CSA IT cloud security alliance Italy Chapter

Cloud Computing

Benefici, rischi e raccomandazioni per la sicurezza delle informazioni

Marzo 2013

PREMESSA

Il documento ENISA "Cloud Computing – Benefits, Risks and Recommandations for Information Security" conserva a tutt'oggi una grande importanza nel panorama della letteratura dedicata alla sicurezza del cloud computing, sebbene sia stato pubblicato nel 2009. Infatti è stato selezionato come uno dei testi di riferimento per la preparazione della certificazione CCSK, assieme alla Guidance.

Il fatto che, come gran parte della documentazione tecnica relativa al cloud e alla sicurezza, sia redatto in lingua inglese, ne limita la diffusione in Paesi poco anglofoni quale ancora è il nostro. CSA Italy è quindi orgogliosa di rendere disponibile la traduzione in lingua italiana del documento ENISA "Cloud Computing – Benefits, Risks and Recommandations for Information Security", nella speranza che possa essere meglio conosciuto e utilizzato da tutte le realtà interessate all'adozione del cloud computing e/o alla certificazione CCSK.

La presente traduzione non intende in alcun modo sostituire il documento originale in lingua inglese, che rimane il solo punto di riferimento ufficiale, ma vuole porsi come strumento di diffusione e di miglior comprensione dei concetti alla base dell'analisi del rischio propedeutica all'adozione di soluzioni di cloud computing.

La traduzione di documentazione tecnica non può essere affidata interamente ai traduttori automatici che, per quanto sempre più precisi, mancano dell'esperienza viva che solo chi opera attivamente nello specifico settore tecnico può fornire e che arricchisce di significato quello che altrimenti si ridurrebbe a una mera elencazione.

Ringrazio perciò i soci che, a vario titolo, hanno contribuito fattivamente alla realizzazione di questo lavoro. Un ringraziamento particolare a Corrado Giustozzi, Marnix Dekker, Ukf Bergstrom di ENISA per gli utili consigli in fase di pubblicazione; e a Daniele Catteddu, Managing Director di Cloud Security Alliance EMEA per il fattivo supporto al successo dell'iniziativa.

RINGRAZIAMENTI

Coordinatore del Gruppo di Lavoro

Yvette Agostini (e, inizialmente, Moreno Carbone)

Traduttori

Yvette Agostini

Moreno Carbone

Loredana Mancini

Andrea Rui

Fabio Vayr

Valerio Vertua

CSAIT Staff

Paolo Foti

Mauro Gris

ABOUT ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors.

This work takes place in the context of ENISA's Emerging and Future Risk programme.

CONTACT DETAILS

This report has been edited by: Daniele Catteddu and Giles Hogben

e-mail:daniele.catteddu@enisa.europa.eu and giles.hogben@enisa.europa.eu,

Internet: http://www.enisa.europa.eu/

ELENCO DEI CONTRIBUTORI

Questo documento è stato prodotto dagli editor di ENISA utilizzando informazioni e commenti da un gruppo selezionato sulla base dell'esperienza nel settore in oggetto, che include esperti dal settore industriale, accademico e governativo.

Le opinioni espresse in questa pubblicazione sono quelle degli autori, salvo che non sia indicato differentemente, e non necessariamente riflettono le opinioni degli esperti partecipanti.

Alessandro Perilli	**Virtualization.info (Independent Analyst)**
Andrea Manieri	**Ingegneria Informatica**
Avner Algom	**The Israeli Association of GRID Technologies**
Craig Balding	**Cloudsecurity.org**
Dr Peter Dickman Engineering Manager	**Google Inc.**
Dr Simone Balboni	**University of Bologna**
Dr. Guy Bunker	**Bunker Associates**
John Rhoton	**Independent Consultant**
Matt Broda	**Microsoft**
Mirco Rohr	**Kaspersky**
Ofer Biran	**IBM**
Pete Lindstrom	**Spire Security**
Philippe Massonet	**Reservoir Project, CETIC**
Raj Samani	**Information Systems Security Association, UK**
Simon Pascoe	**British Telecom**
Srijith K. Nair	**The BEinGRID Project, British Telecom**

Theo Dimitrakos	
Various	**National Health Service (NHS) Technology Office, UK**
Various	**RSA**
Various	**Symantec, Symantec Hosted Services**

Legal input was mainly drafted by

Dr. Paolo Balboni	**Baker & McKenzie - Tilburg University**
Kieran Mccorry	**Hewlett Packard**
W. David Snead, P.C.	**Attorney and Counselor**

INDICE

EXECUTIVE SUMMARY

Il Cloud Computing è un nuovo modo di rendere disponibili risorse di elaborazione, non una nuova tecnologia.

Servizi che spaziano dalla memorizzazione ed elaborazione dati fino al software, come la gestione delle email, sono ora disponibili istantaneamente, senza impegno e su richiesta.

La conclusione chiave di questo documento è che le economie di scala e le flessibilità derivanti dal cloud sono sia favorevoli che sfavorevoli, dal punto di vista della sicurezza. Le massicce concentrazioni di risorse e di dati si configurano come obiettivi assai più interessanti per gli attaccanti, ma d'altra parte le difese implementate a livello di cloud possono essere più robuste, scalabili e convenienti. Questo documento consente un assessment informato dei rischi e dei benefici derivanti dall'utilizzo del cloud computing – fornendo una guida sulla sua sicurezza per utenti attuali e futuri.

Siccome viviamo in tempi in cui occorre risparmiare, questo nuovo modello economico per l'informatica ha trovato terreno fertile e sta riscontrando massicci investimenti globali. Secondo un'analisi dell'IDC, la previsione mondiale per i servizi cloud nel 2009 è nell'ordine di 17.4 miliardi di dollari (1). La stima per il 2013 ammonta a 44.2 miliardi di dollari, con il mercato europeo che crescerà dai 971 milioni di Euro nel 2008 ai 6.005 miliardi di Euro nel 2013 (2).

La conclusione chiave di questo documento è che le economie di scala e la flessibilità derivanti dal cloud sono sia favorevoli sia sfavorevoli, dal punto di vista della sicurezza. Le massicce concentrazioni di risorse e di dati si configurano come obiettivi molto più interessanti per gli attaccanti, ma d'altra parte le difese implementate a livello di cloud possono essere più robuste, scalabili e convenienti. Questo documento consente una valutazione informata dei rischi e dei benefici derivanti dall'utilizzo del cloud computing – fornendo una guida sulla sicurezza per utenti attuali e futuri del cloud computing.

La valutazione della sicurezza è basato su tre scenari tipici: 1) migrazione di PMI verso servizi di cloud computing, 2) l'impatto del cloud computing sulla resilienza del servizio, 3) il cloud computing nell'e-Government (ad esempio, la eSanità).

Il nuovo modello economico ha inoltre indirizzato il cambiamento tecnologico in termini di:

Scala: la mercificazione e la spinta verso l'efficienza economica hanno portato a massicce concentrazioni delle risorse hardware necessarie per erogare i servizi. Ciò promuove le economie di scala – per tutti i tipi di risorse necessarie per fornire servizi di elaborazione.

Architettura: l'utilizzo ottimale delle risorse richiede risorse di elaborazione astratte dall'hardware sottostante. Clienti differenti che condividono risorse hardware e software dipendono, per la protezione dei propri dati, da meccanismi di isolamento tecnologico. L'elaborazione, la memorizzazione e il trattamento dei dati sono massicciamente distribuite.

I mercati globali richiedono reti localizzate di distribuzione grazie alle quali i contenuti vengono portati e ricevuti il più vicino possibile ai clienti. Questa tendenza verso la distribuzione e la ridondanza globale significa che le risorse vengono solitamente gestite in modo massivo, sia dal punto di vista fisico che da quello logico.

In virtù della riduzione dei costi e della flessibilità che porta con sé, la migrazione verso il cloud computing è un aspetto convincente per molte PMI. Tuttavia, lo studio intrapreso come parte di questo report, (cfr. Survey – An SME Perspective on Cloud Computing) conferma che le principali preoccupazioni delle PMI nei confronti della migrazione verso il cloud includono la confidenzialità delle proprie informazioni e la responsabilità derivante da incidenti che coinvolgono l'infrastruttura.

Nondimeno, sia i governi sia le PMI si confrontano con la realtà che molti dei loro impiegati utilizzano servizi basati su cloud sia che questo faccia parte o meno delle proprie politiche ufficiali.

Anche i governi sono interessati alla possibilità di utilizzare il cloud computing per ridurre i costi IT e per aumentare le proprie potenzialità. Ad esempio, la GSA (General Services Administration) del governo degli Stati Uniti ora offre un portale per servizi di cloud computing (3). Anche i governi tuttavia hanno serie

difficoltà da superare, in termini si percezione pubblica del trattamento sicuro delle informazioni personali dei cittadini in infrastrutture di cloud computing. E prima di ciò, vi sono anche ostacoli legali e normativi che impediscono che molte applicazioni di eGovernment migrino verso il cloud. Nondimeno, sia i governi sia le PMI si confrontano con la realtà che molti dei loro impiegati utilizzano servizi basati su cloud sia che questo faccia parte o meno delle proprie politiche ufficiali.

Affinché il cloud computing raggiunga il pieno potenziale promesso dalla tecnologia, deve offrire una robusta sicurezza delle informazioni. Questo studio spiega, basandosi su scenari concreti, cosa significhi il cloud computing per la sicurezza delle reti e delle informazioni, per la protezione dei dati e per la privacy. Esamineremo i benefici del cloud computing per la sicurezza ed i suoi rischi. Copriremo le implicazioni tecniche, di policy e legali. E, cosa più importante, faremo raccomandazioni concrete su come affrontare i rischi e massimizzare i benefici.

Infine, è importante notare che il cloud computing può riferirsi a svariati tipi differenti di servizio, includendo i modelli Application/Software as a Service (SaaS), Platform as a Service (PaaS), ed Infrastructure as a Service (IaaS). I rischi ed i benefici associati a ciascun modello sono differenti, e di conseguenza lo sono anche le considerazioni chiave per negoziare le condizioni per ciascuno di essi. Le sezioni che seguono cercano di distinguere quando i rischi o i benefici si applicano differentemente ai diversi modelli di cloud.

PRINCIPALI RACCOMANDAZIONI

Garanzie per gli acquirenti di servizi cloud

Gli acquirenti di servizi cloud hanno bisogno di garanzie sul fatto che i fornitori seguano solide prassi di sicurezza per la mitigazione dei rischi che si presentano sia per il cliente che per il fornitore (ad esempio, gli attacchi DDoS). Ciò è necessario per operare scelte di business sensate e per mantenere od ottenere certificazioni di sicurezza.

Un primo sintomo di questo bisogno di rassicurazioni è che molti fornitori di servizi cloud sono sommersi dalle richieste di audit.

Per questa ragione, abbiamo espresso molte delle raccomandazioni di questo documento come una lista standard di quesiti che possono essere utilizzati per fornire od ottenere rassicurazioni.

Documenti basati sulla check-list dovrebbero fornire ai clienti un mezzo per:

1. valutare i rischi dell'adozione di servizi di tipo cloud;

2. confrontare offerte di differenti fornitori di servizi cloud;

3. ottenere assicurazioni dai fornitori di servizi cloud selezionati;

4. ridurre l'onere assicurativo che pesa sui fornitori di servizi cloud;

La check-list sulla sicurezza copre tutti gli aspetti dei requisiti di sicurezza compresi gli aspetti legali, la sicurezza fisica, gli aspetti inerenti le politiche e le problematiche tecniche.

Raccomandazioni di natura legale

La maggior parte dei problemi legali nel cloud computing si risolvono di norma durante la valutazione del contratto (e cioè quando si confrontano i diversi fornitori) o nelle negoziazioni. Il caso più comune nel cloud computing è quello di

effettuare una selezione tra le offerte disponibili sul mercato (valutazione del contratto), rispetto alla negoziazione del contratto. Tuttavia, è possibile che esista l'opportunità per i potenziali clienti di servizi cloud di scegliere fornitori i cui contratti sono negoziabili.

Diversamente dai tradizionali servizi Internet, le clausole standard dei contratti meritano una revisione aggiuntiva a causa della natura del cloud computing. Le parti dovrebbero porre particolare attenzione ai propri diritti ed obblighi nel contratto, relativi alla segnalazione di violazioni della sicurezza, al trasferimento di dati, alla creazione di lavori derivati, ai cambiamenti di controllo, e all'accesso ai dati da parte di rappresentanti delle forze dell'ordine. Per il fatto che il cloud può essere utilizzato per esternalizzare infrastrutture critiche interne, e che l'interruzione di tali infrastrutture può avere effetti anche molto ampi, le parti devono considerare attentamente se le limitazioni standard alle responsabilità rappresentino adeguatamente la distribuzione delle responsabilità, visto l'utilizzo del cloud fatto dalle parti, o le responsabilità per l'infrastruttura.

Fino a quando i precedenti legali e le norme non affronteranno le questioni di sicurezza specifiche del cloud computing, fornitori e clienti di servizi cloud dovranno valutare i termini dei propri contratti per affrontare efficacemente i rischi di sicurezza.

Raccomandazioni di natura legale alla Commissione Europea

Raccomandiamo che la Commissione Europea studi o chiarifichi quanto segue:

- alcuni problemi correlati alla Direttiva per la Protezione dei Dati e le raccomandazioni dell'Articolo 29 Data Protection Working Party;
- l'obbligo per i cloud provider di notificare ai propri clienti le violazioni di sicurezza dei dati
- come gli esoneri di responsabilità per gli intermediari, che emergono dagli articoli 12-15 della Direttiva per l'eCommerce si applichino ai cloud provider;

- come supportare al meglio gli standard minimi di protezione dei dati e gli schemi di certificazione per la privacy in modo coerente tra tutti gli Stati membri.

Raccomandazioni per la ricerca

Raccomandiamo aree prioritarie di ricerca al fine di migliorare la sicurezza delle tecnologie del cloud computing. Quelle che seguono sono le categorie che abbiamo preso in considerazione con alcuni esempi di aree specifiche prese dalla lista completa:

- costruire la fiducia nel cloud

- Effetti di diverse forme di segnalazione delle violazioni sulla sicurezza;
- Riservatezza dei dati end-to-end (da capo a capo) nel cloud e oltre;
- Cloud con sicurezza più elevata, cloud privati virtuali (virtual private clouds), ecc.

- protezione dei dati in sistemi di grandi dimensioni e multi-organizzazione

- Forensics e sistemi di raccolta dei mezzi di prova;
- Gestione degli incidenti – monitoraggio e tracciabilità;
- Differenze internazionali nelle normative pertinenti, inclusi protezione dei dati e privacy.

- progettazione di sistemi di calcolo di grandi dimensioni

- Meccanismi di isolamento delle risorse – dati, elaborazione, memoria, log, ecc.;
- Interoperabilità tra cloud provider;
- Resilienza del cloud computing. Come il cloud può migliorare la resilienza?

PRINCIPALI BENEFICI PER LA SICUREZZA

La sicurezza e i benefici di scala

In termini semplici, tutti i tipi di misure di sicurezza sono più economici quando vengono implementati su larga scala. Perciò la medesima quantità di investimenti in sicurezza ci permette di ottenere una protezione migliore. Questo include tutti i tipi di misure difensive come il filtering, la gestione degli aggiornamenti, la blindatura delle istanze delle macchine virtuali e degli hypervisors, ecc. Altri benefici derivanti dalla scala includono: ubicazioni multiple, reti periferiche (i contenuti vengono erogati o elaborati vicino alla loro destinazione), tempestività di risposta, agli incidenti e nella gestione delle minacce.

Perciò la medesima quantità di investimenti in sicurezza ci permette di ottenere una protezione migliore. Questo include tutti i tipi di misure difensive come il filtering, la gestione degli aggiornamenti, la blindatura delle istanze delle virtual machines e degli hypervisors, ecc. Altri benefici derivanti dalla scala includono: ubicazioni multiple, reti periferiche (i contenuti vengono erogati od elaborati vicino alla loro destinazione), tempestività di risposta, agli incidenti e nella gestione delle minacce.

La sicurezza come differenziale commerciale

La sicurezza è una preoccupazione prioritaria per molti clienti del cloud; molti di essi faranno scelte d'acquisto sulla base della reputazione del fornitore in quanto a confidenzialità, integrità e resilienza, e per i servizi di sicurezza offerti. Questo è un forte incentivo per i cloud provider al fine di migliorare le proprie politiche di sicurezza.

Sebbene la concentrazione di risorse abbia indubbiamente degli svantaggi per la sicurezza [cfr. Rischi], ha tuttavia l'ovvio vantaggio di più economici perimetrazione e controllo degli accessi fisici (per risorsa unitaria) e l'applicazione più semplice ed economica di molti processi correlati alla sicurezza.

Interfacce standardizzate per servizi di sicurezza gestiti

I grandi cloud provider possono offrire un'interfaccia standard ed aperta verso fornitori di servizi di gestione della sicurezza. Questo fatto crea un mercato più aperto e immediatamente disponibile per i servizi di sicurezza.

Dimensionamento rapido e intelligente delle risorse

La capacità del cloud provider di riallocare dinamicamente le risorse per il filtraggio, il traffic shaping, l'autenticazione, la crittografia, ecc. verso misure difensive (ad esempio, contro attacchi DDoS) ha ovvi vantaggi per la resilienza.

Controllo e raccolta dei mezzi di prova

Il cloud computing (quando viene utilizzata la virtualizzazione) può fornire immagini forensi dedicate e a consumo delle macchine virtuali, che sono così accessibili senza dover mettere offline l'infrastruttura, portando a minori tempi di indisponibilità a causa dell'analisi forense. Può fornire anche spazio a condizioni più convenienti per i log consentendo un tracciamento più completo senza compromettere le prestazioni.

Aggiornamenti e configurazioni standard più rapide, efficaci ed efficienti

Le immagini di riferimento delle macchine virtuali e dei moduli software utilizzati dal cliente possono essere pre-blindati e aggiornati con i più recenti aggiornamenti ed impostazioni di sicurezza in accordo con processi ben affinati; le API per servizi cloud di tipo IaaS consentono inoltre la memorizzazione di immagini dell'intera infrastruttura virtuale, da effettuarsi regolarmente e confrontarsi con la configurazione di riferimento. Gli aggiornamenti su una piattaforma omogenea possono essere eseguiti molte volte più rapidamente piuttosto che su tradizionali sistemi Client-Server che dipendono dal modello di aggiornamento.

Benefici della concentrazione delle risorse

Sebbene la concentrazione di risorse abbia indubbiamente degli svantaggi per la sicurezza [vedi Rischi], ha tuttavia l'ovvio vantaggio di più economici perimetrazione e controllo degli accessi fisici (per risorsa unitaria) e l'applicazione più semplice ed economica di molti processi correlati alla sicurezza.

PRINCIPALI RISCHI PER LA SICUREZZA

Le classi più importanti di rischi specifici del cloud identificati in questo documento sono:

Perdita di governance

Con l'utilizzo di infrastrutture cloud, il cliente cede necessariamente il controllo al Cloud Provider (CP) su una quantità di aspetti che si ripercuotono sulla sicurezza. Allo stesso tempo, gli SLA possono non offrire un impegno a fornire tali servizi da parte del cloud provider, lasciando così una lacuna nelle misure di difesa per la sicurezza.

