password, biometrico, certificati digitali e Kerberos, Questo garantirà alle aziende un'altra opzione per potere usare la loro infrastruttura esistente.

Federazione – Raccomandazioni

In un ambiente di Cloud Computing la federazione di identità è una chiave per abilitare aziende alleate per autenticarsi, consentire SSO e scambiare attributi di identità fra il Service Provider (SP) e l'*Identity Provider* (IdP). Le organizzazioni che considerano *l'identity management* federato nel Cloud dovrebbero capire le varie sfide e le possibili soluzioni per rispondere, nei confronti del ciclo di vita dell'*identity management,* dei metodi di autenticazione, formati token e *non-repudiation*.

- ✓ Le imprese in cerca di un Cloud provider devono verificare che il provider supporti almeno uno degli standard di primo piano (SAML e WS-Federation). Il SAML sta emergendo come uno standard di federazione largamente supportato ed è supportato dai maggiori SaaS e PaaS Cloud provider. Il supporto di standard multipli permette un maggior grado di flessibilità

- ✓ I Cloud provider dovrebbero avere la flessibilità di accettare i format standard di federazione da diversi identity provider. Tuttavia molti Cloud provider come di questo scrivente, supportano un solo standard, per es. SAML 1.1 o SAML 2.0. I Cloud provider che desiderino supportare formati di federazione token multipli, dovrebbero prendere in considerazione l'idea di implementare alcuni tipi di federation gateway

- ✓ Le organizzazioni possono desiderare di valutare il Federated Public SSO rispetto al Federated Private SSO. Il Federated Public SSO si basa su standard quali il SAML e il WS-Federation con il Cloud provider, mentre il Federated Private SSO fa uso di architetture SSO via VPN esistenti. Nel lungo periodo il Federated Public SSO sarà l'ideale, tuttavia un'organizzazione con

un'architettura SSO matura e un numero limitato di schieramenti di Cloud può guadagnare benefici in termini di costi a breve termine con un Federated Private SSO

- ✓ Le organizzazioni possono desiderare di optare per federation gateways in modo da esternalizzare l'implementazione della loro federazione, così da gestire la distribuzione e la verifica dei token. Usando questo metodo le organizzazioni delegano la distribuzione dei vari tipi di token alla faderation gateway, che quindi si occuperà dello spostamento dei token da un formato a un altro.

Controllo degli accessi – Raccomandazioni

Selezionare o rivalutare l'adeguatezza di soluzioni di controllo degli accessi per servizi Cloud ha molti aspetti, e implica le seguenti considerazioni:

- ✓ Rivedere l'adeguatezza del modello di controllo degli accessi per il tipo di servizi o dati.
- ✓ Identificare sorgenti di policy e di informazioni di profili utente autorevoli
- ✓ Valutare il supporto di policy di privacy necessarie per i dati
- ✓ Selezionare un formato col quale specificare policy e informazione utente
- ✓ Determinare il meccanismo per trasmettere le policy da un Policy Administration Point (PAP) a un Policy Decision Point (PDP).
- ✓ Determinare il meccanismo per trasmettere informazione utente da un Policy Information Point (PIP) a un Policy Decision Point (PDP).
- ✓ Richiedere una policy di decisione da un Policy Decision Point (PDP).
- ✓ Forzare una policy di decisione al Policy Enforcement Point (PEP).
- ✓ Fare un log dell'informazione necessaria per l'audit

IDaaS Raccomandazioni

L'Identity as a Service dovrebbe seguire le stesse best practice di un'implementazione di IAM interna, con l'aggiunta di considerazioni su privacy, integrità e controllabilità (*auditability*).

- ✓ Per utenti aziendali interni, i custodi devono rivedere le opzioni del Cloud provider nel fornire accesso sicuro al Cloud, o attraverso una VPN diretta o attraverso uno standard industriale come SAML o strong authentication. La riduzione dei costi derivante dall'uso del Cloud ha bisogno di essere bilanciata dalle misure di riduzione del rischio per rispondere alle considerazioni sulla privacy inerenti all'avere informazioni di dipendenti salvate all'esterno.
- ✓ Per utenti esterni come i partner, il proprietario dell'informazione ha bisogno di incorporare le interazioni con il provider IAM nel loro SDLC, così come nella loro valutazione delle minacce. Deve anche essere considerata e attivata la

protezione nei confronti della sicurezza delle applicazioni – le interazioni delle varie componenti l'una con l'altra e le vulnerabilità create in tal modo (come SQL injection e Cross Site Scripting, fra le altre).