Lock-in (NdT: accordo in esclusiva)

A oggi c'è ben poco in offerta per quanto riguarda strumenti, procedure, formati standard dei dati e interfacce verso i servizi che possano garantire la portabilità di dati, applicazioni e servizi. Questo fatto può rendere difficoltoso per il cliente migrare da un fornitore a un altro, o riportare indietro dati e servizi verso un ambiente IT interno. Ciò introduce una dipendenza da uno specifico CP per la fornitura dei servizi, specialmente se la portabilità dei dati, l'aspetto in assoluto più importante, non è abilitata.

Mancato isolamento: La multi-tenancy e la condivisione delle risorse stanno definendo le caratteristiche del cloud computing. Questa categoria di rischi copre il fallimento dei meccanismi preposti alla separazione dello storage, della memoria, del routing, ed anche della reputazione tra tenants diversi (ad esempio, i cosiddetti attacchi guest-hopping). Tuttavia si deve considerare che gli attacchi ai meccanismi di isolamento delle risorse (ad esempio, contro gli hypervisor) sono ancora meno numerosi e molto più difficili da mettere in pratica per un attaccante in confronto agli attacchi ai sistemi operativi tradizionali.

Mancato isolamento

La multi-tenancy e la condivisione delle risorse stanno definendo le caratteristiche del cloud computing. Questa categoria di rischi copre il fallimento

dei meccanismi preposti alla separazione dello storage, della memoria, del routing, ed anche della reputazione tra tenants diversi (ad esempio, i cosiddetti attacchi guest-hopping). Tuttavia si deve considerare che gli attacchi ai meccanismi di isolamento delle risorse (ad esempio, contro gli hypervisor) sono ancora meno numerosi e molto più difficili da mettere in pratica per un attaccante in confronto agli attacchi ai sistemi operativi tradizionali.

Rischi di compliance

Gli investimenti per ottenere certificazioni (ad esempio, standard industriali o requisiti normativi) possono essere messi a rischio migrando verso il cloud:

- se il CP non è in grado di fornire prova della propria conformità con i requisiti applicabili;
- se il CP non permette lo svolgimento di controlli da parte del Cliente del Cloud (CC).

In alcuni casi, ciò significa anche che utilizzare un'infrastruttura cloud pubblica implica che alcuni tipi di conformità non possono essere ottenuti (ad esempio, PCI DSS (4)).

Compromissione dell'interfaccia di gestione

Le interfacce di gestione per il cliente di un fornitore di cloud pubblico sono accessibili attraverso Internet e mediano l'accesso a una maggiore quantità di risorse (rispetto ai tradizionali fornitori di hosting) e perciò pongono un aumento dei rischi, specialmente quando sono combinate con accessi remoti e vulnerabilità dei web browser.

Protezione dei dati

Il cloud computing pone diversi rischi per la protezione dei dati per i clienti e i fornitori di servizi cloud. In alcuni casi, può essere difficoltoso per il cliente (nel suo ruolo di titolare dei dati) il verificare efficacemente le prassi di gestione dei dati del cloud provider ed essere così sicuro che i dati siano gestiti in modo lecito. Questo problema è aggravato nei casi di trasferimenti multipli di dati, ad

esempio tra molteplici cloud federati. D'altro lato alcuni cloud provider forniscono informazioni sulle proprie prassi di gestione dei dati. Alcuni offrono anche sintesi delle certificazioni delle proprie attività di trattamento e gestione della sicurezza dei dati e delle misure di controllo che hanno in essere, come ad esempio la certificazione SAS70.

Cancellazione insicura o incompleta dei dati

Quando viene fatta una richiesta di cancellazione di una risorsa nel cloud, così come viene fatto con la maggior parte dei sistemi operativi, questa potrebbe non risolversi con una reale eliminazione dei dati. Una eliminazione o tempestiva eliminazione dei dati può addirittura risultare impossibile (o non desiderabile, dal punto di vista del cliente), o perché le copie extra dei dati sono immagazzinate ma non disponibili, o perché il disco che andrebbe distrutto contiene dati di altri clienti. Nel caso di multitenancy e di riutilizzo delle risorse hardware, questo rappresenta un rischio più elevato rispetto alla situazione con hardware dedicato.

Insider malevolo

Sebbene sia generalmente più improbabile, il danno che può essere causato da insider malevoli è spesso molto più grande. Le architetture cloud necessitano di alcuni ruoli che sono ad elevatissimo rischio. Alcuni esempi includono amministratori di sistema CP e fornitori di servizi per la gestione della sicurezza.

NB: i rischi sopra elencati non seguono uno specifico ordine di criticità; essi sono soltanto dieci dei più importanti rischi specifici per il cloud computing identificati durante lo studio. I rischi nell'utilizzo del cloud computing dovrebbero essere confrontati con i rischi legati al rimanere su soluzioni tradizionali, come i modelli basati su computer desktop. Per agevolare ciò, nel documento principale abbiamo incluso le stime dei relativi rischi confrontati con tipici ambienti tradizionali.

Si noti che è spesso possibile, e in alcuni casi auspicabile, che il cliente del cloud trasferisca il rischio al cloud provider; tuttavia non tutti i rischi possono essere trasferiti: se un rischio può portare al fallimento di un business, a seri danni alla

reputazione o ad implicazioni legali, è difficile o impossibile per qualsiasi altra parte compensare il danno. In definitiva, potete delegare la responsabilità, ma non potete delegare l'imputabilità.

A CHI SI RIVOLGE IL DOCUMENTO

I destinatari di questo documento sono:

- responsabili del business, ed in particolare quelli delle PMI (Piccole e Medie Imprese), per agevolare la loro valutazione e mitigazione dei rischi associati all'adozione di tecnologie di cloud computing;
- i legislatori europei, per aiutarli nelle decisioni sulle politiche per la ricerca (per sviluppare tecnologie per mitigare i rischi);
- i legislatori europei, per assisterli nelle decisioni sulle appropriate politiche ed incentivi economici, sulle misure legislative, sulle iniziative per la diffusione della consapevolezza, ecc. confrontandosi faccia a faccia con le tecnologie del cloud computing;
- i singoli o i cittadini, per aiutarli a valutare costi e benefici dell'utilizzo delle versioni di mercato di queste applicazioni.

CLOUD COMPUTING – DEFINIZIONE DI RIFERIMENTO

- Questa è la definizione di riferimento di cloud computing che utilizziamo per gli scopi di questo studio. Non deve intendersi come un'altra definizione monolitica. Le fonti per la nostra definizione possono essere verificate in (5), (6) e (54).
- Il Cloud Computing è un modello di servizio su richiesta per la fornitura di servizi IT, basato spesso su tecnologie di virtualizzazione e di elaborazione distribuita. Le architetture di Cloud Computing hanno:
- un alto grado di astrazione delle risorse
- scalabilità e flessibilità praticamente istantanee
- messa a disposizione praticamente immediata
- risorse condivise (hardware, database, memoria, ecc.)
- 'servizi a richiesta', normalmente con un sistema di contabilizzazione 'a consumo'
- gestione programmatica (ad esempio, attraverso WS API).

Il Cloud Computing è un modello di fornitura a richiesta, spesso basato su tecnologie di virtualizzazione e calcolo distribuito. Le architetture di cloud computing hanno:

- ***risorse estremamente astratte***
- ***scalabilità e flessibilità quasi istantanee***
- ***fornitura quasi istantanea***
- ***risorse condivise (hardware, basi di dati, memoria, ecc.)***
- ***'servizio su richiesta', di solito con sistema di fatturazione 'a consumo'***
- ***gestione programmatica (ad esempio, mediante WS API)***

Vi sono tre categorie di cloud computing:

- Software as a service (SaaS): si tratta di software offerto da fornitori di terze parti, disponibile su richiesta, di norma via Internet e configurabile remotamente. Esempi includono strumenti di word processing e fogli elettronici online, l'offerta di servizi di CRM e di fornitura di contenuti (CRM di gestione della forza vendita, Google Docs, ecc.).

- Platform as a service (PaaS): consente agli acquirenti di sviluppare nuove applicazioni utilizzando API pubblicate e configurabili remotamente. Le piattaforme includono strumenti di sviluppo, il configuration management, e piattaforme di produzione. Esempi sono Microsoft Azure, e i motori di Force e Google App.
- Infrastructure as service (IaaS): fornisce macchine virtuali e l'astrazione di altro hardware e di sistemi operativi che possono essere controllati attraverso API di servizio. Esempi includono Amazon EC2 ed EC3, Terremark Enterprise Cloud, Windows Live Skydrive e Rackspace Cloud.

I cloud possono essere suddivisi anche in:

- **public:** pubblicamente disponibili – qualsiasi organizzazione può sottoscriverli
- **private:** servizi costruiti in accordo ai principi del cloud computing, ma accessibili soltanto dall'interno di reti private
- **partner:** servizi cloud offerti da un fornitore ad un numero ben definito e limitato di parti.

In generale il bene, il costo, la responsabilità e la garanzia dei cloud variano in relazione alla seguente figura:

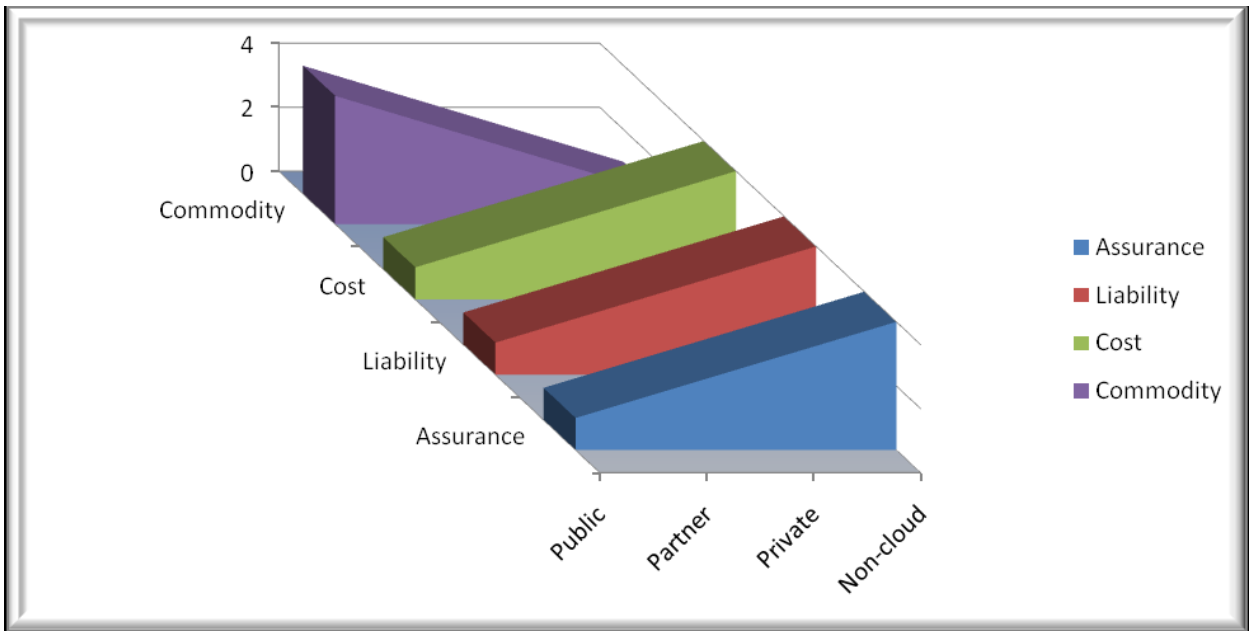


Figura 1: caratteristiche del cloud di tipo pubblico, partner e privato

Valutazione dei lavori esistenti

Nella compilazione di questo rapporto, abbiamo valutato i lavori esistenti sui rischi del cloud computing e sulla loro mitigazione, includendo la Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance (55)), Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration (Jericho Forum (56)) e l'Accessing the Security Risks of Cloud Computing (Gartner (57)), al fine di comprendere dove focalizzare gli sforzi per ottenere il massimo valore aggiunto.

1. I BENEFICI DEL CLOUD IN TERMINI DI SICUREZZA

In parole semplici, tutti i tipi di misure di sicurezza sono più economici se implementati su larga scala. Quindi lo stesso ammontare investito in sicurezza corrisponde a una miglior protezione.

Non è necessario ripetere che intere foreste sono state utilizzate per scrivere dei benefici economici, tecnici, architetturali ed ecologici del cloud computing. Tuttavia, nell'esperienza diretta dei membri del nostro gruppo di esperti, così come in accordo alle recenti novità dal 'mondo reale', un esame dei rischi di sicurezza del cloud computing deve essere controbilanciato da una verifica dei suoi benefici specifici per la sicurezza. Il cloud computing ha un potenziale significativo per migliorare la sicurezza e la resilienza. Ciò che segue è una descrizione dei principali modi in cui può essere d'aiuto.

La sicurezza e i benefici di scala

Semplicemente, tutti i tipi di misure di sicurezza sono più economici quando implementati su larga scala. Perciò la stessa quantità di investimenti nella sicurezza permette di ottenere una protezione migliore. Ciò include tutti i tipi di misure difensive come il filtering, la gestione degli aggiornamenti, la blindatura delle istanze delle macchine virtuali e degli hypervisor, le risorse umane e la loro gestione e controllo, la ridondanza di hardware e software, l'autenticazione forte, un efficiente controllo d'accesso basato su ruoli e soluzioni di default di identity management federative, che migliorano inoltre gli effetti di rete della collaborazione tra diversi partner coinvolti nella difesa. Altri benefici di scala includono:

- **Ubicazioni multiple**: la maggior parte dei cloud provider ha le risorse economiche per replicare di default i contenuti in più locazioni. Ciò aumenta la ridondanza e l'indipendenza da disservizi e fornisce un grado di disaster recovery 'di serie'.
- **Reti periferiche**: l'archiviazione, elaborazione e la fornitura più prossima al perimetro della rete significano che l'affidabilità e la qualità vengono

complessivamente elevate e che è meno probabile che i problemi delle reti locali abbiano effetti collaterali a livello globale.

- **Miglioramento dei tempi di risposta**: sistemi di dimensioni superiori ben condotti, per esempio grazie alla rilevazione precoce del rilascio di nuovo malware, possono sviluppare capacità di **gestione degli incidenti** più efficaci ed efficienti.
- **Gestione delle minacce**: i cloud provider possono anche permettersi di assumere degli specialisti per affrontare specifiche minacce alla sicurezza, mentre le aziende minori possono permettersi soltanto un piccolo numero di persone con competenze più generali.

La sicurezza come differenziatore di mercato

La sicurezza è una preoccupazione prioritaria per molti clienti del cloud [si veda lo studio: An SME perspective on Cloud Computing] – i clienti fanno scelte di acquisto sulla base della reputazione in fatto di confidenzialità, integrità e resilienza e dei servizi di sicurezza offerti dal fornitore, molto più che in ambienti tradizionali. Questo è un forte spunto per i fornitori di cloud per il miglioramento delle proprie prassi di sicurezza e per competere sul tema della sicurezza.

Interfacce standardizzate per servizi di sicurezza gestiti

I grandi fornitori di cloud possono offrire un'interfaccia aperta e standardizzata verso fornitori di gestione dei servizi di sicurezza (MSS) offrendo servizi a tutti i propri clienti. Ciò crea potenzialmente un mercato più aperto e più immediatamente accessibile per i servizi di sicurezza in cui i clienti possono cambiare fornitore più facilmente e con minori costi di avviamento.

Dimensionamento rapido e intelligente delle risorse

La lista delle risorse cloud che possono essere rapidamente scalate su richiesta include già, ad

La capacità di scalare dinamicamente le risorse difensive sulla base della domanda presenta ovvi vantaggi in termini di resilienza. Inoltre, quanto più tutti i tipi di risorse individuali possono essere scalati in modo granulare, senza influire sul ridimensionamento delle altre risorse, tanto più è economica la risposta a improvvisi (non malevoli) picchi di richiesta.

esempio, lo storage, il tempo CPU, la memoria, le richieste a web service e le istanze di macchine virtuali, ed il livello di controllo granulare sul consumo di risorse sta aumentando al maturare della tecnologia.

Un cloud provider ha il potenziale per riallocare dinamicamente le risorse per il filtering, il traffic shaping, la crittografia, ecc. così da aumentare il supporto per le misure difensive (ad esempio, contro attacchi di tipo DDoS) quando un attacco sta per verificarsi o quando è già in corso. Il cloud provider può essere in grado di limitare gli effetti che alcuni attacchi potrebbero avere sulla disponibilità delle risorse che i servizi legittimamente ospitati utilizzano, così come limitare gli effetti dell'aumento dell'utilizzo di risorse fatto dalle difese per la sicurezza per contrastare tali attacchi, grazie alla capacità di allocazione dinamica delle risorse, combinata con appropriati metodi di ottimizzazione delle risorse. Ottenere ciò richiede tuttavia che il fornitore implementi un adeguato coordinamento di autonomica per la difesa della sicurezza e per la gestione e l'ottimizzazione delle risorse.

La capacità di scalare dinamicamente le risorse difensive su richiesta ha ovvi vantaggi per la resilienza. Inoltre, più possono essere scalati in modo granulare tutti i tipi delle singole risorse, senza bisogno di scalare tutte le risorse di sistema, più è economico rispondere a rapidi picchi (non malevoli) nella richiesta.

Controllo e raccolta dei mezzi di prova

L'offerta IaaS supporta la clonazione su richiesta delle macchine virtuali. Nel caso di una presunta violazione di sicurezza, il cliente può effettuare un'immagine di una macchina virtuale in esecuzione – o di sue componenti virtuali – per l'analisi forense offline, comportando quindi minori tempi di fermo sistema per l'analisi. Con lo storage a disposizione, possono essere effettuate più clonazioni e parallelizzate le attività di analisi al fine di ridurre i tempi investigativi. Ciò migliora l'analisi ex-post degli incidenti di sicurezza e aumenta le probabilità di tracciare gli attaccanti e di correggere le vulnerabilità.

Tuttavia, si presume che il cliente abbia accesso a esperti tecnici forensi (cosa che al momento della scrittura non è un servizio standard del cloud).

Si può anche fornire spazio più economico per la memorizzazione dei log, permettendo così di tracciare in modo più completo senza compromettere le prestazioni. Il modello di pagamento a consumo per lo spazio di memorizzazione sul cloud porta trasparenza sui costi di storage per i vostri controlli e rende più semplice l'effettuare affinamenti per soddisfare i requisiti per i log dei futuri controlli.

Tutto ciò rende più efficiente il processo dell'identificazione degli incidenti di sicurezza appena questi si verificano (7)

Configurazioni di base e aggiornamenti più efficaci, efficienti e puntuali

Le immagini delle macchine virtuali e dei moduli software utilizzati dai clienti, possono essere preventivamente rafforzate e aggiornate con i più recenti aggiornamenti e impostazioni di sicurezza in accordo con processi ben affinati; inoltre, le API dei servizi cloud IaaS consentono di congelare periodicamente le immagini dell'infrastruttura virtuale e di confrontarle con una configurazione di riferimento (ad esempio, per assicurare che le regole di firewall software non siano cambiate) (8). Gli aggiornamenti possono essere rilasciati molte volte più rapidamente su una piattaforma omogenea piuttosto che su sistemi tradizionali basati su client che si affidano al modello di aggiornamento. Infine nei modelli PaaS e SaaS è più probabile che le applicazioni siano state blindate per essere eseguite all'esterno dell'ambiente aziendale, la qual cosa le rende più portabili e robuste rispetto all'equivalente software aziendale (se esistente). È anche più probabile che esse vengano aggiornate e corrette regolarmente in un modello centralizzato minimizzando la finestra di vulnerabilità.