- ✓ I clienti PaaS dovrebbero ricercare la misura in cui i vendor IDaaS supportano gli standard dell'industria per la fornitura, l'autenticazione, la comunicazione riguardo le policy di controllo degli accessi e l'informazione di audit

- ✓ Le soluzioni proprietarie presentano un rischio significativo per le componenti di ambienti IAM nel Cloud, a causa della perdita di trasparenza nei componenti proprietari. Protocolli di rete proprietari, algoritmi di crittografia e comunicazione dati sono spesso meno sicuri, meno robusti e meno interfunzionali. E' importante usare standard aperti per le componenti di IAM che si stanno esternalizzando.

- ✓ Peri clienti IaaS, le immagini di terze parti usate per lanciare server virtuali devono essere verificate per garantire l'autenticità dell'utente e dell'immagine. Una revisione del supporto fornito per la gestione del ciclo di vita dell'immagine deve verificare gli stessi principi del software installato sulla propria rete interna.

Contributors: Subra Kumaraswamy, Sitaraman Lakshminarayanan, Michael Reiter, Joseph Stein, Yvonne Wilson

Dominio 13: Virtualizzazione

L'abilità di fornire servizi di Cloud a livello di infrastruttura, piattaforma o software a più destinatari, è spesso sostenuta dall'abilità di fornire una qualche forma di virtualizzazione per beneficiare di un'economia di scala. Questo aspetto porta però con sé ulteriori preoccupazioni sulla sicurezza. Questo dominio si occupa di questi aspetti di sicurezza. Sebbene vi siano diverse forme di virtualizzazione, sicuramente quella più comune è la virtualizzazione dei sistemi operativi, e questo è il focus in questa versione della guida. Se la tecnologia di Virtual Machine (VM) viene usata nell'infrastruttura dei servizi di Cloud, allora noi dobbiamo preoccuparci della compartimentalizzazione e della robustezza di questi sistemi virtuali.

La realtà delle pratiche correnti legate alla gestione dei sistemi operativi virtuali, è che molti dei processi che forniscono sicurezza automaticamente sono mancanti, e un'attenzione particolare va posta per la sostituzione. Il nucleo stesso della tecnologia di virtualizzazione introduce nuove superfici di attacco nell'*hypervisor* e in altre componenti di gestione, ma l'aspetto più importante ancora è l'impatto che la virtualizzazione ha sulla sicurezza a livello di network. Le macchine virtuali ora comunicano su un *backplane* hardware, piuttosto che su una rete. Il risultato è che i controlli standard di sicurezza del network sono ciechi di fronte a questo traffico e non possono garantire un monitoraggio o un blocco all'occorrenza. Questi controlli devono prendere una nuova forma per funzionare in un ambiente virtuale.

La commistione dei dati in servizi e depositi centralizzati è un'altra preoccupazione. Un database centralizzato come quello fornito da un servizio di Cloud Computing, in teoria dovrebbe migliorare la sicurezza rispetto ai dati distribuiti su un vasto numero e un insieme di endpoint. Tuttavia ciò significa anche centralizzare il rischio, e aumentare le conseguenze di una violazione.

Un'altra preoccupazione è la commistione di macchine virtuali di diversa sensibilità e sicurezza. In un ambiente di Cloud Conputing, il minimo comune denominatore di sicurezza sarà condiviso fra tutti i destinatari in un ambiente virtuale multi-destinatario, a meno che non si ottenga una nuova architettura di sicurezza che non "cabli" ogni dipendenza dal network per la protezione.

Raccomandazioni

- ✓ Identificare quale tipo di virtualizzazione il Cloud provider usa, se ne fa uso
- ✓ I sistemi operativi virtualizzati dovrebbero essere rafforzati da tecnologie di terze parti per fornire controlli di sicurezza stratificati e ridurre la dipendenza dal solo fornitore della piattaforma
- ✓ Capire quali controlli di sicurezza interni alle macchine virtuali sono in atto, oltre all'isolamento predefinito dell'hypervisor– quali intrusion detection, antivirus, scansione delle vulnerabilità ecc. La configurazione di sicurezza di default deve essere assicurata seguendo o superando le baseline dell'industria
- ✓ Capire quali controlli di sicurezza esterni alle macchine virtuali sono in atto, per proteggere le interfacce di amministrazione (interfacce web, API, ecc.) esposte ai clienti

- ✓ Validare le origini e l'integrità di ogni immagine o modello di macchina virtuale che proviene dal Cloud provider prima dell'uso