Gli aggiornamenti possono essere distribuiti molto più rapidamente su una piattaforma omogenea che in un modello tradizionale client-based, che si fonda sul modello degli aggiornamenti.

Controllo e SLA per una migliore gestione dei rischi

La necessità di quantificare le penali per i vari scenari di rischio negli SLA e il possibile impatto di incidenti di sicurezza sulla reputazione (vedi La sicurezza

come differenziatore di mercato) motivano controlli interni più rigorosi e procedure di risk assessment (valutazione dei rischi) che altrimenti non esisterebbero. I frequenti controlli imposti ai CP (Cloud Provider) tendono a portare alla luce rischi che non verrebbero altrimenti scoperti, avendo perciò il medesimo effetto positivo.

Benefici derivanti dalla concentrazione delle risorse

Sebbene la concentrazione di risorse abbia indubbiamente svantaggi per la sicurezza (vedi Rischi) ha l'ovvio vantaggio di più economiche perimetrazione fisica e controllo fisico degli accessi (per risorsa unitaria) ed una più semplice ed economica applicazione di una politica globale per la sicurezza e del controllo sulla gestione dei dati, degli aggiornamenti, degli incidenti e sui processi di manutenzione. Il grado con cui questi risparmi vengono trasferiti ai clienti ovviamente varia.

2. RISK ASSESSMENT (Valutazione dei rischi)

Scenari di casi d'uso

Per gli scopi del risk assessment del cloud computing, abbiamo analizzato tre scenari di casi d'uso:

- una prospettiva delle PMI sul Cloud computing
- L'impatto del Cloud computing sulla resilienza dei servizi
- il Cloud computing e l'eGovernment (eSanità, ….)

Per amor di brevità abbiamo deciso di pubblicare la versione completa di uno scenario di caso d'uso di PMI (vedi ALLEGATO II) ed un sommario degli scenari per la resilienza e per la eSanità (vedi ALLEGATO III).

Per gli scopi del risk assessment del cloud computing, abbiamo analizzato tre scenari di casi d'uso:

- ***una prospettiva delle PMI sul Cloud computing***
- ***L'impatto del Cloud computing sulla resilienza dei servizi***
- ***il Cloud computing e l'eGovernment (eSanità, ….)***

Questa selezione è stata basata sul razionale della previsione che in Europa il mercato del cloud avrà un grande impatto sulle nuove attività e start-up, così come sul modo in cui evolveranno i modelli correnti di business. Dal momento che l'industria europea è principalmente basata su PMI (il 99% delle imprese, secondo le fonti europee (9)) ha senso focalizzarsi sulle PMI. Tuttavia, abbiamo incluso alcuni rischi e raccomandazioni che si applicano specificamente ai governi e alle imprese più grandi.

Lo scenario delle PMI è basato sui risultati dello studio: le prospettive delle PMI sul Cloud Computing (si veda qui), e NON deve essere inteso come una roadmap per le imprese che considerano, pianificano o hanno avviato progetti ed investimenti sul cloud computing.

È stata utilizzata un'impresa di medie dimensioni come caso tipo per garantire all'assessment un livello sufficientemente alto della complessità dell'IT, degli aspetti legali e del business. L'intenzione era quella di portare alla luce tutti i possibili rischi per la sicurezza delle informazioni. Alcuni di questi rischi sono specifici per le imprese di medie dimensioni; altri sono rischi generali che anche le micro e piccole imprese possono probabilmente trovarsi a dover fronteggiare nel caso di una migrazione verso un approccio al cloud computing.

Lo scenario NON intendeva essere completamente realistico per ogni singolo cliente o fornitore di cloud, ma è probabile che tutti gli elementi dello scenario si presentino in molte organizzazioni nel prossimo futuro.

Processo di Risk Assessment

Il livello di rischio viene stimato sulla base della probabilità che si verifichi un incidente, mappato rispetto al relativo impatto negativo stimato. La probabilità che si verifichi un incidente è data dallo sfruttamento di una vulnerabilità da parte di una minaccia, con una data probabilità.

La probabilità di ogni possibile casistica di incidente e del suo impatto sul business è stata determinata mediante consultazioni con il gruppo di esperti che ha contribuito a questo rapporto, derivandolo dalla loro esperienza collettiva. Nei casi in cui non si è ritenuto possibile fornire una stima ben fondata della probabilità di occorrenza, il valore riportato è N/A. In molti casi la stima della probabilità dipende pesantemente dal modello di cloud o dall'architettura considerati.
Quanto segue mostra il livello di rischio in funzione dell'impatto sul business e della probabilità dello scenario d'incidente. Il rischio risultante viene misurato con una scala da 0 a 8 che può essere valutata in relazione ai criteri di accettazione del rischio. La scala dei rischi può anche essere mappata su una semplice scala generale di quantificazione del rischio:

- Basso rischio: 0-2
- Medio Rischio: 3-5
- Alto Rischio: 6-8

	Probabilità dello scenario di incidente	Molto bassa	Bassa	Media	Alta	Molto Alta
Impatto sul Business	Molto Bassa	0	1	2	3	4
	Bassa	1	2	3	4	5
	Media	2	3	4	5	6
	Alta	3	4	5	6	7
	Molto Alta	4	5	6	7	8

Abbiamo basato la stima dei livelli di rischio sulla ISO/IEC 27005:2008 (10).

3. RISCHI

È opportuno notare i seguenti punti in relazione alla descrizione dei rischi sottostanti:

- Il rischio dovrebbe essere sempre compreso in relazione alle opportunità complessive di business ed alla sua appetibilità – a volte il rischio è compensato dalle opportunità.

Il rischio dovrebbe sempre essere compreso in relazione alle opportunità di business ed all'appetito per il rischio complessivi – talvolta il rischio è compensato dall'opportunità.

- I servizi cloud non riguardano soltanto uno storage conveniente e accessibile da molteplici dispositivi, ma includono anche importanti benefici quali una comunicazione più conveniente e una collaborazione istantanea multi-punto. Perciò un'analisi comparativa deve confrontare non solo i rischi relativi alla memorizzazione di dati in posti differenti (in azienda rispetto al cloud), ma anche i rischi che sorgono quando dati locali memorizzati internamente – ad esempio un foglio elettronico – vengono inviati via email ad altre persone per i loro contributi, in confronto ai problemi di sicurezza di un foglio elettronico memorizzato nel cloud ed aperto alla collaborazione tra tali persone. Pertanto i rischi derivanti dall'utilizzo del cloud computing dovrebbero essere paragonati a quelli relativi al rimanere su soluzioni tradizionali, come i modelli basati su desktop.
- Il livello di rischio in molti casi varia significativamente in relazione al tipo di architettura cloud considerata.
- Per il cliente del cloud è possibile trasferire il rischio al cloud provider ed i rischi dovrebbero essere valutati in relazione al vantaggio economico derivante dai servizi. Tuttavia non tutti i rischi possono essere trasferiti: se un rischio può portare al fallimento di un'impresa, a seri danni alla reputazione o ad implicazioni legali, è difficile se non impossibile per qualsiasi altra parte compensare tale danno.
- L'analisi dei rischi in questo documento si applica alla tecnologia cloud. Non si applica ad alcuna specifica offerta o cloud provider. Questo documento

non intende sostituire alcun risk assessment organizzativo di progetti specifici.

Perciò, il rischio connesso all'utilizzo del cloud computing dovrebbe essere comparato con quello connesso alle soluzioni tradizionali, quali il modello basato sul desktop.

- Il livello di rischio viene espresso dal punto di vista del cliente del cloud. Ove viene considerato il punto di vista del cloud provider, questo viene esplicitamente evidenziato.

La tabella seguente mostra la distribuzione delle probabilità di rischio e degli impatti.

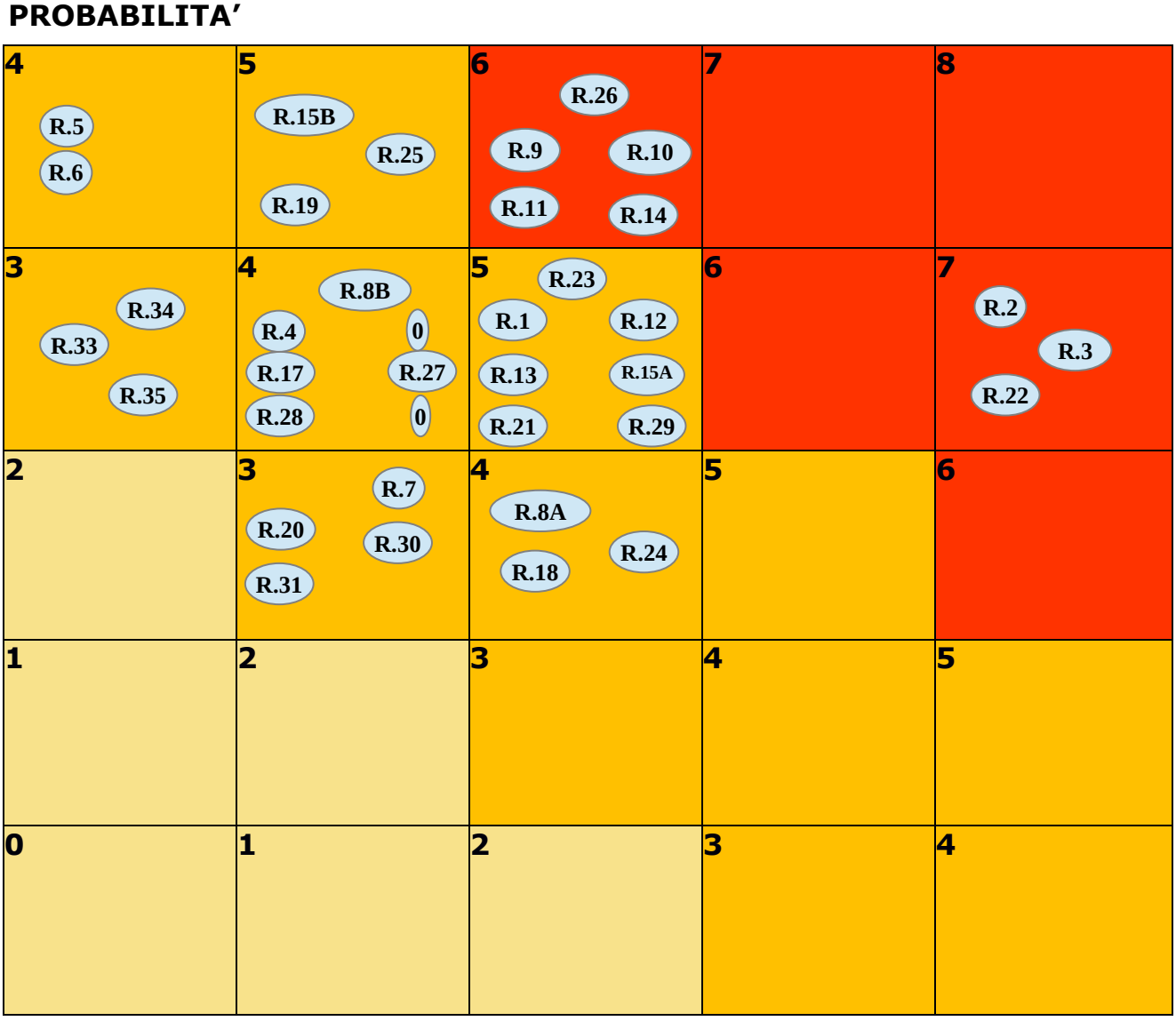


Figura 2: distribuzione del rischio

I rischi identificati nell'assessment sono classificati in tre categorie:

- Organizzativi e relativi alle politiche
- Tecnici
- Legali

Ciascun rischio viene presentato in tabelle che includono:

- Livello di probabilità
- Livello di impatto
- Riferimento alle vulnerabilità
- Riferimento agli asset interessati
- Livello di rischio.

Inoltre, ove significativo, abbiamo aggiunto i comparativi per la probabilità e per l'impatto, per confrontare il rischio del cloud computing ed i rischi degli approcci IT standard. Non abbiamo aggiunto un rischio comparato poiché si presume che tutti i rischi selezionati siano superiori.

D'altronde, non tutti i rischi possono essere trasferiti: se un rischio conduce al fallimento di un affare, a un serio danno di reputazione o a implicazioni legali, è difficile se non impossibile per una qualsiasi delle parti compensare questo danno.

RISCHI ORGANIZZATIVI E RELATIVI ALLE POLITICHE

R.1 Lock-in

Probabilità	ALTO	Comparativo: più alto
Impatto	MEDIO	Comparativo: uguale
Vulnerabilità	V13. Carenza di tecnologie e di soluzioni standard V46. Selezione di fornitori carente V47. Mancanza di ridondanza di fornitori V31. Mancanza di completezza e trasparenza delle condizioni di utilizzo	
Assets interessati	A1. Reputazione aziendale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi real time A10. Erogazione del servzio	
Rischio	**ALTO**	

Attualmente, per quanto concerne strumenti, procedure, formati standard dei dati ed interfacce dei servizi che potrebbero garantire la portabilità di dati e servizi (sebbene esistano alcune iniziative, come ad esempio, vedi (58)), l'offerta è piuttosto scarsa. Ciò rende estremamente difficoltoso per un cliente migrare da un fornitore ad un altro, o migrare dati e servizi da o verso un'infrastruttura IT interna. Inoltre, i cloud provider possono sentirsi incentivati a prevenire (direttamente o indirettamente) la portabilità dei servizi e dei dati dei propri clienti.

Questa potenziale dipendenza da un particolare CP per la fornitura di servizi, in relazione all'impegno del CP, può portare ad un catastrofico fallimento commerciale nel caso in cui il cloud provider dovesse fallire (vedi R.5) ed il percorso per la migrazione di dati e servizi verso un altro provider risultasse

troppo costoso (finanziariamente o temporalmente) o non venisse dato un sufficiente preavviso (senza preavviso).

Anche l'acquisizione del cloud provider (R.6) può avere un effetto simile, poiché aumenta la probabilità di improvvisi cambiamenti nelle politiche del provider e negli accordi non vincolanti, quali le condizioni d'uso (CdU).

E' importante capire che l'estensione e la natura dell'accordo in esclusiva variano in base alla tipologia di cloud:

SaaS Lock-in

- I dati del cliente sono tipicamente memorizzati in database con schema proprietario disegnato dal SaaS provider. La maggior parte dei provider SaaS offre chiamate ad API per la lettura (e quindi per 'esportare') i record di dati. Tuttavia, se il fornitore non rende disponibile una procedura già pronta per l'esportazione dei dati, il cliente dovrà sviluppare un programma per estrarre i propri dati e per salvarli in file pronti per l'importazione verso un altro provider. Occorre notare che esistono pochi accordi formali sulla struttura dei record di business (ad esempio, un record del cliente presso un provider SaaS può avere campi differenti presso un altro provider), sebbene vi siano formati di base comuni dei file per l'esportazione e l'importazione dei dati, come ad esempio XML. Il nuovo provider può di norma aiutare in quest'operazione concordandone il costo. Tuttavia, se i dati sono da riportare sui propri sistemi, il cliente dovrà scrivere le procedure di importazione che tengano conto della mappatura di ogni dato richiesto a meno che il CP non offra una tale routine. Dal momento che i clienti valuteranno questo aspetto prima di prendere importanti decisioni di migrazione, è negli interessi di business di lungo termine dei CP il rendere la portabilità dei dati il più possibile semplice, completa ed economica.
- Il lock-in delle applicazioni è la forma più ovvia di lock-in (sebbene non sia specifica dei servizi cloud). I provider SaaS sviluppano tipicamente un'applicazione proprietaria ritagliata sulle esigenze del loro mercato target. I clienti SaaS con una larga base di utenti possono incorrere in costi

di cambiamento molto alti in caso di migrazione verso un altro provider SaaS, in quanto ha impatto sull'esperienza degli utenti finali (ad esempio, può essere necessaria della nuova formazione). Nel caso in cui il cliente abbia sviluppato dei programmi per interagire direttamente con le API del provider (ad esempio, per l'integrazione con altre applicazioni), anche questi dovranno essere riscritti per adattarsi alle API del nuovo provider.

PaaS Lock-in

Il lock-in di tipo PaaS si verifica sia al livello API (per esempio, a causa di chiamate ad API specifiche della piattaforma) sia a livello di componente. Ad esempio, il provider PaaS può offrire un data store di back-end molto efficiente. Non solo il cliente deve sviluppare del codice utilizzando le API proprietarie offerte dal provider, ma deve anche codificare le procedure di accesso ai dati in un modo tale da essere compatibile con il data store di back-end.

Il codice non sarà necessariamente portabile tra provider PaaS, anche se vengono offerte delle API apparentemente simili, in quanto il modello di accesso ai dati può essere differente (ad esempio, relazionale invece che hashing).

- Il lock-in PaaS a livello API si verifica ogniqualvolta provider diversi offrono API differenti.
- Il lock-in PaaS si verifica a livello di runtime siccome spesso runtime 'standard' vengono pesantemente personalizzati per funzionare in modo sicuro in un ambiente cloud. Per esempio, a un runtime di Java possono essere rimosse delle chiamate 'pericolose', o comunque modificate per motivi di sicurezza. Rimane agli sviluppatori dei clienti l'onere di comprendere e tenere in conto tali differenze.

Inoltre il fornitore cloud potrebbe affidare in outsourcing o subappaltare servizi a terze parti (fornitori sconosciuti) che potrebbero non offrire le stesse garanzie (quali la fornitura del servizio a norma di legge) proposte dal fornitore cloud. O il controllo del fornitore cloud cambia, così che pure i termini e le condizioni di servizio potrebbero cambiare.

- Il modello PaaS soffre anche del lock-in dei dati, nello stesso modo che nel modello SaaS, ma in questo caso l'onere di creare procedure di esportazione incombe totalmente a carico del cliente.

Nell'utilizzo di infrastrutture cloud, il cliente cede necessariamente al fornitore cloud il controllo su un certo numero di aspetti che potrebbero interessare la sicurezza. Ad esempio, i Termini di Utilizzo potrebbero proibire scansioni delle porte, vulnerability assessment e penetration test. Inoltre, potrebbero esserci conflitti tra le procedure di hardening del cliente e l'ambiente cloud (si veda R 20). D'altro canto, gli SLA potrebbero non offrire un impegno da parte del fornitore cloud a fornire tali servizi, lasciando perciò un'area scoperta nella difesa della sicurezza.

IaaS-Lock-in

II lock-in di tipo IaaS varia in relazione agli specifici servizi in infrastruttura utilizzati. Per esempio, un cliente che utilizza cloud storage non subirà un impatto da formati non compatibili delle virtual machine.