- ✓ Devono essere utilizzati meccanismi di sicurezza specifici per macchine virtuali, insiti nelle API dell'hypervisor, per dare un monitoraggio granulare del traffico che attraversa i backplane delle macchine virtuali, altrimenti opachi ai tradizionali controlli di sicurezza del network

- ✓ L'accesso amministrativo e il controllo dei sistemi operativi virtuali è cruciale e dovrebbe includere strong authentication, integrata con enterprise identity management, così come logging a prova di manomissione (tamper-proof) e strumenti di monitoraggio dell'integrità

- ✓ Esaminare l'efficacia e la praticabilità della separazione delle macchine virtuali e della creazione di zone di sicurezza per tipologia d'uso (per es. desktop contro server), fasi di produzione (per es. sviluppo, produzione e test) e la sensibilità dei dati su componenti hardware fisicamente separati come server, storage ecc.

- ✓ Avere un meccanismo di reportistica in atto che dia evidenza dell'isolamento e che innalzi degli allarmi in caso in cui vi fossero delle violazioni all'isolamento

- ✓ Fare attenzione a quelle situazioni di multi-destinatari con le vostre macchine virtuali dove preoccupazioni regolamentari possono garantire la segregazione

Contributors: Bikram Barman, Girish Bhat, Sarabjeet Chugh, Philip Cox, Joe Cupano, Srijith K. Nair, Lee Newcombe, Brian O'Higgins

References

A guide to security metrics. SANS Institute, June 2006. http://www.sans.org

Amazon EC2 API - http://docs.amazonwebservices.com/AWSEC2/2006-10-01/DeveloperGuide/

Amazon Elastic Compute Cloud Developer Guide, http://docs.amazonwebservices.com/AWSEC2/2009-03-01/DeveloperGuide/

Amazon Simple Queue Service Developer Guide, http://docs.amazonwebservices.com/AWSSimpleQueueService/2008-01-01/SQSDeveloperGuide/

Amazon Simple Storage Service Developer Guide, http://docs.amazonwebservices.com/AmazonS3/2006-03-01/

Amazon SimpleDB Developer Guide, http://docs.amazonwebservices.com/AmazonSimpleDB/2007-11-07/DeveloperGuide/

Amazon web services blog: Introducing amazon virtual private cloud (vpc), Amazon, August 2009.
http://aws.typepad.com/aws/2009/08/introducing-amazon-virtual-private-cloud-vpc.html

Amazon Web Services: Overview of Security Processes, September 2008
An Innovative Policy-based Cross Certification methodology for Public Key Infrastructures.
Casola V., Mazzeo A., Mazzocca N., Rak M. 2nd EuroPKI Workshop. Springer-Verlag LNCS 35. Editors: D. Chadwick, G. Zhao. 2005.

Auditing the Cloud, Grid Gurus, http://gridgurus.typepad.com/grid_gurus/2008/10/auditing-thecl.html, October 20, 2008

Azure Services Platform, http://msdn.microsoft.com/en-us/library/dd163896.aspx

Balanced Scorecard for Information Security Introduction", Published: March 06, 2007,
http://technet.microsoft.com/en-us/library/bb821240.aspx

BITS Kalculator and BITS Financial Services Shared Assessments Program (third party provider assessment methodology)

Building Security In Maturity Model, http://www.bsi-mm.com/

Business case for a comprehensive approach to identity and access management, May 2009
https://wiki.caudit.edu.au/confluence/display/CTSCIdMWG/Business+case

Business Roundtable, Principles of Corporate Governance, 2005

Business Roundtable, Statement on Corporate Governance, 1997.

Business Software Alliance, Information Security Governance: Towards a Framework for Action Centers for Medicare and Medicaid Services Information Security Risk Assessment Methodology

Cloud Computing and Compliance: Be Careful Up There, Wood, Lamont, ITWorld, January 30 2009

Cloud computing definition, by P. Mell and T. Grance, NIST June 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Cloud Computing is on the Up, but what are the Security Issues?, Mather, Tim, Secure Computing Magazine (UK), March 2, 2009.

Cloud Computing Use Case Group Whitepaper -http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing use cases whitepaper, August 2009. http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

Cloud computing vocabulary (cloud computing wiki) http://sites.google.com/site/cloudcomputingwiki/Home/cloud-computing-vocabulary

Cloud Computing: Bill of Rights, http://wiki.cloudcomputing.org/wiki/CloudComputing:Bill_of_Rights

Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum, V 1.0 April 2009

Cloud Security and Privacy – An Enterprise perspective on Risks and Compliance from O'Reilly - http://oreilly.com/catalog/9780596802776/ -

Cloud Standards Organization - http://cloud-standards.org/

Cloud Storage Strategy, Steve Lesem, July 19, 2009, http://www.cloudstoragestrategy.com/2009/07/cloud-storage-and-the-innovators-dilemma.html

Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (DRAFT), 2009. http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf

Contracting for Certified Information Security: Model Contract Terms and Analysis (published by the Internet Security Alliance and available at www.cqdiscovery.com) Contracting for Information Security: Model Contract Terms (published by the Internet Security Alliance and available at www.cqdiscovery.com)

CPMC ClearPoint Metric Catalog, 2009 Online Available: http://www.clearpointmetrics.com/newdev_v3/catalog/MetricApplicationPackage.aspx

CVSS A Complete Guide to the Common Vulnerability Scoring System, Version 2.0, 2007 Online Available: http://www.first.org/cvss/cvss-guide.html

Data Lifecycle Management Model Shows Risks and Integrated Data Flow, by Ernie Hayden, Information Security Magazine, July 2009 http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1321704_mem1,00.html

Data Privacy Clarification Could Lead to Greater Confidence in Cloud Computing, Raywood, Dan, Secure Computing Magazine (UK), March 9, 2009.

Defending Electronic Mail as Evidence—The Critical E-Discovery Questions, Jeffrey Ritter, (available at www.cqdiscovery.com)

Does Every Cloud Have a Silver Compliance Lining?, Tom McHale, July 21, 2009 Online Available: http://blog.ca-grc.com/2009/07/does-every-cloud-have-a-silver-compliance-lining/

Encryption of Data At-Rest: Step-by-step Checklist", a whitepaper prepared by the Security Technical Working Group of the Storage Network Industry Association (SNIA).

ENISA - http://www.enisa.europa.eu/

Fedora Infrastructure Metrics, 2008. http://fedoraproject.org/wiki/Infrastructure/Metrics

Few Good Information Security Metrics, By Scott Berinato, July 2005 Online Available: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Force.com Web Services API Developer's Guide, http://www.salesforce.com/us/developer/docs/api/index.htm

Global Privacy & Security, Francoise Gilbert, (Aspen Publishing 2009).

GoGrid API - http://wiki.gogrid.com/wiki/index.php/API

GSA to launch online storefront for cloud computing services, August 2009. http://www.nextgov.com/nextgov/ng_20090715_3532.php

Guidelines for Media Sanitization," NIST's Special Publication 800-88

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, T. Ristenpart, et al,

http://blog.odysen.com/2009/06/security-and-identity-as-service-idaas.html

http://blogs.forrester.com/srm/2007/08/two-faces-of-id.html

http://blogs.intel.com/research/2008/10/httpseverywhere_encrypting_the.php

http://code.google.com/apis/accounts/docs/AuthForWebApps.html

http://code.google.com/apis/accounts/docs/OpenID.html

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

http://csrc.nist.gov/publications/PubsSPs.html

http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

http://www.aspeninstitute.org/publications/identity-age-cloud-computing-next-generationinternets-impact-business-governance-socia

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

http://www.sas70.com

https://siswg.net/index.php?option=com_docman&task=cat_view&gid=21&Itemid=99999999

Information Security Governance: A Call to Action, National Cyber Security Summit Task Force, Corporate Governance Task Force Report, April 2004.

Information Security Law: Emerging Standard for Corporate Compliance, Thomas Smedinghoff, (ITGP 2008).

ISACA, IT Governance Institute, Control Objectives for Information and related Technology (CobiT), 4.1

ISO/IEC 19011:2002 Guidelines for quality and/or environmental management systems auditing

ISO/IEC 20000-1:2005 Information technology—service management—Part 1: Specification

ISO/IEC 20000-1:2005 Information technology—service management—Part 2: Code of practice

ISO/IEC 21827:2008 Information technology—Systems Security Engineering—Capability Maturity Model (SSE-CMM®)

ISO/IEC 27000:2009 Information technology—Security techniques—Information security management systems—Overview and vocabulary

ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements.