- I provider di servizi IaaS tipicamente offrono virtual machines basate su hypervisor. Il software e i metadati sono impacchettati insieme per la portabilità – tipicamente soltanto all'interno del cloud del provider. La migrazione tra provider non sarà semplice fino a quando non verranno adottati degli standard aperti, come OVF (11).
- L'offerta dei provider di storage IaaS può variare da semplici archivi basati su chiave/valore fino ad archivi policy-based basati su file. Può variare molto l'insieme delle caratteristiche, così come fanno le semantiche dello storage. Tuttavia la dipendenza a livello applicativo da specifiche caratteristiche delle policy (ad esempio, i controlli d'accesso) può limitare la scelta del provider da parte del cliente.
- Il lock-in dei dati è l'ovvia preoccupazione nel caso di servizi di storage IaaS. Quanto più i clienti del cloud portano dati nello storage di tipo cloud, tanto più il lock-in sui dati cresce, a meno che il CP non dia supporto per la portabilità dei dati.

Comune a tutti i provider è la possibilità di uno scenario di "corsa agli sportelli" per un dato cloud provider. Un tale scenario suppone che ci sia una crisi di fiducia nella posizione finanziaria del cloud provider, che genera una conseguente uscita e ritiro di massa dei contenuti, sulla logica del primo arrivato, primo servito. Quindi, in una situazione in cui un provider limiti la quantità di 'contenuti' (dati e codice applicativo) che può essere 'ritirata' in una determinata quantità di tempo, alcuni clienti non saranno mai in grado di recuperare i propri dati e le proprie applicazioni.

R.2 Perdita di governance

Probabilità	MOLTO ALTA	Comparativo: Più Alto
Impatto	MOLTO ALTO (dipende dall'organizzazione) (IaaS MOLTO ALTO, SaaS Basso)	Comparativo: Uguale
Vulnerabilità	V34. Ruoli e responsabilità non chiari V35. Implementazione carente di ruoli e definizioni V21. Sincronizzazione di responsabilità o obblighi contrattuali esterni al cloud V23. Clausole negli SLA con promesse in conflitto verso diversi stakeholder V25. Audit o certificazioni non rese disponibili ai clienti V22. Applicazioni cross-cloud che creano dipendenze nascoste V13. Mancanza di tecnologie e di soluzioni standard V29. Memorizzazione dei dati in giurisdizioni multiple e mancanza di trasparenza in merito V14. Nessun accordo di contratto sul codice sorgente (source escrow) V16. Nessun controllo sul processo di valutazione delle vulnerabilità V26. Schemi di certificazione non adattati alle infrastrutture cloud V30. Mancanza di informazioni sulle giurisdizioni V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso V44. Proprietà dell'asset non chiara	
Assets interessati	A1. Reputazione aziendale A2. Fiducia dei clienti A3. Lealtà ed esperienza del dipendente A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi real time A10. Erogazione del servzio	
Rischio	**ALTO**	

Nell'utilizzo delle infrastrutture cloud, il cliente cede necessariamente il controllo al CP su una serie di aspetti che possono minare la sicurezza. Ad esempio le CdU possono proibire attività di port scan, valutazione delle vulnerabilità e di penetration test. Inoltre possono sussistere conflitti tra le procedure di hardening

del cliente e l'ambiente cloud (vedi R20). D'altra parte gli SLA possono non impegnare il fornitore cloud a fornire tali servizi, lasciando così un varco nelle misure di sicurezza.

Inoltre il cloud provider può dare in outsourcing o subappaltare i servizi a terze parti (fornitori sconosciuti) che potrebbero non offrire le medesime garanzie (come ad esempio erogare il servizio in modo legale) dichiarate dal cloud provider. Oppure cambia il controllo del cloud provider, cosicché i termini e le condizioni dei loro servizi possono cambiare.

La perdita di governance e di controllo potrebbe avere un potenziale grave impatto sulla strategia dell'organizzazione, e quindi sulla capacità di rispettare la propria mission e i propri obiettivi. La perdita di controllo e di governance può portare all'impossibilità di conformarsi ai requisiti di sicurezza, alla perdita di confidenzialità, integrità e disponibilità dei dati, e al deterioramento delle prestazioni e della qualità del servizio, per non menzionare l'introduzione di rischi per la conformità (vedi R3).

R.3 Conformità

Probabilità	MOLTO ALTO – dipende da PCI, SOX	Comparativo: Più alto
Impatto	ALTO	Comparativo: Uguale
Vulnerabilità	V25. Audit o certificazioni non rese disponibili ai clienti V13. Mancanza di tecnologie e di soluzioni standard V29. Memorizzazione dei dati in giurisdizioni multiple e mancanza di trasparenza in materia V26. Schemi di certificazione non adattati alle infrastrutture cloud V30. Mancanza di informazioni sulle giurisdizioni V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso	
Assets Interessati	A20. Certificazione	
Rischio	**ALTO**	

Nella migrazione al Cloud, alcune organizzazioni hanno fatto considerevoli investimenti per conseguire certificazioni sia per avere un vantaggio competitivo che per soddisfare standard industriali o requisiti regolamentari (ad esempio, PCI DSS).

Alcune organizzazioni che migrano verso il cloud hanno fatto considerevoli investimenti per conseguire la certificazione sia per vantaggio competitivo sia per rispettare gli standard industriali o i requisiti normativi (ad esempio, PCI DSS). Gli investimenti possono essere messi a rischio con la migrazione al cloud:

- se il CP non può fornire l' evidenza della propria conformità ai requisiti applicabili;
- se il CP non consente al cliente di effettuare audit.

In alcuni casi, ciò significa anche che utilizzare un'infrastruttura cloud pubblica implichi che alcuni tipi di conformità non possano essere conseguite e dunque che servizi ospitati sul cloud non possano essere utilizzati per i servizi che ne hanno necessità. Ad esempio, EC2 afferma che i clienti avrebbero difficoltà a

ottenere la conformità alla PCI sulla propria piattaforma. E così i servizi ospitati su EC2 non possono essere utilizzati per le transazioni con carta di credito.

R.4 Danno reputazionale a causa di attività di co-tenants

Probabilità	BASSO
Impatto	ALTO
Vulnerabilità	V5. Vulnerabilità dell'hypervisor V6. Mancanza di isolamento delle risorse V7. Mancanza di isolamento reputazionale
Assets interessati	A1. Reputazione aziendale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi real time A10. Erogazione del servizio
Rischio	**MEDIO**

La condivisione delle risorse significa che attività malevole condotte da un tenant possono avere effetto sulla reputazione di un altro. Ad esempio, lo spamming, il port scanning o l'esposizione di contenuti malevoli dall'infrastruttura cloud possono portare a:

- Il blocco di un range di indirizzi IP, che include sia quelli dell'attaccante sia quelli di altri tenant innocenti nella medesima infrastruttura;
- Confisca di risorse a causa di attività dei tenant contigui (per citazione in giudizio di un tenant)

La condivisione delle risorse implica che attività malevole condotte da un co-tenant possano interessare la reputazione di un altro co-tenant.

L'impatto può riguardare il deterioramento dell'erogazione del servizio e la perdita di dati, così come problemi reputazionali dell'organizzazione.

R.5 Cessazione o fallimento del servizio cloud

Probabilità	N/A	
Impatto	MOLTO ALTO	Comparativo: Più alto
Vulnerabilità	V46. Scarsa selezione di fornitori V47. Mancanza di ridondanza di fornitori V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso	
Assets interessati	A1. Reputazione Aziendale A2. Fiducia dei clienti A3. Lealtà ed esperienza del cliente A9. Erogazione del servizio – servizi real time A10. Erogazione del servizio	
Rischio	**MEDIO**	

Come in ogni nuovo mercato IT, la pressione per la competizione, strategie di business inadeguate, la mancanza di sostegno finanziario, ecc. possono portare alcuni provider ad uscire dal business o almeno a costringerli a ristrutturare il portfolio dell'offerta dei propri servizi. In altre parole, è possibile che nel breve o medio termine alcuni servizi di cloud computing possano essere cessati.

L'impatto di questa minaccia per il cliente del cloud è facilmente intuibile, dal momento che può portare ad una perdita o al deterioramento delle prestazioni nell'erogazione di un servizio, sulla qualità del servizio, così come ad una perdita degli investimenti.

Inoltre, fallimenti in servizi esternalizzati verso il CP, possono avere un impatto significativo sulla capacità del cliente del cloud di rispettare i propri doveri ed obblighi verso i propri clienti. Il cliente del cloud provider può quindi trovarsi esposto a responsabilità contrattuali anche contorte verso i propri clienti a causa della negligenza del proprio fornitore. I fallimenti dei cloud provider possono

avere effetto anche in termini di responsabilità del cliente verso i propri dipendenti.

R.6 Acquisizione del fornitore cloud

Probabilità	N/A	
Impatto	MEDIO	Comparativo: Più alto
Vulnerabilità	V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso	
Assets interessati	A1. Reputazione aziendale A2. Fiducia dei clienti A3. Lealtà ed esperienza del dipendente A4. Proprietà intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati sulle risorse umane (HR) A9. Erogazione del servizio – servizi real time A10. Erogazione del servzio	
Rischio	**MEDIO**	

L'acquisizione del cloud provider può aumentare la probabilità di un cambiamento strategico e può mettere a rischio accordi non vincolanti (come ad esempio le interfacce software, gli investimenti sulla sicurezza, i controlli di sicurezza non contrattualizzati). Ciò potrebbe rendere impossibile soddisfare i requisiti di sicurezza. L'impatto finale potrebbe essere il danneggiamento di asset cruciali quali: la reputazione dell'organizzazione, la fiducia dei clienti o dei pazienti, e la fedeltà e la soddisfazione dei dipendenti.

R.7 Fallimento del ciclo di approvvigionamento

Probabilità	BASSA	Comparativo: Più alto
Impatto	MEDIO	Comparativo: Più alto
Vulnerabilità	V31. Mancanza di completezza e trasparenza nelle condizioni d'uso V22. Applicazioni cross-cloud che creano dipendenze nascoste V46. Carente selezione dei fornitori V47. Ridondanza dei fornitori assente	
Assets interessati	A1. Reputazione aziendale A2. Fiducia dei clienti A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi real time A10. Erogazione del servzio	
Rischio	**MEDIO**	

Un Cloud provider può terzializzare alcune attività specialistiche della propria catena di 'produzione'. In una tale situazione il livello di sicurezza del cloud provider può dipendere dal livello di sicurezza di ciascuna delle connessioni e dal livello di dipendenza del cloud provider dalle terze parti.

Ogni interruzione o corruzione nella catena o mancanza di coordinamento delle responsabilità tra tutte le parti coinvolte può portare a: indisponibilità dei servizi, perdita della confidenzialità, integrità e disponibilità dei dati, perdite economiche e di reputazione a causa dell'incapacità di soddisfare le esigenze dei clienti, violazioni degli SLA, fallimento dei servizi in cascata, ecc.

Un importante esempio di questo tipo è l'esistenza di una dipendenza critica da un servizio di single-sign-on o di identity management di terze parti. In questo caso, un'interruzione del servizio della terza parte o della connessione del CP verso il servizio o una debolezza nelle loro procedure di sicurezza, possono compromettere la disponibilità o la confidenzialità di un cliente del cloud o addirittura dell'intera offerta cloud.

In tale situazione il livello di sicurezza del cloud provider potrebbe dipendere dal livello di sicurezza di ciascuno dei collegamenti e dal livello di dipendenza da terze parti del cloud provider stesso.

In generale, una mancanza di trasparenza nel contratto può essere un problema per l'intero sistema. Se un provider non dichiara quali servizi IT centrali siano dati all'esterno – non è realistico che il fornitore debba elencare i propri fornitori dal momento che questi possono cambiare frequentemente – il cliente non si trova in una posizione tale da poter valutare appropriatamente il rischio che sta affrontando. Questa mancanza di trasparenza potrebbe ridurre il livello di affidabilità del provider.

RISCHI TECNICI

R.8 Esaurimento delle risorse (sotto o sovra approvvigionamento)

Probabilità	**A**. Incapacità di fornire ulteriore capacità al cliente: MEDIO	Comparativo: N/A
	B. Incapacità di fornire il livello corrente di capacità concordato: BASSO	Comparativo: Più alto
Impatto	**A**. Incapacità di fornire ulteriore capacità al cliente: BASSO/MEDIO (ad esempio, sotto Natale)	Comparativo: N/A
	B. Incapacità di fornire il livello corrente di capacità concordato: ALTO	Comparativo: Uguale
Vulnerabilità	V15. Modellazione non accurata dell'utilizzo delle risorse V27. Inadeguatezza dell'erogazione delle risorse e degli investimenti in infrastrutture V28. Mancanza di politiche per il fissare l'utilizzo massimo delle risorse V47. Mancanza di ridondanza di fornitori	
Assets interessati	A1. Reputazione aziendale A2. Fiducia del cliente A10. Erogazione del servizio A11. Controllo degli accessi / autenticazione / autorizzazione (root/admin verso altri)	
Rischio	**MEDIO**	

I servizi di tipo cloud sono servizi su richiesta [vedi Cloud computing – definizione di riferimento]. DI conseguenza c'è un certo rischio calcolato nell'allocazione di tutte le risorse di un servizio cloud, poiché le risorse vengono allocate in accordo a proiezioni statistiche. Una modellazione non accurata dell'utilizzo delle risorse – i comuni algoritmi di allocazione delle risorse sono vulnerabili a distorsioni dell'imparzialità – oppure una inadeguata erogazione di

risorse ed investimenti inadeguati in infrastrutture possono portare, dal punto di vista del CP, a:

- Indisponibilità del servizio: difetti in certi scenari applicativi altamente specifici che utilizzano una particolare risorsa in modo molto intensivo (ad esempio, elaborazioni macina-numeri o simulazioni che fanno pesante uso di memoria o CPU, come le previsioni delle quotazioni di borsa);
- Compromissione del controllo degli accessi: in alcuni casi può essere possibile forzare un sistema a consentire l'accesso in caso di esaurimento delle risorse. [rif: CWE-400: Consumo non controllato delle risorse: Esaurimento delle risorse (12)];
- Perdite economiche e di reputazione: a causa dell'incapacità di soddisfare la domanda dei clienti.

Le opposte conseguenze della stima non accurata delle necessità di risorse possono portare a:

- Sovradimensionamento dell'infrastruttura: un eccesso di disponibilità di risorse che porta a perdite economiche e a una perdita di profitti.

Quindi c'è un livello di rischio calcolato nell'allocamento di tutte le risorse di un servizio cloud, perché le risorse sono allocate sulla base di proiezioni statistiche.

Dal punto di vista del cliente del cloud, la selezione di un provider inadeguato e la mancanza di una ridondanza di fornitori potrebbe portare a:

- Indisponibilità dei servizi: fallimento nell'erogare (o degrado delle prestazioni) dei servizi sia in tempo reale che non in tempo reale;
- Sistema di controllo degli accessi compromesso: mette a rischio la confidenzialità e l'integrità dei dati;
- Perdite economiche e di reputazione: dovute all'incapacità di soddisfare la domanda, a violazioni degli SLA, al fallimento dei servizi in cascata, ecc.

Nota: questo rischio potrebbe essere anche una conseguenza di un attacco di tipo DDoS (vedi R.15) e del comportamento non corretto di applicazioni a causa di una scarsa compartimentalizzazione delle applicazioni nei sistemi di alcuni cloud provider.

R.9 Mancato isolamento

Probabilità	BASSO (Private Cloud)	Comparativo: Più alto
Impatto	MOLTO ALTO	Comparativo: Più alto
Vulnerabilità	V5. Vulnerabilità dell'hypervisor V6. Mancanza di isolamento delle risorse V7. Mancanza di isolamento reputazionale V17. Possibilità di esplorazione della rete interna (del cloud) V18. Possibilità che vengano effettuati dei controlli di co-residenza	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio	
Rischio	**ALTO**	

La multi-tenancy e la condivisione delle risorse sono due delle caratteristiche che definiscono gli ambienti di cloud computing. La capacità di elaborazione, lo storage, e la rete sono condivisi tra più utenti.

Questa classe di rischi include il fallimento dei meccanismi che separano lo storage, la memoria, il routing e persino la reputazione tra differenti tenants dell'infrastruttura condivisa (ad esempio, gli attacchi cosiddetti guest-hopping, attacchi del tipo SQL injection che espongono dati di più clienti che stanno nella stessa tabella, e gli attacchi di tipo side channel).

Si noti che la probabilità di questo scenario di incidente dipende dal modello di cloud considerato; è probabilmente bassa per cloud privati e più elevata (media) nel caso di cloud pubblici.

L'impatto, per il fornitore cloud e i suoi clienti, può essere una perdita di dati di valore o sensibili, danno reputazionale e interruzione del servizio.

Questa classe di rischi include il fallimento dei meccanismi che separano lo storage, la memoria, il routing e persino la reputazione tra differenti tenants dell'infrastruttura condivisa (ad esempio, gli attacchi cosiddetti guest-hopping, attacchi del tipo SQL injection che espongono dati di più clienti che stanno nella stessa tabella, e gli attacchi di tipo side channel).

R.10 Insider malevolo presso il cloud provider – Abuso di ruoli con privilegi elevati

Probabilità	MEDIA (Inferiore a quella tradizionale)	Comparazione: inferiore
Impatto	MOLTO ALTO (Superiore a quello tradizionale)	Comparazione: superiore (aggregato) Comparazione: Uguale (per il singolo cliente)
Vulnerabilità	V1. Vulnerabilità AAA V34. Ruoli e responsabilità non definiti V35. Applicazione carente delle definizioni dei ruoli V36. Mancata applicazione del principio del need to know V39. Vulnerabilità di Sistema o sistema operativo V37. Procedure di sicurezza fisica inadeguate V10. Impossibilità di trattare i dati in forma cifrata V48. Vulnerabilità applicative o gestione degli aggiornamenti insufficiente	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A3. Lealtà ed esperienza dei dipendenti A4. Proprietà Intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati delle Risorse Umane (HR) A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio	

Rischio	ELEVATO

Le attività malevole di un insider potrebbero impattare su: confidenzialità, integrità e disponibilità di tutti i tipi di dati, sulla Proprietà Intellettuale, e su ogni tipo di servizio, impattando quindi indirettamente sulla reputazione dell'organizzazione, sulla fiducia della clientela e sull'esperienza dei dipendenti. Ciò riveste una particolare importanza nel caso del cloud computing perché le architetture cloud necessitano di ruoli che possono presentare un rischio estremamente alto. Esempi di tali ruoli includono gli amministratori di sistema del CP, i suoi auditor e i servizi di sicurezza gestiti che operano sui report di intrusione e sulla risposta agli incidenti. Al crescere dell'utilizzo del cloud, i dipendenti dei cloud provider sono sempre di più soggetti ad attacchi da parte di gruppi criminali (analogamente a quanto è stato osservato per i dipendenti dei call center nell'industria dei servizi finanziari (13), (14)).

R.11 Compromissione dell'interfaccia di gestione (Manipolazione, disponibilità dell'infrastruttura)

Probabilità	MEDIA	Comparativo: Superiore
Impatto	MOLTO ALTO	Comparativo: Superiore
Vulnerabilitià	V1. Vulnerabilità AAA V4. Accesso remoto all'interfaccia di amministrazione V38. Malconfigurazione V39. Vulnerabilità di sistema o del sistema operativo V48. Vulnerabilità delle applicazioni o inadeguata gestione degli aggiornamenti	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio A14. Interfaccia di gestione dei servizi cloud	
Rischio	**MEDIO**	

Le interfacce di amministrazione del cliente dei cloud provider pubblici sono accessibili da Internet e mediano l'accesso verso insiemi di risorse più ampi (rispetto ai tradizionali provider di hosting) e presentano perciò un rischio aumentato specialmente quando combinate con l'accesso remoto e con le vulnerabilità dei browser web.