ISO/IEC 27002:2005 Information technology—Security techniques—Code of practice for information security management

ISO/IEC 27005:2008 Information technology—Information security techniques—Information security risk management

ISO/IEC 27006:2007 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 28000:2007 Specification for security management systems for the supply chain

ISO/IEC 38500:2008 Corporate governance of information technology

IT Governance Institute, Board Briefing on Governance, 2nd Edition, 2003

IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006

ITGI Enterprise Risk: Identify Govern and Manage IT Risk—The Risk IT Framework, Exposure Draft version 0.1 February 2009.

Jericho Forum - http://www.opengroup.org/jericho/ and the Jericho Cloud Cube model http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Justify Identity Management Investment with Metrics, by Roberta J. Witty, Kris Brittain and Ant Allan, 23 Feb 2004. Gartner Research ID number TG-22-1617.

Managing Assurance, Security and Trust for Services. Online. Available: http://www.masterfp7.eu/

National Association for Information Destruction Inc - http://www.naidonline.org/forms/cert/cert_program_us.pdf

NIST Guidelines for Media Sanitization (800-88) - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

NIST Recommended Security Controls for Federal Information Systems (SP800-53)

NIST SP 800-30 Risk Management Guide for Information Technology Systems

OATH- http://www.openauthentication.org

OCEG, Foundation Guidelines Red Book, v1 10/27/2008

OCTAVE-S Implementation Guide, Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody, Version 1, 2005

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Open Cloud Computing Interface Working Group - http://www.occi-wg.org/doku.php

Open Security Architecture Group - http://www.opensecurityarchitecture.org

OpenCrowd - http://www.opencrowd.com/views/cloud.php

OpenID – http://openid.net

OpenID attribute exchange http://openid.net/specs/openid-attribute-exchange-1_0.htmlOAuth (created by a small group of individuals) http://OAuth.net/

OpenSocial – sharing social networking information http://www.opensocial.org/

ORCM Overcoming Risk And Compliance Myopia, August 2006 Online Available: http://logic.stanford.edu/POEM/externalpapers/grcdoc.pdf

OSAG Security Landscape - http://www.opensecurityarchitecture.org/cms/foundations/osalandscape

OWASP Top Ten Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Princeton Startup Lawyer, "Company Formation-Fiduciary Duties (the basics)", June 17, 2009, http://princetonstartuplawyer.wordpress.com/2009/06/17/company-formation-fiduciary-dutiesthe-basics/

Python Runtime Environment, http://code.google.com/appengine/docs/

Rackspace API - http://www.rackspacecloud.com/cloud_hosting_products/servers/api

Sailing in Dangerous Waters: A Director's Guide to Data Governance, E. Michael Power & Roland L. Trope, (American Bar Association, 2005).

SAML- http://www.oasis-open.org/specs/index.php#saml

Security Guidance for Critical Areas of Focus in Cloud Computing, Version 1, by Cloud Security Alliance, April 2009

Service Level Agreements: Managing Cost and Quality in Service Relationships, Hiles, A. (1993), London:Chapman & Hall SNIA Encryption of Data At Rest: A Step-by-Step Checklist http://www.snia.org/forums/ssif/knowledge_center/white_papers/forums/ssif/knowledge_center/white_papers/Encryption-Steps-Checklist_v3.060830.pdf

SNIA Introduction to Storage Security http://www.snia.org/forums/ssif/knowledge_center/white_papers/Storage-Security-Intro1.051014.pdf

SNIA Storage Security Best Current Practices http://www.snia.org/forums/ssif/forums/ssif/programs/best_practices/

Storage Security Best Current Practices (BCPs)" by the Security Technical Working Group of SNIA Sun Project Kenai API - http://kenai.com/projects/suncloudapis

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management—Integrated Framework (2004).

The Darker Side of Cloud Computing, by Matthew D. Sarrel, PC Mag.com, February 1, 2009

The Force.com Workbook, http://wiki.developerforce.com/index.php/Forcedotcomworkbook

The Institute of Internal Auditors, Critical Infrastructure Assurance Project, "Information Security Governance: What Directors Need to Know", 2001

The International Grid Trust Federation (IGTF). http://www.igtf.net

United States General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, 1999.

United States Sentencing Commission, Guidelines Manual

vCloud API - http://www.vmware.com/solutions/cloud-computing/vcloud-api.html

Where We're Headed: New Developments and Trends in the Law of Information Security, Thomas J. Smedinghoff, Privacy and Data Security Law Journal, January 2007, pps. 103-138

Windows Azure SDK, http://msdn.microsoft.com/en-us/library/dd179367.aspx

Windows Cardspace - http://msdn.microsoft.com/en-us/library/aa480189.aspx

WS-Federation : http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-specos.html