Le interfacce di amministrazione del cliente dei cloud provider pubblici sono accessibili da Internet e mediano l'accesso verso set di risorse più ampi (rispetto ai tradizionali provider di hosting) e pongono perciò un rischio aumentato specialmente quando combinate con l'accesso remoto e con le vulnerabilità dei browser web.

Ciò include le interfacce del cliente che controllano più macchine virtuali e, cosa più importante, le interfacce del CP che controllano l'operatività dell'intero sistema cloud. Naturalmente, il rischio può essere mitigato con maggiori investimenti nei fornitori di sicurezza.

R.12 Intercettazione dei dati in transito

Probabilità	MEDIO	Comparativo: Più alto (per un determinato dato)
Impatto	ALTO	Comparativo: Uguale
Vulnerabilità	V1. Vulnerabilità AAA V8. Vulnerabilità della crittografia delle comunicazioni V9. Mancanza o debolezza della crittografia degli archivi e dei dati in transito V17. Possibilità di esplorazione della rete interna (al cloud) V18. Possibilità che vengano effettuati dei controlli di co-residenza V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso	
Asset interessati	A1. Reputazione aziendale A2. Fiducia della clientela A4. Proprietà intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati delle Risorse Umane (HR) A23. Dati di backup o d'archivio	
Rischio	**MEDIO**	

Il cloud computing, essendo un'architettura distribuita, implica una maggior quantità di dati in transito rispetto alle infrastrutture tradizionali. Ad esempio, i dati devono essere trasferiti al fine di sincronizzare multiple immagini distribuite di macchine, immagini distribuite attraverso molteplici macchine fisiche, tra l'infrastruttura cloud e client web remoti, ecc. Inoltre, il principale utilizzo dell'hosting in data center viene implementato utilizzando un ambiente con connessioni sicure analoghe alle VPN, una prassi non sempre seguita nel contesto cloud.

Attacchi di sniffing, spoofing e di man-in-the-middle, attacchi di side channel e replay dovrebbero essere considerati come possibili fonti di minacce. In aggiunta, in alcuni casi il CP non offre clausole di confidenzialità o di riservatezza oppure tali clausole non sono sufficienti a garantire il rispetto della protezione delle informazioni segrete del cliente e del 'know-how' che circola nel 'cloud'.

R.13 Perdita di dati in up/download verso e tra cloud

Probabilità	MEDIO (N/A)
Impatto	ALTO
Vulnerabilità	V1. Vulnerabilità AAA V8. Vulnerabilità della crittografia delle comunicazioni V17. Possibilità di esplorazione della rete interna (al cloud) V10. Impossibilità di elaborare dati in forma criptata V48. Vulnerabilità delle applicazioni o inadeguata gestione degli aggiornamenti
Asset interessati	A1. Reputazione aziendale A2. Fiducia della clientela A3. Lealtà ed esperienza del personale A4. Proprietà Intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati delle Risorse Umane (HR) A12. Credenziali A13. Directory degli utenti (dati) A14. Interfaccia di gestione del servizio cloud
Rischio	**MEDIO**

Questo rischio è identico al precedente, ma si applica al trasferimento di dati tra il cloud provider ed il cliente del cloud.

R.14 Eliminazione insicura o inefficace dei dati

Probabilità	MEDIA	Comparativo: Più alta
Impatto	Molto ALTA	Comparativo: Più alto
Vulnerabilità	V20. Sanitizzazione di supporti sensibili (sensitive media sanitization)	
Assets Interessati	A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A12. Credenziali	
Rischio	**MEDIO**	

Ogniqualvolta si cambia fornitore, le risorse vengono ridimensionate, l'hardware fisico viene riallocato, ecc., i dati possono rimanere disponibili oltre al tempo specificato nelle policy di sicurezza. Può risultare impossibile eseguire le procedure specificate dalle policy di sicurezza, dal momento che la completa eliminazione dei dati è possibile soltanto distruggendo un disco che contiene dati anche di altri clienti. Quando viene fatta una richiesta per l'eliminazione di una risorsa del cloud, questa può non risolversi in una reale eliminazione dei dati (come accade sui principali sistemi operativi). Ove è richiesta l'effettiva eliminazione dei dati, si devono seguire procedure speciali e ciò può non essere supportato dalle API standard (o non supportato del tutto).

Se viene utilizzata la crittografia, allora il rischio può essere considerato minore.

R.15 Negazione del servizio distribuita (DDOS)

Probabilità	Cliente: MEDIO	Comparativo: Più basso
	Fornitore: BASSO	Comparativo: N/A
Impatto	Cliente: ALTO	Comparativo: Più alto
	Fornitore: MOLTO ALTO	Comparativo: Più basso
Vulnerabilità	V38. Configurazioni errate V39. Vulnerabilità di sistema o del sistema operativo V53. Risorse di filtering inadeguate o mal configurate	
Assets Interessati	A1. Reputazione aziendale A2. Fiducia della clientela A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio A14. Interfaccia di gestione del servizio cloud A16. Rete (connessioni, ecc.)	
Rischio	**MEDIO**	

R.16 Negazione del servizio di natura economica (EDOS)

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	V1. Vulnerabilità AAA V2. Vulnerabilità nell'assegnazione delle risorse V3. Vulnerabilità nella revoca delle risorse V4. Accesso remoto all'interfaccia di amministrazione V28. Mancanza di politiche per il fissare l'utilizzo massimo delle risorse
Assets Interessati	A1. Reputazione aziendale A2. Fiducia della clientela A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio
Rischio	**MEDIO**

Vi sono diversi possibili scenari in cui le risorse di un cliente del cloud possono essere utilizzate da altre parti in modi malevoli che hanno un impatto economico:

Esistono differenti scenari nei quali le risorse di un cliente cloud potrebbero essere usate da altri in modo malevolo che ha un impatto economico.

- Furto d'identità: un attaccante utilizza un account e utilizza le risorse del cliente per il proprio profitto personale o al fine di danneggiare economicamente il cliente.
- Il cliente del cloud non ha impostato efficacemente i limiti all'utilizzo di risorse pagate a consumo e riscontra un carico inaspettato su tali risorse attraverso azioni non malevole.
- Un attaccante utilizza un canale pubblico per utilizzare le risorse a pagamento del cliente – ad esempio, ove il cliente paghi per ogni richiesta http, un attacco DDoS può avere questo effetto.

L'EDoS distrugge le risorse economiche; lo scenario nel caso peggiore potrebbe essere il fallimento del cliente o un serio impatto economico. NOTA: il generico asset DENARO non è menzionato nell'elenco.

R.17 Perdita delle chiavi di cifratura

Probabilità	BASSA	Comparativo: N/A
Impatto	ALTO	Comparativo: Più alto
Vulnerabilità	V11. Procedure scadenti di gestione delle chiavi V12. Generazione delle chiavi: bassa entropia per il generatore di numeri casuali	
Assets interessati	A4. Proprietà Intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle Risorse Umane (HR) A12. Credenziali	
Rischio	**MEDIO**	

Questo rischio include la diffusione di chiavi segrete (SSL, crittografia dei file, chiavi private del cliente, ecc.) o di password a malintenzionati, la perdita o la corruzione di tali chiavi, ed il loro utilizzo non autorizzato per l'autenticazione ed il non ripudio (firma digitale).

R.18 Esecuzione di indagini e scansioni malevole

Probabilità	MEDIA	Comparativo: Più bassa
Impatto	MEDIO	Comparative: Più basso
Vulnerabilità	V17. Possibilità di esplorazione della rete interna (del cloud) V18. Possibilità che vengano effettuati dei controlli di co-residenza	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio	
Rischio	**MEDIO**	

Indagini o scansioni malevole, così come la mappatura delle reti, sono minacce indirette all'asset considerato. Possono essere utilizzate per raccogliere informazioni nel contesto di un tentativo di hacking. Un possibile impatto può essere quello della perdita di confidenzialità, integrità e disponibilità di servizi e dati.

R.19 Compromissione del motore del servizio

Probabilità	BASSA
Impatto	MOLTO ALTO
Vulnerabilità	V5. Vulnerabilità dell'hypervisor V6. Carenza di isolamento delle risorse
Assets interessati	A5. Dati Personali sensibili A6. Dati Personali A7. Dati Personali - critici A8. Dati delle Risorse Umane (HR) A9. Erogazione del servizio – Servizi in tempo reale A10. Erogazione del servizio
Rischio	**MEDIO**

Ogni architettura cloud si appoggia su una piattaforma altamente specializzata, in cui un motore del servizio siede sopra le risorse hardware fisiche e gestisce le risorse dei clienti a differenti livelli di astrazione. Ad esempio, nei cloud di tipo IaaS questo componente software può essere l'hypervisor. Il motore del servizio viene sviluppato e supportato dai venditori di piattaforme cloud ed in alcuni casi dalla comunità open source. Può quindi essere ulteriormente personalizzato dai fornitori di cloud computing.

Come ogni altro strato software, il codice del motore del servizio può avere delle vulnerabilità ed è soggetto ad attacchi o a malfunzionamenti inattesi. Un attaccante può compromettere il motore del servizio forzandolo dall'interno di una macchina virtuale (cloud IaaS), dall'ambiente di sistema (cloud PaaS), dal pool delle applicazioni (cloud SaaS), o attraverso le API.

Forzare il motore del servizio può essere utile per evadere dall'isolamento tra i differenti ambienti dei clienti (jailbreak) e ottenere l'accesso ai dati contenuti al loro interno, per controllare e modificare le

I fornitori Cloud devono implementare una chiara separazione delle responsabilità che dettagli le minime azioni che i clienti devono intraprendere.

informazioni al loro interno in modo trasparente (senza interazioni dirette con le applicazioni all'interno dell'ambiente del cliente), o per ridurre le risorse a loro assegnate, causando l'indisponibilità del servizio.

R.20 Conflitti tra le procedure di hardening del cliente e l'ambiente cloud

Probabilità	BASSA
Impatto	MEDIO
Vulnerabilità	V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso V23. Clausole negli SLA con promesse in conflitto verso diversi stakeholder V34. Ruoli e responsabilità non chiari
Assets interessati	A4. Proprietà Intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali – critici
Rischio	**MEDIO**

I fornitori cloud devono impostare una chiara segregazione delle responsabilità che definisca le azioni minime che i clienti devono intraprendere. L'incapacità dei clienti nel rendere sicuri in modo appropriato i propri ambienti può presentare una vulnerabilità verso la piattaforma cloud se il fornitore cloud non ha intrapreso i passi necessari per garantire l'isolamento. I fornitori cloud dovrebbero inoltre esporre i propri meccanismi di isolamento e fornire le linee guida basate sulle *best practice* per assistere i propri clienti nel rendere sicure le proprie risorse.

I clienti devono riconoscere e assumersi le proprie responsabilità in quanto il non farlo potrebbe esporre i loro dati e risorse ad ulteriori rischi.

I clienti devono riconoscere e assumersi le proprie responsabilità in quanto l'incapacità di fare ciò potrebbe esporre i loro dati e le loro risorse ad ulteriori rischi. I clienti del cloud, in alcuni casi, hanno impropriamente assunto che il fornitore cloud fosse responsabile, e stesse gestendo, tutte le attività richieste per garantire la sicurezza dei propri dati. Questa assunzione da parte del cliente, e/o la mancanza di una chiara elencazione da parte del fornitore cloud, ha posto rischi non necessari sui dati del cliente. È imperativo che il cliente del cloud identifichi le proprie responsabilità e si conformi a esse.

I cloud provider, per la loro stessa natura, hanno il compito di fornire ambienti

multi-tenant, sia che questo avvenga mediante la virtualizzazione su un server sia che avvenga sulla rete comune condivisa dai clienti. La co-locazione di molti clienti inevitabilmente crea conflitti per il cloud provider in quanto è probabile che i requisiti dei clienti per la sicurezza delle comunicazioni siano divergenti tra di loro.

Si prenda, per esempio, il caso di due clienti su una tradizionale infrastruttura di rete condivisa. Se un cliente vuole che il firewall blocchi tutto il traffico tranne quello SSH, mentre un altro cliente che gestisce una web server farm richiede il passaggio di traffico HTTP e HTTPS, chi vince? Lo stesso tipo di problema viene sollevato da clienti che hanno requisiti di compliance in competizione ed in conflitto. Questo tipo di sfida può solo peggiorare con l'aumentare del numero dei tenant e con la disparità dei loro requisiti. Perciò i fornitori cloud devono trovarsi in una posizione tale da poter gestire queste sfide attraverso la tecnologia, le policy e la trasparenza (ove appropriato).

RISCHI LEGALI

R.21 Ordine di comparizione o di produzione in giudizio e acquisizione delle prove elettroniche nel processo (c.d. e-discovery)

Probabilità	ALTA
Impatto	MEDIO
Vulnerabilità	V6. Carenza di isolamento delle risorse V29. Conservazione dei dati in più giurisdizioni e carenza di trasparenza in proposito V30 Carenza di informazioni sulle giurisdizioni
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7 Dati personali - critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio
Rischio	**ELEVATO**

Nell'eventualità di un sequestro dell'hardware fisico da parte delle forze dell'ordine come risultato di un ordine di comparizione o di produzione in giudizio o di una causa civile (15), l'accentramento dello storage, così come l'affitto condiviso dell'hardware fisico, implica che molti più clienti rischino la divulgazione dei propri dati a parti indesiderate (16), (17), (18).

Allo stesso tempo, potrebbe essere impossibile per l'autorità di una singola nazione sequestrare un 'cloud' in virtù dei grandi progressi fatti nella migrazione su lunga distanza degli hypervisor.

R.22 Rischi derivanti dal cambio di giurisdizione

Probabilità	MOLTO ALTA
Impatto	ALTO
Vulnerabilità	V29. Conservazione dei dati in più giurisdizioni e carenza di trasparenza in proposito V30 Carenza di informazioni sulle giurisdizioni
Aassets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7 Dati personali - critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio
Rischio	**ALTO**

I dati dei clienti potrebbero essere conservati in più giurisdizioni, alcune delle quali potrebbe essere ad alto rischio. Se i data center sono localizzati in Paesi ad alto rischio, ad esempio quelli che non hanno uno stato di diritto e hanno un imprevedibile contesto legale e di attuazione, stati di polizia autocratici, stati che non rispettano gli accordi internazionali, ecc., i siti potrebbero essere perquisiti dalle autorità locali e i dati o i sistemi essere oggetto di divulgazione forzata o di sequestro. Si noti che non si sta qui intendendo che tutte le misure di ordine di comparizione o di produzione in giudizio della polizia siano inaccettabili, ma solo che alcune potrebbero esserlo, e che alcuni legittimi sequestri di hardware (che risultano rari) potrebbero interessare più clienti rispetto a quello che è l'obiettivo dell'azione delle forze dell'ordine, in relazione a come sono conservati i dati (19), (20).

R.23 Rischi per la protezione dei dati

Probabilità	ALTA
Impatto	BASSO
Vulnerabilità	V29. Storage dei dati in più giurisdizioni e carenza di trasparenza in proposito V30 Carenza di informazioni sulle giurisdizioni
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7 Dati personali - critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio
Rischio	**ELEVATO**

Il cloud computing comporta diversi rischi di protezione dei dati per i clienti e per i fornitori di cloud.

- Può essere difficile per il cliente del cloud (nel suo ruolo di titolare del trattamento) controllare efficacemente il trattamento dei dati che il cloud provider svolge, e quindi essere sicuro che i dati siano trattati in modo lecito. Deve essere chiaro che il cliente del cloud sarà il principale responsabile del trattamento dei dati personali, anche quando tale trattamento è effettuato dal cloud provider nel suo ruolo di incaricato esterno al trattamento. Il mancato rispetto della legge sulla protezione dei dati può comportare sanzioni amministrative, civili e anche penali, che variano da Paese a Paese, per il titolare del trattamento. Questo problema è aggravato nel caso di trasferimenti multipli di dati, ad esempio tra cloud federati. D'altro lato, alcuni fornitori di servizi cloud forniscono informazioni sulle modalità di trattamento dei dati che svolgono. Alcuni offrono anche una sintesi di certificazione del loro trattamento dei dati, delle attività di sicurezza sui dati e dei controlli dei dati che hanno messo in campo, ad esempio. SAS70 certificazione fornitori.

- Ci possono essere violazioni della sicurezza dei dati che non vengono notificati al titolare dei dati da parte del cloud provider.
- Il cliente del cloud può perdere il controllo dei dati trattati dal cloud provider. Questo problema aumenta nel caso di trasferimenti multipli di dati (ad esempio, tra i fornitori di cloud federati).
- Il cloud provider può ricevere dati che non sono stati legalmente raccolti dal suo cliente (il titolare).

R.24 Rischi di licenza

Probabilità	MEDIA	Comparativo: Più alta
Impatto	MEDIO	Comparativo: Più alto
Vulnerabilità	V31. Mancanza di completezza e di trasparenza nelle condizioni d'uso	
Assets interessati	A1. Reputazione aziendale A9. Erogazione del servizio – servizi in tempo reale A20. Certificazione	
Rischio	**MEDIO**	

Alcune condizioni di licenza, come ad esempio accordi per sito e verifiche di licenze on-line, possono diventare impraticabili in un ambiente cloud. Per esempio, se il software viene fatturato sulla base di ogni singola istanza, ogni volta che una nuova macchina viene attivata, i costi di licenza del cliente del cloud potrebbero aumentare in modo esponenziale, anche se sta utilizzando lo stesso numero di istanze di macchine per la stessa durata. Nel caso di PaaS e IaaS, vi è la possibilità di creare lavoro inedito nel cloud (nuove applicazioni, software, ecc.). Come con tutta la proprietà intellettuale, se non protetto da appropriate clausole contrattuali (cfr. allegato I - Cloud computing - Principali questioni giuridiche, Proprietà intellettuale), questo lavoro inedito potrebbe essere a rischio.

RISCHI NON SPECIFICI DEL CLOUD

Nel corso della nostra analisi del rischio abbiamo identificato le seguenti minacce che non sono specifiche del cloud computing, ma dovrebbero essere comunque considerate attentamente quando si stia valutando il rischio di un tipico sistema basato sul cloud.

R.25 Interruzioni di rete

Probabilità	BASSA	Comparativo: Uguale
Impatto	MOLTO ALTO	Comparativo: Più alto
Vulnerabilità	V38. Mal configurazione V39. Vulnerabilità del sistema o del sistema operativo V6. Carenza di isolamento delle risorse V41. Mancanza, o inadeguati o non verificati, piani di business continuity e di disaster recovery	
Assets interessati	A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio	
Rischio	**MEDIO**	

Uno dei rischi a più elevato impatto! Potenzialmente migliaia di clienti allo stesso tempo potrebbero essere interessati.

R.26 Gestione della rete (ad esempio, congestione / mala connessione / utilizzo non ottimale della rete)

Probabilità	MEDIA	Comparativo: Uguale
Impatto	MOLTO ALTO	Comparativo: Più alto
Vulnerabilità	V38. Mal configurazione V39. Vulnerabilità di sistema o di sistema operativo V6. Carenza di isolamento delle risorse V41. Mancanza, o inadeguati o non verificati, piani di business continuity e di disaster recovery	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A3. Lealtà ed esperienza dei dipendenti A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio A16 Rete (connessioni, ecc.)	
Rischio	**ELEVATO**	

R.27 Modifica del traffico di rete

Probabilità	BASSA
Impatto	ALTO
Vulnerabilità	V2. Vulnerabilità nella creazione degli utenti V3. Vulnerabilità della revoca degli utenti V8. Vulnerabilità della crittografia delle comunicazioni V16. Nessun controllo sul processo di valutazione delle vulnerabilità
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali – critici A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio
Rischio	**MEDIO**

R.28 Aumento dei privilegi

Probabilità	BASSA	Comparativo: Più bassa
Impatto	ALTO	Comparativo: Più alto (per il fornitore cloud)
Vulnerabilità	V1. Vulnerabilità AAA V2. Vulnerabilità nella creazione degli utenti V3. Vulnerabilità della revoca degli utenti V5. Vulnerabilità dell'hypervisor V34. Ruoli e responsabilità non chiari V35. Scarsa imposizione della definizione dei ruoli V36. Principio del *need-to-know* non applicato V38. Mal configurazione	
Assets interessati	A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle Risorse Umane (HR) A11. Controllo accessi / Autenticazione / Autorizzazione (root/admin rispetto ad altri) A13. Directory degli utenti (dati)	
Rischio	**MEDIO**	

R.29 Attacchi di ingegneria sociale (ad esempio, impersonificazione)

Probabilità	MEDIA	Comparativo: Uguale
Impatto	ALTO	Comparativo: Più alto
Vulnerabilità	V2. Vulnerabilità nella creazione degli utenti V6. Mancanza di isolamento delle risorse V8. Vulnerabilità della crittografia delle comunicazioni V32. Mancanza di consapevolezza sulla sicurezza V37. Procedure per la sicurezza fisica non adeguate	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A3. Lealtà ed esperienza dei dipendenti A4. Proprietà Intellettuale A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle Risorse Umane (HR) A11. Controllo accessi / Autenticazione / Autorizzazione (root/admin rispetto ad altri) A12. Credenziali	
Rischio	**MEDIO**	

R.30 Perdita o compromissione di log operazionali

Probabilità	BASSA	Comparativo: Più bassa
Impatto	MEDIO	Comparativo: Uguale (per il cliente)
Vulnerabilità	V1. Vulnerabilità AAA V2. Vulnerabilità nella creazione degli utenti V3. Vulnerabilità della revoca degli utenti V19. Mancanza di predisposizione per l'analisi forense V39. Vulnerabilità di sistema o del sistema operativo V52. Mancanza di politiche, o procedure scadenti, per la raccolta e conservazione dei log	
Assets interessati	A21. Log operazionali (Cliente e fornitore cloud)	
Rischio	**MEDIO**	

R.31 Perdita o compromissione di log di sicurezza (manipolazione di investigazioni forensi)

Probabilità	BASSA	Comparativo: Più bassa
Impatto	MEDIO	Comparativo: Uguale (per il cliente)
Vulnerabilità	V1. Vulnerabilità AAA V2. Vulnerabilità nella creazione degli utenti V3. Vulnerabilità della revoca degli utenti V19. Mancanza di predisposizione per l'analisi forense V39. Vulnerabilità di sistema o del sistema operativo V52. Mancanza di politiche, o procedure scadenti, per la raccolta e conservazione dei log	
Assets interessati	A22. Log di sicurezza	
Rischio	**MEDIO**	

R.32 Furto, perdita dei backup

Probabilità	BASSA	Comparativo: Più bassa
Impatto	ALTO	Comparativo: Uguale (per il cliente)
Vulnerabilità	V1. Vulnerabilità AAA V2. Vulnerabilità nella creazione degli utenti V3. Vulnerabilità della revoca degli utenti V37. Procedure per la sicurezza fisica non adeguate	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle Risorse Umane (HR) A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio A23. Dati di backup o archivio	
Rischio	**MEDIO**	

R.33 Accesso non autorizzato ai locali tecnici (incluso l'accesso fisico ai macchinari e ad altri locali/servizi tecnici)

Probabilità	MOLTO BASSA	Comparativo: Più basso
Impatto	ALTO (un impatto molto elevato si ha con attacco mirato (che punta a una specifica macchina, ecc.), se no l'impatto è alto)	Comparativo: Più alto
Vulnerabilità	V37. Procedure per la sicurezza fisica non adeguate	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle risorse umane (HR) A23. Dati di archivio o backup	
Rischio	**MEDIO**	

R.34 Furto di attrezzatura di calcolo

Probabilità	MOLTO BASSA	Comparativo: Più basso
Impatto	ALTO	Comparativo: Più alto
Vulnerabilità	V37. Procedure per la sicurezza fisica non adeguate	
Assets interessati	A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle risorse umane (HR) A17. Hardware fisico	
Rischio	**MEDIO**	

R.35 Disastri naturali

Probabilità	MOLTO BASSA	Comparativo: Più alto
Impatto	ALTO	Comparative: Più alto
Vulnerabilità	V41. Mancanza, o inadeguati o non verificati, piani di business continuity e di disaster recovery	
Assets interessati	A1. Reputazione aziendale A2. Fiducia della clientela A5. Dati personali sensibili A6. Dati personali A7. Dati personali - critici A8. Dati dalle risorse umane (HR) A9. Erogazione del servizio – servizi in tempo reale A10. Erogazione del servizio A23. Dati di archivio o backup	
Rischio	**MEDIO**	

In termini generali, il rischio da disastro naturale è più basso rispetto a infrastrutture tradizionali perché i fornitori cloud offrono di base siti e percorsi di rete multipli ridondati.

4. VULNERABILITÀ

La seguente lista di vulnerabilità non è esaustiva ma è, tuttavia, sufficientemente dettagliata per gli scopi della nostra analisi. Essa contiene vulnerabilità sia specifiche del cloud sia generali della sicurezza delle informazioni.

V1. Vulnerabilità AAA

Un sistema per l'autenticazione, l'autorizzazione e il tracciamento carente potrebbe facilitare l'accesso non autorizzato alle risorse, all'escalation dei privilegi, all'impossibilità di tracciare l'abuso delle risorse e, più in generale, gli incidenti di sicurezza, ecc. attraverso:

- Conservazione non sicura da parte del cliente delle credenziali di accesso al cloud;
- Insufficiente disponibilità di ruoli;
- Credenziali conservate su una macchina di transizione.

Inoltre, il cloud rende molto più importante l'impatto degli attacchi all'autenticazione basata su password (tendenza a realizzare frodi utilizzando un Trojan per trafugare le password aziendali) dal momento che ora le applicazioni aziendali sono esposte su Internet. Perciò le autenticazioni basate su password diverranno insufficienti, e diventerà necessaria un'autenticazione più forte o a due fattori per accedere alle risorse del cloud.

V2. Vulnerabilità nella creazione degli utenti

- Il cliente non può controllare il processo di gestione.
- L'identità del cliente non è adeguatamente verificata al momento della registrazione.
- Possono verificarsi ritardi nella sincronizzazione tra componenti del sistema cloud (temporali e di contenuto del profilo).
- Creazione di copie multiple e non sincronizzate delle identità.
- Le credenziali sono vulnerabili all'intercettazione e al riutilizzo.

V3. Vulnerabilità della revoca degli utenti

Le credenziali revocate sono ancora valide a causa di ritardi temporali nella distribuzione della revoca.

V4. Accesso remoto all'interfaccia di amministrazione

In teoria, questo consente a vulnerabilità presenti in macchine terminali di compromettere l'infrastruttura cloud (singolo cliente o CP) attraverso, ad esempio, l'autenticazione debole di risposte e richieste.

V5. Vulnerabilità dell'hypervisor

Gli attacchi a livello di hypervisor sono estremamente allettanti: l'hypervisor infatti controlla completamente le risorse fisiche e le VM che girano sopra di esso, e così qualsiasi vulnerabilità in questo strato è estremamente critica. Sfruttare l'hypervisor significa potenzialmente forzare ogni VM. La prima dimostrazione di realizzabilità di un attacco dal livello inferiore contro un hypervisor è stata pubblicata da King e colleghi nel documento (21), in cui gli autori introducono il concetto di un Rootkit basato su macchine virtuali. Da quel momento sono state identificate a oggi poche vulnerabilità negli hypervisor più diffusi (ad esempio, (22) e (23)) che possono essere sfruttate senza privilegi amministrativi di accesso, ma nessuno dei loro risultati è stato dis-aggiornato (un-patched) al momento della stesura del documento.

Un tipico scenario abilitato dallo sfruttamento di una vulnerabilità dell'hypervisor è la cosiddetta 'evasione dall'ospite all'host', di cui un esempio è 'Cloudburst', una vulnerabilità di VMware scoperta recentemente e documentata nel riferimento (24). Un altro scenario è il 'VM hopping', in cui un attaccante forza una VM utilizzando alcuni metodi standard e quindi – sfruttando alcune vulnerabilità dell'hypervisor – prende il controllo delle altre VM in esecuzione sullo stesso hypervisor. Per ulteriori informazioni, fare riferimento a *Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments* (vedi (25)).

V6. Mancanza di isolamento delle risorse

L'utilizzo delle risorse da parte di un cliente può avere effetti sull'utilizzo delle risorse da parte di un altro cliente.

Le infrastrutture di cloud computing di tipo IaaS fanno principalmente riferimento su progetti architetturali in cui le risorse fisiche sono condivise tra più macchine virtuali e perciò tra più clienti.

Le vulnerabilità nel modello di sicurezza dell'hypervisor possono portare all'accesso non autorizzato a tali risorse condivise. Per esempio, le macchine virtuali del Cliente 1 e del Cliente 2 hanno i propri dischi fissi virtuali salvati nella medesima LUN condivisa (Logic Unit Number) all'interno di una SAN. Il Cliente 2 può riuscire a mappare il dico fisso virtuale del Cliente 1 sulla propria macchina virtuale ed accedere ed utilizzare i dati al suo interno.

Gli hypervisor utilizzati nei cloud IaaS offrono ricche API che il cloud provider utilizza per implementare un'interfaccia di gestione, di allocazione e di reporting proprietaria che viene esposta verso i propri clienti. Le vulnerabilità nel modello di sicurezza dell'hypervisor o nelle 'interfacce di amministrazione' possono portare ad accessi non autorizzati alle informazioni del cliente. Allo stesso tempo una vulnerabilità a questo livello può consentire ad un attaccante di manipolare gli asset all'interno della struttura del cloud, provocando inaccessibilità dei servizi (come ad esempio effettuando lo shutdown delle macchine virtuali), fughe di dati (ad esempio, la copia ed il trasferimento di dati delle macchine virtuali fuori dal cloud), la compromissione di dati (ad esempio, sostituendo le macchine virtuali con copie modificate), o danni finanziari diretti (ad esempio, replicando e lanciando molte copie delle macchine virtuali).

In un articolo, Craig Gentry stima che eseguendo una ricerca con parole chiave cifrate – una semplice e perfettamente ragionevole applicazione di questo algoritmo – aumenterebbe il tempo di calcolo di circa un trilione (28). Ciò significa che per ancora gran tempo a venire, I clienti cloud che non fanno altro che immagazzinare I propri dati nel cloud dovranno fidarsi del fornitore cloud.

Inoltre, la mancanza di controlli sulla cartografia cloud e sulla co-residenza

e sulle vulnerabilità di tipo cross side channel (vedi (26)) possono creare seri rischi all'isolamento delle risorse. Per esempio, se l'utilizzo delle risorse non è indipendente tra il Cliente 1 ed il Cliente 2, il Cliente 1 può mapparsi le risorse del Cliente 2. Ciò può essere fatto, per esempio, utilizzando il caricamento controllato delle risorse del Cliente 2 mentre si misurano i cambiamenti negli schemi di disponibilità delle risorse propri del Cliente 1.

Infine, la mancanza di strumenti per imporre una condizione di servizio (ToS) o un livello di servizio (SLA) più specifico, come prodotti per la qualità del servizio (QoS) o per la schedulazione di risorse distribuite (DRS), possono consentire ad un cliente di monopolizzare l'utilizzo del complesso del cloud, con un impatto sugli altri clienti di indisponibilità del servizio o con scarse prestazioni.

V7. Mancanza di isolamento reputazionale

Le attività effettuate da un cliente hanno un impatto sulla reputazione di un altro cliente.

V8. Vulnerabilità della crittografia delle comunicazioni

Queste vulnerabilità riguardano la possibilità di leggere i dati in transito per mezzo, ad esempio, di attacchi MITM, autenticazione debole, accettazione di certificati auto-firmati, ecc.

V9. Mancanza o debolezza della crittografia degli archivi e dei dati in transito

La mancata crittografia di dati in transito, di dati conservati in archivi e database, di immagini non montate di macchine virtuali, di immagini e dati forensi, di log sensibili e di altri dati a riposo, mette a rischio i dati. Naturalmente il costo per l'implementazione della gestione delle chiavi [V11] e i costi di elaborazione devono essere tenuti in conto e confrontati con il rischio di business introdotto.

V10. Impossibilità di elaborare i dati in forma criptata

Criptare i dati a riposo non è difficile, ma nonostante i recenti progressi nella crittografia omomorfica (27), ci sono scarse prospettive che qualsiasi sistema commerciale sia in grado di sostenere questo tipo di crittografia durante l'elaborazione. In un articolo, Bruce Schneier stima che effettuare una ricerca sul web con parole chiave criptate – una semplice applicazione perfettamente plausibile di questo algoritmo – aumenterebbe la quantità di tempo di elaborazione di circa mille miliardi di volte (28). Ciò significa che ancora per molto tempo a venire, i clienti del cloud che fanno qualsiasi attività oltre alla semplice memorizzazione di dati nel cloud devono fidarsi del cloud provider.

V11. Procedure scadenti di gestione delle chiavi

Le infrastrutture di cloud computing richiedono la gestione e la memorizzazione di molti diversi tipi di chiavi; esempi includono le chiavi di sessione per proteggere i dati in transito (come le chiavi SSL), chiavi per la criptazione dei file, le coppie di chiavi che identificano il cloud provider, le coppie di chiavi che identificano i clienti, i token di autorizzazione ed i certificati di revoca (29). Per il fatto che le macchine virtuali non hanno un'infrastruttura hardware fissa ed i contenuti basati su cloud tendono ad essere geograficamente distribuiti, è molto più difficile applicare controlli standard, quali supporti di archiviazione con moduli di sicurezza hardware (HSM), alle chiavi sulle infrastrutture cloud. Ad esempio:

- Gli HSM sono per necessità altamente protetti dal punto di vista fisico (dal furto, intercettazione e forzatura). Ciò rende molto difficoltoso distribuirli nelle diverse località utilizzate nelle architetture cloud (per esempio, geograficamente distribuite e altamente replicate). Gli standard per la gestione delle chiavi come il PKCS#10 e gli standard associati come il PKCS@11 (30) non forniscono adattamenti standard per interfacciarsi con sistemi distribuiti.(30)
- Le interfacce per la gestione delle chiavi che sono pubblicamente accessibili attraverso Internet (anche se non direttamente) sono più vulnerabili, in quanto si riduce la sicurezza nel canale di comunicazione tra il cliente e lo

storage delle chiavi del cloud, e nel meccanismo di mutua autenticazione remota.

- Le nuove macchine virtuali che hanno la necessità di autenticarsi devono essere rappresentate con qualche forma di segretezza. La distribuzione di tali segreti può presentare forme di scalabilità. La rapida scalata delle certification authority che rilasciano le coppie di chiavi si realizza facilmente se le risorse sono note a priori, ma la scalata dinamica e non pianificata di autorità gerarchiche di trust è difficile da realizzare a causa del sovraccarico delle risorse nella creazione di nuove autorità (di registrazione o di certificazione, nell'autenticazione di nuovi componenti e nella distribuzione di nuove credenziali, ecc.)
- La revoca delle chiavi in un'architettura distribuita è anch'essa un'attività costosa. Una revoca efficace implica che le applicazioni verifichino lo stato della chiave (normalmente del certificato) in accordo a limiti temporali noti che determinano la finestra di rischio. Sebbene esistano meccanismi distribuiti per ottenere questo (si veda, ad esempio, (31) e (32)) l'assicurare che parti differenti del cloud ricevano un livello di servizio equivalente, così da non essere associate a diversi livelli di rischio, rimane una sfida. Soluzioni centralizzate come OCSP sono costose e non riducono necessariamente il rischio a meno che la CA e la CRL non siano strettamente legate.

V12. Generazione delle chiavi: bassa entropia per la generazione di numeri casuali

La combinazione di immagini standard di sistema, di tecnologie di virtualizzazione e della mancanza di dispositivi di input significa che i sistemi hanno molta meno entropia degli RNG fisici; si veda *Cloud Computing Security* (33). Ciò significa che un attaccante su una macchina virtuale può riuscire a indovinare le chiavi crittografiche generate su altre macchine virtuali perché le fonti di entropia utilizzate per generare i numeri casuali possono essere simili. Questo non è un problema difficile da risolvere, ma se non è tenuto in conto durante la progettazione del sistema, può avere importanti conseguenze.

V13. Mancanza di soluzioni e tecnologie standard

Una mancanza di standard implica che i dati possano essere 'legati' a un provider. Questo è un grave rischio nel caso in cui il provider dovesse cessare di operare.

Ciò può inibire l'utilizzo di servizi di gestione della sicurezza e di tecnologie di sicurezza esterne quali FIM.

V14. Mancanza di accordi di deposito dei sorgenti presso terzi

La mancanza di deposito dei sorgenti presso terzi implica che se un provider di tipo PaaS o SaaS fallisce, i suoi clienti non sono protetti.

V15. Modellizzazione inaccurata dell'utilizzo delle risorse

I servizi cloud sono particolarmente vulnerabili all'esaurimento delle risorse poiché queste sono assegnate statisticamente. Sebbene molti provider consentano ai clienti di riservare le risorse in anticipo, gli algoritmi di allocazione delle risorse possono fallire a causa di:

- una modellazione non accurata dell'utilizzo delle risorse, che può portare all'overbooking o alla sovra-allocazione (che portano allo spreco di risorse da parte del cloud provider). Ben noti algoritmi di allocazione delle risorse sono il Token Buket (34), il Fair Queuing (35) e il Class Based Queuing (36). Essi sono vulnerabili a distorsioni di equità; per un esempio, si veda (37).
- un fallimento degli algoritmi di allocazione delle risorse a causa di eventi straordinari (come ad esempio, fatti di cronaca estera per la distribuzione dei contenuti).
- un fallimento degli algoritmi di

Sebbene molti fornitori consentano ai clienti di prenotare in anticipo le risorse, gli algoritmi di assegnazione delle stesse possono fallire per imprecisa modellizzazione dell'utilizzo, che può portare a overbooking o over-provisioning (con conseguente spreco di risorse da parte del fornitore di cloud).

allocazione delle risorse che utilizzano una classificazione a job o a pacchetto in quanto le risorse sono mal classificate.

- fallimenti nell'allocazione generale delle risorse (in contrapposizione a sovraccarichi temporanei).

V16. Nessun controllo sul processo di valutazione delle vulnerabilità

Le restrizioni sulla scansione delle porte e sul test delle vulnerabilità sono un'importante vulnerabilità che, combinata con condizioni d'uso (ToU) che scaricano sul cliente la responsabilità per rendere sicuri gli elementi dell'infrastruttura, sono un serio problema di sicurezza.

V17. Possibilità di esplorazione della rete interna (del cloud)

I clienti del cloud possono effettuare scansioni delle porte ed altri test su sistemi di altri clienti all'interno della rete.

V18. Possibilità che vengano effettuati dei controlli di co-residenza

Attacchi di tipo side-channel, che sfruttano una mancanza di isolamento delle risorse, consentono agli attaccanti di determinare quali risorse siano condivise tra quali clienti.

V19. Mancanza di predisposizione per le attività forensi

Mentre il cloud ha il potenziale per migliorare la predisposizione per l'analisi forense, molti provider non rendono disponibili servizi e condizioni d'uso appropriate per consentirlo. Per esempio, i fornitori SaaS tipicamente non danno accesso ai log degli IP dei clienti che fanno accesso ai contenuti. I provider IaaS possono non rendere disponibili servizi forensi come le immagini recenti di VM e dischi.

V20. Sanitizzazione dei supporti sensibili

L'affitto condiviso dello storage fisico comporta che i dati sensibili possano essere diffusi in quanto le policy per la distruzione dei dati, applicabili al termine del

ciclo di vita, possono essere impossibili da implementare o perché, per esempio, i supporti non possono essere fisicamente distrutti in quanto un disco è ancora utilizzato da un altro affittuario o perché non può essere localizzato, oppure perché non esistono procedure a riguardo.

V21. Sincronizzazione delle responsabilità ed obblighi contrattuali esterni al cloud

I clienti del cloud sono spesso inconsapevoli delle responsabilità che gli vengono attribuite con le condizioni di servizio. Esiste una tendenza verso l'errata attribuzione di responsabilità al cloud provider per attività come la criptazione degli archivi anche quando è chiaramente stabilito nei termini contrattuali tra le due parti che non verrà assunta alcuna responsabilità di questo tipo.

V22. Applicazioni cross-cloud che creano dipendenze nascoste

Esistono delle dipendenze nascoste nella catena di fornitura dei servizi (dipendenze intra- ed extra-cloud) e l'architettura del cloud provider che non supporta operazioni continuative dal cloud quando le terze parti coinvolte, i subfornitori o la società cliente, sono state separate dal fornitore del servizio e viceversa.

V23. Clausole negli SLA con promesse in conflitto tra differenti portatori di interesse

Alcune clausole sugli SLA possono essere in conflitto con promesse fatte in altre clausole o da clausole da altri fornitori.

V24. Clausole degli SLA che contengono rischi eccessivi per l'operatività

Gli SLA possono portare con sé troppi rischi per l'operatività di un fornitore, dato l'attuale rischio di problemi tecnici. Dal punto di vista del cliente, gli SLA possono contenere clausole che risultano essere deleterie – ad esempio, nell'area della proprietà intellettuale, uno SLA può specificare che il fornitore cloud si riserva i diritti su ogni contenuto memorizzato nell'infrastruttura cloud.

V25. Controlli o certificazioni non resi disponibili ai clienti

Il fornitore cloud non può fornire alcuna assicurazione al cliente mediante controlli di certificazione.

Ad esempio, alcuni fornitori cloud stanno utilizzando hypervisor open source o loro versioni personalizzate (ad esempio, XEN (38)) che non hanno conseguito alcuna certificazione Common Criteria (39), che è un requisito fondamentale per alcune organizzazioni (ad esempio, le agenzie governative statunitensi).

Si prega di notare che non stiamo dicendo che vi sia una correlazione diretta tra la certificazione e il livello di vulnerabilità (dal momento che non disponiamo di sufficienti informazioni riguardo al profilo di protezione e degli obiettivi di sicurezza dei prodotti certificati).

V26. Schemi di certificazione non adattati alle infrastrutture cloud

Non vi è alcun controllo specifico del cloud, il che significa che quelle vulnerabilità di sicurezza verranno probabilmente omesse.

V27. Inadeguatezza dell'erogazione delle risorse e degli investimenti in infrastrutture

Gli investimenti in infrastrutture richiedono tempo. Se il modello previsionale fallisce, il cloud provider può essere inadempiente per un lungo periodo.

V28. Mancanza di politiche che fissino l'utilizzo massimo delle risorse

Se non c'è un modo flessibile e configurabile per il cliente e/o per il cloud provider di impostare dei limiti alle risorse, questo può diventare problematico quando l'utilizzo delle risorse diventa imprevedibile.

V29. Memorizzazione dei dati in giurisdizioni multiple e relativa mancanza di trasparenza

Il mirroring dei dati per la distribuzione mediante reti periferiche e storage ridondante senza che al cliente sia data la disponibilità di informazioni in tempo

reale di dove i dati siano effettivamente memorizzati introduce un livello di vulnerabilità. Le società possono trovarsi a violare inconsapevolmente le norme, specialmente se non vengono fornite informazioni chiare sulla giurisdizione applicabile allo storage.

V30. Mancanza di informazioni sulle giurisdizioni

I dati possono essere memorizzati e/o conservati in giurisdizioni ad alto rischio ove essi sono vulnerabili alla confisca attraverso mandati d'accesso coatti. Se quest'informazione non è disponibile per i clienti del cloud, essi non possono intraprendere passi per evitarlo.

V31. Mancanza di completezza e trasparenza nelle condizioni di utilizzo

VULNERABILITA' NON SPECIFICHE DEL CLOUD

Nel corso della nostra analisi dei rischi abbiamo identificato le seguenti vulnerabilità che non sono specifiche del cloud computing ma che dovrebbero essere, nondimeno, attentamente considerate quando si verifica un tipico sistema basato su cloud.

V32. Mancanza di consapevolezza sulla sicurezza

I clienti del cloud non sono consapevoli dei rischi che potrebbero trovarsi ad affrontare con la migrazione verso il cloud, e particolarmente quei rischi che sono generati da minacce specifiche per il cloud, come ad esempio la perdita di controllo, la dipendenza dal fornitore, l'esaurimento delle risorse del CP, ecc. Questa mancanza di consapevolezza potrebbe ripercuotersi anche sul cloud provider che potrebbe non rendersi conto delle azioni che devono essere intraprese per mitigare tali rischi.

V33. Mancanza di processi di controllo

Dal momento che possono esistere dei ruoli ad elevato privilegio all'interno dei cloud provider, per via degli interventi sui ruoli coinvolti, la mancanza o l'inadeguatezza dei controlli dei profili di rischio dello staff con tali ruoli è un'importante vulnerabilità.

V34. Ruoli e responsabilità non chiari

Queste vulnerabilità riguardano l'attribuzione non adeguata di ruoli e responsabilità nell'organizzazione del cloud provider.

V35. Carente implementazione delle definizioni dei ruoli

All'interno del cloud provider, un difetto nella separazione dei ruoli può portare a ruoli eccessivamente privilegiati che possono rendere vulnerabili sistemi estremamente grandi. Ad esempio, a nessuna persona dovrebbero essere concessi privilegi di accesso all'intero cloud.

V36. Mancata applicazione del principio del need-to-know

Questo è un caso speciale di una vulnerabilità che riguarda ruoli e responsabilità. Alle parti non dovrebbe essere concesso un accesso non necessario ai dati. Se ciò accade, questo può costituire un rischio non necessario.

V37. Procedure per la sicurezza fisica inadeguate

Queste possono includere:

- mancanza di controlli sui perimetri fisici (autenticazione mediante smart card all'ingresso);
- mancanza di schermatura elettromagnetica per asset critici vulnerabili all'intercettazione.

V38. Configurazione errata

Questa classe di vulnerabilità include: applicazione non adeguata delle procedure delle linee di base e delle procedure di consolidamento della sicurezza, errori umani e amministratori non istruiti.

V39. Vulnerabilità di sistema o di sistema operativo

V40. Software non affidabile

V41. Assenza, o inadeguatezza, o mancanza di verifica dei piani di business continuity e disaster recovery

V42. Mancanza, o incompletezza o inaccuratezza dell'inventario dei beni

V43. Mancanza, o inadeguata, o scarsa classificazione degli asset

V44. Proprietà del bene non chiara

V45. Scadente identificazione dei requisiti di progetto

Questo include la mancata considerazione dei requisiti di sicurezza e di conformità legale, l'assenza del coinvolgimento degli utenti dei sistemi e delle applicazioni, requisiti di business non chiari o non adeguati, ecc..

V46. Scarsa selezione dei fornitori

V47. Mancanza di ridondanza dei fornitori

V48. Vulnerabilità delle applicazioni o inaccurata gestione degli aggiornamenti

Questa classe di vulnerabilità include: errori nel codice applicativo, procedure di aggiornamento in conflitto tra fornitore e cliente, applicazione di correzioni non testate, vulnerabilità dei browser, ecc.

V49. Vulnerabilità legate al consumo di risorse

V50. Violazione degli accordi di riservatezza da parte del fornitore

V51. Responsabilità per la perdita di dati (fornitore cloud)

V52. Mancanza di politiche, o procedure scadenti, per la raccolta e conservazione dei log

V53. Risorse di filtraggio inadeguate o mal configurate

5. ASSETS (Risorse)

Asset	Descrizione o riferimento agli elementi sopra descritti	Possessore [attori o organizzazioni interessati]	Valore Percepito [Scala: MOLTO BASSO – BASSO – MEDIO – ALTO – MOLTO ALTO]
A1. Reputazione Aziendale		Cliente Cloud	**MOLTO ALTO**
A2. Fiducia della clientela	Include l'avviamento, può essere misurato dalle lamentele	Cliente Cloud	**MOLTO ALTO**
A3. Lealtà ed esperienza dei dipendenti		Cliente Cloud	**ALTO**
A4. Proprietà intellettuale		Cliente Cloud	**ALTO**
A5. Dati personali sensibili	(come definito nella European Data Protection Directive)	Cloud Provider / Cliente Cloud	**MOLTO ALTO** (Poichè include dati sugli utilizzatori di sistemi di assistenza domiciliare)
A6. Dati personali	(come definito nella European Data Protection Directive)	Cloud Provider / Cliente Cloud	**MEDIO** (valore operativo) / **ALTO** (valore se perduto)
A7. Dati personali critici	(tutti i dati inclusi nella categoria dei dati personali, secondo la European Data Protection Directive, e che sono classificati o considerati CRITICI per l'organizzazione o l'azienda	Cloud Provider / Cliente Cloud	**ALTO** (valore operativo) / **ALTO** (valore se perduto)
A8. Dati dalle Risorse Umane (HR)	Dati che sono rilevanti da una prospettiva operativa, accanto ai requisiti di Protezione dei Dati	Cliente Cloud	**ALTO**
A9. Erogazione del servizio – servizi In tempo reale	Tutti quei servizi per cui il fattore tempo è critico e che richiedono un livello di disponibilità prossimo al 100%	Cloud Provider / Cliente Cloud	**MOLTO ALTO**

Asset	Descrizione o riferimento agli elementi sopra descritti	Possessore [attori o organizzazioni interessati]	Valore Percepito [Scala: MOLTO BASSO – BASSO – MEDIO – ALTO – MOLTO ALTO]
A10. Erogazione del servizio		Cloud Provider / Cliente Cloud	**MEDIO**
A11. Access control/ authentication/ authorization (root/admin rispetto ad altri)		Cloud Provider / Cliente Cloud	**ALTO**
A12. Credenziali	Di pazienti e personale che accede al sistema	Cliente Cloud	**MOLTO ALTO**
A13. User directory (data)	Se non funziona, nessuno può accedere	Cliente Cloud	**ALTO**
A14. Interfaccia di gestione dei servizi Cloud	E' l'interfaccia di gestione (basata su web o su shell remota, o…) che gestisce tutti i servizi forniti attraverso il cloud.	Cloud Provider / Cliente Cloud	**MOLTO ALTO**
A15. API dell'interfaccia di gestione		Cloud Provider / Cliente Cloud / EuropeanHealth	**MEDIO**
A16. Rete (connessioni, ecc.)	Include le connessioni intra ed extra cloud	Cloud Provider / Cliente Cloud	**ALTO**
A17. Hardware fisico		Cloud Provider / Cliente Cloud	**BASSO** (dipende da quanto se ne perde) / **MEDIO** (potrebbe essere serio se rubato e non protetto)
A18. Edifici		Cloud Provider / Cliente Cloud	**ALTO**
A19. Applicazioni del fornitore cloud (codice sorgente)		Cloud Provider / Cliente Cloud	**ALTO**
A20. Certificazione	ISO, PCI DSS, ecc.	Cloud Provider / Cliente Cloud	**ALTO**
A21. Log operativi (del cliente e del fornitore cloud)	Quei log utilizzati per supportare e ottimizzare i processi di business e per fini di audit	Cloud Provider / Cliente Cloud	**MEDIO**
A22. Log di sicurezza	Utili come evidenze di brecce nella sicurezza e per analisi forense	Cloud Provider / Cliente Cloud	**MEDIO**
A23. Backup o archivi di dati		Cloud Provider / Cliente Cloud	**MEDIO**

6. RACCOMANDAZIONI E MESSAGGI CHIAVE

Questa sezione comprende l'insieme delle principali raccomandazioni e i messaggi chiave:

- Information Assurance Framework – una lista di controllo standard che può essere utilizzata (dai clienti cloud) per ottenere, e (dai fornitori cloud) per fornire, garanzie
- Raccomandazioni di natura legale
- Raccomandazioni per la ricerca.

Quadro della Sicurezza delle informazioni

Introduzione

Una delle più importanti raccomandazioni di questo documento è l'insieme di criteri di garanzia pensato per:

Questa sezione delle raccomandazioni fornisce un insieme di domande che le organizzazioni possono porre ai fornitori cloud per assicurarsi che questi stiano proteggendo in modo adeguato le informazioni loro affidate.

- valutare il rischio connesso all'adozione di servizi cloud (comparando i rischi del mantenere una situazione organizzativa e architetturale 'classica' con quelli della migrazione ad un ambiente cloud).
- confrontare le offerte di differenti fornitori di servizi cloud.
- ottenere garanzie dai fornitori cloud selezionati. La preparazione di questionari per valutare la sicurezza di terze parti fornitrici di servizi costituisce un significativo impegno di risorse per i clienti cloud ed è difficile da realizzare se non si possiede esperienza delle specifiche architetture cloud.
- ridurre il peso delle garanzie sui fornitori cloud. Un rischio molto importante specifico delle infrastrutture cloud è introdotto dai requisiti NIS. Molti fornitori cloud stanno sperimentando come un gran numero di clienti richiedano loro audit delle infrastrutture e delle politiche che essi

adottano. Ciò può accrescere in modo critico il carico di lavoro sul personale che si occupa di sicurezza e accrescere il numero di persone che hanno accesso all'infrastruttura, con un significativo aumento del rischio di attacco dovuto a mal utilizzo di informazioni critiche per la sicurezza, furto di dati sensibili, ecc. I fornitori cloud potranno far fronte a questa tendenza grazie ad un chiaro framework per la gestione di questo tipo di richieste.

Questa sezione delle raccomandazioni fornisce un insieme di domande che un'organizzazione può porre ai fornitori per assicurarsi che essi pongano in atto le misure sufficienti a proteggere le informazioni a loro affidate.

Queste domande intendono costituire una base minima. Ciascuna organizzazione potrebbe perciò avere richieste aggiuntive specifiche, non coperte da questa base minima.

Allo stesso modo, questo documento non fornisce al cloud provider un formato di risposta standard, perciò le risposte sono in formato testo libero. Tuttavia è destinato ad alimentare le domande in un più dettagliato quadro globale che sarà sviluppato come seguito di questo lavoro; ciò consentirà di avere una serie di risposte consistenti, comparabili. Tali risposte forniranno una metrica quantificabile per valutare la maturità della sicurezza delle informazioni del provider.

Resta inteso che la metrica di cui sopra sia consistente tra fornitori, così da rendere possibile alle organizzazioni utenti finali una comparazione (delle offerte).

Suddivisione delle responsabilità

La seguente tabella mostra la suddivisione delle responsabilità attesa tra cliente e fornitore.

	Cliente	**Fornitore**
Legittimità del contenuto	Intera responsabilità	Responsabilità di intermediario, con deroghe secondo i termini della direttiva sull'E-commerce[1] e sue interpretazioni.
Incidenti di sicurezza (comprese le perdite di dati, l'uso di account per lanciare un attacco)	Responsabilità secondo dovuta diligenza per ciò che è sotto il suo controllo, in accordo con le condizioni contrattuali	Responsabilità secondo dovuta diligenza per ciò che è sotto il suo controllo
Stato della Legge Europea sulla protezione dei dati	Titolare del trattamento	Titolare (esterno) del trattamento

Ripartizione delle competenze

Rispetto agli incidenti di sicurezza, è necessaria una chiara definizione e comprensione dei ruoli e responsabilità rilevanti, tra il cliente ed il fornitore.

Per quanto attiene agli incidenti di sicurezza, tra il cliente e il fornitore ci deve essere, una chiara definizione e comprensione dei ruoli e delle responsabilità rilevanti per la sicurezza. La linea di demarcazione può variare notevolmente tra le offerte SaaS e le offerte IaaS, con quest'ultime che delegano maggiori responsabilità al cliente. Una tipica e razionale divisione di responsabilità è mostrata nella seguente tabella. *In ogni caso, per ogni tipo di servizio, il cliente e il fornitore devono definire chiaramente chi di loro è responsabile per tutti gli elementi qui di seguito elencati.* Nel caso di condizioni standard di servizio (vale a dire, nessuna trattativa possibile), i clienti del cloud dovrebbero verificare ciò che compete loro.

[1] Cfr. definizione di servizi per la società dell'informazione come da Art. 2 della Direttiva 98/48/EC e da Art. 2 della Direttiva 2000/31/EC, in congiunzione con le deroghe contenute negli Articoli 12-15 della Direttiva 2000/31/EC (Direttiva sull'e-Commerce).

Software As A Service

Cliente	Fornitore
• Conformità alla normativa sulla protezione dei dati per quanto riguarda i dati dei clienti raccolti e trattati • Manutenzione del sistema di gestione delle identità • Gestione del sistema di gestione delle identità • Gestione degli aggiornamenti dell'OS e procedure di hardening (verificare anche ogni conflitto tra procedure di hardening dei clienti) • Gestione della piattaforma di autenticazione (incluse l'applicazione delle politiche relative alle password) e le politiche di sicurezza del fornitore • Configurazione di sicurezza della piattaforma (regole del firewall, configurazione dell'IDS/IPS, ecc.) • Monitoraggio dei sistemi	• Infrastruttura fisica di supporto (impianti, spazio a rack, alimentazione, raffreddamento, cablaggi, ecc.) • Sicurezza e disponibilità dell'infrastruttura fisica (server, storage, ampiezza di banda, ecc.) • Manutenzione della sicurezza della piattaforma (Firewall, Host IDS/IPS, antivirus, packet filtering) • Raccolta dei log e monitoraggio della sicurezza

Platform As A Service

Cliente	Fornitore
• Manutenzione del sistema di gestione delle identità • Gestione del sistema di gestione delle identità • Gestione della piattaforma di autenticazione (inclusa l'applicazione delle politiche relative alle password)	• Infrastruttura fisica di supporto (impianti, spazio a rack, alimentazione, raffreddamento, cablaggi, ecc.) • Sicurezza e disponibilità dell'infrastruttura fisica (server, storage, ampiezza di banda, ecc.) • Gestione degli aggiornamenti dell'OS e procedure di hardening (verificare anche ogni conflitto tra procedure di hardening dei clienti) • Configurazione di sicurezza della piattaforma (regole del firewall, configurazione dell'IDS/IPS, ecc.) • Monitoraggio dei sistemi • Manutenzione della sicurezza della piattaforma (Firewall, Host IDS/IPS, antivirus, packet filtering) • Raccolta dei log e monitoraggio della sicurezza

Infrastructure As A Service

Laddove i clienti siano responsabili per la sicurezza delle proprie infrastrutture (IaaS), essi dovrebbero considerare quanto segue:

Sicurezza applicativa nell'Infrastructure As A Service

I fornitori di applicazioni IaaS trattano le applicazioni nell'istanza virtuale del cliente come una "scatola nera" e quindi sono completamente agnostici per quanto concerne l'operatività e la gestione di un'applicazione del cliente. L'intero 'stack' – applicazione del cliente, piattaforma applicativa run time (.Net, Java, Ruby, PHP, ecc.) - è fatta girare sul server del cliente (nell'infrastruttura del fornitore) ed è gestita dai clienti stessi. Per questa ragione è di vitale importanza notare che i clienti devono assumersi completa responsabilità della messa in sicurezza delle proprie applicazioni distribuite attraverso il cloud. Di seguito si dà una breve lista di controllo e la descrizione delle migliori prassi per la progettazione e la gestione sicura delle applicazioni:

- Le applicazioni cloud distribuite devono essere progettate per il modello di minaccia Internet (anche se sono distribuite come parte di un VPC - virtual cloud privato).
- Le applicazioni devono essere progettate o integrate con misure di sicurezza standard per premunirsi contro le vulnerabilità Web comuni (vedi OWASP Top Ten (40)).
- I clienti sono responsabili dell'aggiornamento puntuale delle proprie applicazioni - e devono quindi garantire di avere una strategia di aggiornamento (per garantire che le loro applicazioni siano protette dal malware e dalle scansioni che gli hacker compiono alla ricerca delle vulnerabilità che consentano loro di accedere in modo non autorizzato ai dati nel cloud).

Per questa ragione è di vitale importanza notare che i clienti assumono completa responsabilità della messa in sicurezza delle proprie applicazioni distribuite attraverso il cloud.

- I clienti dovrebbero resistere alla tentazione di utilizzare implementazioni personalizzate di autenticazione, autorizzazione e accounting (AAA), poiché queste, se non correttamente implementate, possono rivelarsi deboli.

In sintesi: le applicazioni aziendali distribuite nel cloud devono essere eseguite attuando molti controlli per la messa in sicurezza dell'host (e della rete - vedi sezione precedente), dell'accesso degli utenti, e attuando i controlli a livello applicativo (si vedano le guide OWASP (41) relative alla progettazione di web/online sicuro). Inoltre, va tenuto presente che molti tra i principali fornitori, quali Microsoft, Oracle, Sun, ecc., pubblicano una completa documentazione su come proteggere la configurazione dei loro prodotti.

Metodologia

Le sezioni principali di questo documento si basano sulle ampie classi di controlli degli standard ISO 27001/2 (42), (43) e BS25999 (44). Dettagli all'interno di queste sezioni sono derivati da entrambe le norme, così come dalle migliori prassi del settore. In tutto, abbiamo selezionato solo i controlli che sono pertinenti ai cloud provider di terze parti e outsourcer.

Il quadro dettagliato previsto in uscita nel 2010 è destinato a includere standard aggiuntivi, quali NIST SP 800-53 (45).

Avvertenza

La serie di domande dettagliate all'interno della sezione che segue è una selezione di controlli comuni. Non è destinato a essere un elenco esaustivo, allo stesso modo, alcune domande possono non essere applicabili a implementazioni particolari. Di conseguenza questo elenco dovrebbe essere utilizzato come una base di controlli comuni, e ulteriori dettagli dovrebbero essere ricercati laddove necessario.

E' anche interessante notare che, sebbene sia possibile trasferire molti dei rischi a un fornitore esterno, l'effettivo costo del trasferimento del rischio è

molto raramente compreso. Ad esempio, un incidente di sicurezza che comporta la divulgazione non autorizzata dei dati del cliente può causare una perdita finanziaria per il fornitore, tuttavia la pubblicità negativa e la perdita di fiducia dei consumatori e le potenziali sanzioni normative (PCI-DSS) sarebbero sostenute dal cliente finale. Tale scenario evidenzia l'importanza di distinguere tra rischio e rischio commerciale. E' possibile trasferire il rischio commerciale, ma in definitiva il rischio rimane sempre al cliente finale.

Qualsiasi risposta ai risultati di una valutazione dei rischi - in particolare l'importo e il tipo di investimento da fare nella mitigazione, dovrebbe essere deciso sulla base della propensione al rischio dell'organizzazione e delle opportunità e dei risparmi finanziari che si perdono seguendo una particolare strategia di mitigazione del rischio.

I clienti cloud dovrebbero anche svolgere le proprie analisi del rischio specifiche per il contesto. Alcune metodologie di Gestione del Rischio / Valutazione del Rischio possono essere reperite nel sito: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

Poiché l'ambiente normativo e di lavoro muta e sorgono nuovi rischi, la valutazione del rischio dovrebbe essere un'attività regolare, piuttosto che un evento isolato.

Nota per i governi

I seguenti controlli si rivolgono principalmente alle PMI impegnate nella valutazione di fornitori cloud. Possono anche essere utili per governi con le seguenti clausole. *Le caratteristiche del cloud utilizzato dovrebbero essere valutate attentamente in relazione ad ogni programma di classificazione delle informazioni dell'ente governativo.*

- L'utilizzo di cloud pubblici - anche se con esiti favorevoli dal seguente questionario - non è raccomandato per nessun utilizzo, se non per i dati che appartengono alle classi più basse di sicurezza.

- Per i dati che ricadono nelle classi di sicurezza più elevate, la lista di controlli suggerita in questo documento è valida, ma dovrebbe essere integrata con controlli aggiuntivi. Questo documento non intende coprire tali controlli, ma quanto segue sono esempi di questioni che dovrebbero essere considerate:
  - Il fornitore offre informazioni trasparenti e pieno controllo sulla localizzazione fisica di tutti I dati? L'elevata sicurezza dei dati è spesso ridotta in virtù della loro localizzazione.
  - Il fornitore supporta gli schemi di classificazione dei dati in uso?
  - Quali garanzie offre il fornitore in merito al pieno isolamento delle risorse del cliente (ad esempio, non condivisione di macchine fisiche)?
  - Supponendo che le macchine fisiche non siano condivise tra clienti, fino a che punto l'archiviazione dei dati, la memoria e altre tracce sono completamente cancellate prima della riallocazione delle macchine?
  - Il fornitore supporta o addirittura richiede l'utilizzo dell'autenticazione a due fattori con token fisico per l'accesso del cliente?
  - Il fornitore è certificato ISO 27001/2? Qual è l'ambito di certificazione?
  - I prodotti utilizzati dal fornitore sono certificati Common Criteria? A che livello? Quali sono il profilo di protezione e l'obiettivo di sicurezza dei prodotti?

REQUISITI DI SICUREZZA DELLE INFORMAZIONI

Sicurezza del personale

La maggior parte delle domande riguardanti il personale sono simili a quelle che si porrebbero in relazione al proprio personale addetto all'IT o ad altro personale che abbia a che fare con i vostri sistemi IT. Come in molte valutazioni, c'è un bilanciamento tra rischi e costi.

- Quali politiche e procedure sono state attuate all'atto dell'assunzione degli amministratori IT o di altri con accesso al sistema? Queste dovrebbero includere:
    - controlli pre-assunzione (identità, nazionalità o Stato, storia dell'impiego e delle referenze, condanne penali, e controlli preliminari (per personale con anzianità e quello in ruoli con privilegi elevati)).
- Ci sono politiche diverse a seconda di dove sono memorizzati i dati o di dove vengono eseguite le applicazioni?
    - Ad esempio, le politiche di assunzione possono differire da una regione all'altra.
    - Le prassi devono essere consistenti tra regioni.
    - Può verificarsi che i dati sensibili siano memorizzati in una regione specifica con personale adeguato.
- Quale programma di educazione alla sicurezza viene somministrato a tutti i dipendenti?
- Esiste un processo di valutazione continua?
    - Con quale *cadenza*?
    - Ulteriori c*olloqui*
    - censimento degli accessi e privilegi di sicurezza
    - *censimento de*lle politiche e delle procedure

Sicurezza della catena di fornitura (Supply Chain)

Le seguenti domande si applicano qualora il provider cloud subappalti a terzi alcune operazioni fondamentali per la sicurezza (ad esempio, un provider SaaS che affidi in outsourcing a un fornitore terzo la piattaforma sottostante, un fornitore cloud che dia in outsourcing servizi di sicurezza ad un fornitore di servizi di sicurezza gestita, l'uso di un fornitore esterno per la gestione delle identità dei sistemi operativi, ecc.). Esso comprende anche soggetti terzi che abbiano accesso fisico o da remoto al fornitore di infrastrutture cloud. Si presume che questo intero questionario possa essere applicato ricorsivamente al terzo (o ennesimo) fornitore cloud di servizi esterni.

- Definire i servizi fondamentali per la sicurezza delle operazioni (inclusa la disponibilità) che, nella catena di fornitura, sono appaltati o dati in outsourcing.
- Dettagliare le procedure utilizzate per dare accesso (fisico e/o logico) a terze parti all'infrastruttura.
  - Si eseguono audit degli outsourcer e dei subappaltatori, e con quale frequenza?
- Gli SLA garantiti dagli outsourcer sono inferiori a quelli che offrite ai vostri clienti? In caso contrario, sono in atto misure di ridondanza dei fornitori?
- Quali misure sono adottate per garantire che i livelli di servizio delle terze parti siano soddisfatti e mantenuti?
- Il fornitore cloud può confermare che la politica di sicurezza e i controlli sono (contrattualmente) applicati ai propri fornitori terzi?

Sicurezza operativa

Si prevede che qualsiasi accordo commerciale con fornitori esterni comprenda livelli di servizio per tutti i servizi di rete. Tuttavia, in aggiunta agli accordi definiti, il cliente finale deve comunque garantire che il fornitore applichi controlli appropriati per mitigare divulgazioni non autorizzate.

- Specificare le politiche e le procedure di controllo dei cambiamenti. Queste dovrebbero includere anche il processo utilizzato per valutare i rischi connessi ai cambiamenti e chiarificare quali output siano disponibili ai clienti finali.
- Definire le politiche di accesso remoto
- Il fornitore mantiene procedure operative documentate per i sistemi di informazione?
- L'ambiente è organizzato per la riduzione del rischio, ad esempio esistono ambienti separati per sviluppo, test e ambiente operativo?
- Definire i controlli di rete e di host utilizzati per proteggere i sistemi che ospitano le applicazioni e le informazioni del cliente finale. Questi dovrebbero comprendere i dettagli relativi alle certificazioni secondo standard esterni (ad esempio, ISO 27001/2).
- Specificare i controlli utilizzati per la protezione da codice malevolo.
- Sono implementate configurazioni sicure che consentono l'esecuzione solo di funzionalità e di codice mobile autorizzati (ad esempio, l'esecuzione solo di comandi specifici)?
- Dettagliare le politiche e le procedure per i backup. Esse dovrebbero comprendere procedure per la gestione di supporti rimovibili e metodi per la distruzione sicura dei backup quand'essi non sono più necessari. (Sulla base delle proprie necessità, il cliente potrebbe voler implementare una strategia di backup indipendente. Ciò è particolarmente rilevante quando il tempo di accesso ai backup sia critico.)

Il controllo dei log è utilizzato in caso di incidente che richieda un'indagine, ma può essere utilizzato anche per la risoluzione di problemi. A tal fine, al cliente finale dovrà essere garantita la disponibilità di tali informazioni:

- Il fornitore può dettagliare quali informazioni sono registrate nei log di audit?
  - Per quale periodo sono conservate tali informazioni?

  - E' possibile segmentare i dati dei log così che siano disponibili per il cliente finale e/o per le forze dell'ordine senza compromettere i log degli altri clienti ed in modo che siano ammissibili in giudizio?
  - Quali controlli sono implementati per proteggere i log dagli accessi non autorizzati e dalla manomissione?
  - Quale metodo è utilizzato per verificare e proteggere l'integrità dei log?
- Come sono verificati i log? Quali eventi registrati generano reazioni?
- Quale fonte è utilizzata per la sincronizzazione dei tempi sui sistemi e per fornire la marcatura temporale accurata dei log?

SICUREZZA DEL SOFTWARE

- Definire i controlli utilizzati per proteggere l'integrità del sistema operativo e delle applicazioni software in uso. Includere tutte le norme che vengono seguite, ad esempio, OWASP (46), Lista di controllo SANS (47), SAFECode (48).
- Come viene verificata l'idoneità e l'assenza di rischi dei nuovi rilasci (backdoor, trojan, ecc.)? Essi sono recensiti prima dell'utilizzo?
- Quali prassi vengono seguite per mantenere in sicurezza le applicazioni?
- Sono effettuati dei penetration test al rilascio del software così da accertare che non vi siano vulnerabilità? Qualora vengano riscontrate delle vulnerabilità, qual è il processo per porvi rimedio?

Gestione degli aggiornamenti

- Fornire dettagli sulla procedura di gestione degli aggiornamenti.
- E' possibile garantire che il processo di gestione degli aggiornamenti copra tutti gli strati delle tecnologie di distribuzione cloud – ad esempio, rete (componenti di infrastruttura, router e switch, ecc.), sistemi operativi dei server, software di virtualizzazione, sottosistemi ed applicazioni di sicurezza (firewall, gateway antivirus, sistemi di intrusion detection, ecc.)?

Controlli dell'architettura di rete

- Definire i controlli utilizzati per mitigare gli attacchi DDoS (denial–of-service distribuito).
  - Defense in depth (analisi approfondita dei pacchetti, throttling del traffico, packet black-holing, ecc.)
  - Sono implementate difese contro attacchi interni (che originano dalle reti del fornitore cloud) ed esterni (che originano dalle reti del Cliente o da internet)?
- Quali livelli di isolamento sono utilizzati?
  - Per le macchine virtuali, le macchine fisiche, le reti, lo storage (ad esempio, storage area networks), i sistemi per la gestione della rete e dei sistemi, ecc.
- L'architettura supporta la continuità dell'operatività dal cloud qualora l'azienda fosse separata dal fornitore di servizio e viceversa (ad esempio, c'è una dipendenza critica dal sistema LDAP del cliente)?
- L'infrastruttura di rete virtuale utilizzata dai fornitori cloud (in architettura PVLANs and VLAN tagging 802.1q (49)) è messa in sicurezza secondo gli standard specifici e/o migliori prassi (ad esempio, la prevenzione dagli attacchi di MAC spoofing, ARP poisoning, ecc. è attuata mediante una configurazione di sicurezza specifica)?

Architettura dell'Host

- Il fornitore garantisce che le immagini virtuali siano hardenizzate di default?
- L'immagine virtuale hardenizzata è protetta dagli accessi non autorizzati?
- Il fornitore può confermare che le immagini virtualizzate non contengano le credenziali di autenticazione?
- Il firewall dell'host ha aperto il numero minimo di porte per i servizi dell'istanza virtuale?
- Può essere utilizzato un IPS (intrusion prevention service) nell'istanza virtuale?

PaaS – Sicurezza applicativa

In generale, i fornitori di servizi PaaS sono responsabili per la sicurezza dello stack software della piattaforma, e le raccomandazioni in questo documento sono una buona base per garantire che un fornitore PaaS abbia preso in considerazione i principi di sicurezza durante la progettazione e la gestione della sua piattaforma PaaS. Spesso è difficile ottenere informazioni dettagliate da parte dei fornitori PaaS su come esattamente essi proteggono le proprie piattaforme - tuttavia le seguenti domande, insieme ad altre sezioni all'interno di questo documento, dovrebbero essere utili per valutare le loro offerte.

- Richiedere informazioni su come le applicazioni multi-tenant sono isolate l'una dall'altra - è necessaria una descrizione d'alto livello delle misure di contenimento e di isolamento.
- Che garanzie può fornire il provider PaaS che l'accesso ai dati è limitato agli utenti aziendali ed alle applicazioni che il cliente possiede?
- L'architettura della piattaforma dovrebbe essere il classico 'sandbox' - il fornitore garantisce che per la piattaforma PaaS sandbox esiste un controllo relativo a nuovi bug e vulnerabilità?
- I fornitori PaaS dovrebbero essere in grado di offrire un insieme di funzionalità di sicurezza (riutilizzabili tra i loro clienti) - queste includono l'autenticazione degli utenti, il Single Sign-On, l'autorizzazione (gestione dei privilegi), e SSL / TLS (messo a disposizione tramite un API)?

SAAS – Sicurezza applicativa

Il modello SaaS impone che il fornitore gestisca l'intera suite di applicazioni fornite agli utenti finali. Pertanto i fornitori di SaaS sono i principali responsabili per la protezione di queste applicazioni. I clienti sono, di solito, responsabili dei processi operativi di sicurezza (gestione degli utenti e dell'accesso). Tuttavia, le seguenti domande, insieme ad altre sezioni all'interno di questo documento, dovrebbero aiutare a valutare le loro offerte:

- Quali controlli di amministrazione (sistemi) vengono forniti e quali tra questi possono essere utilizzati per assegnare i privilegi di lettura e scrittura ad altri utenti?
- Il controllo accessi SaaS è granulare e può essere personalizzato dall'organizzazione cliente sulla base delle proprie politiche?

Approvvigionamento delle risorse

- Nell'eventualità di un sovraccarico di risorse (elaborazione, memoria, storage, rete)?
  - Quali informazioni sono fornite sulla priorità relativa assegnata alla richiesta in caso di un problema nell'approvvigionamento?
  - C'è un lasso di tempo per il cambiamento nei livelli di servizio e nei requisiti?
- Quanto si può scalare a crescere? Il fornitore offre garanzie su un massimo di risorse disponibili entro un periodo minimo?
- Quanto velocemente si può scalare a crescere? Il fornitore offre garanzie sulla disponibilità di risorse supplementari entro un periodo minimo?
- Quali processi sono in atto per la gestione su larga scala delle tendenze di utilizzo delle risorse (ad esempio, stagionalità)?

Gestione dell'identità e degli accessi

I controlli seguenti si applicano ai sistemi di gestione dell'identità e degli accessi del fornitore (quelli che ricadono sotto il suo controllo):

AUTORIZZAZIONE

- Esistono account che hanno ampi privilegi per l'intero sistema cloud e, se così fosse, per quali attività (lettura/scrittura/cancellazione)?
- Come sono autenticati e gestiti gli account che hanno il più alto livello di privilegi?
- Come sono autorizzate le decisioni maggiormente critiche (autorizzazione singola o doppia, e quali sono nell'organizzazione i ruoli interessati) (ad esempio, distacco simultaneo di grandi blocchi di risorse)?

- Ci sono più ruoli con alti privilegi assegnati a uno stesso individuo? Questa assegnazione contraddice la regola della separazione delle funzioni o del minor privilegio?
- E' in uso il controllo degli accessi basato sul ruolo (RBAC)? Viene seguito il principio del minor privilegio?
- Quali cambiamenti vengono apportati ai privilegi e ruoli amministrativi, se ne vengono fatti, per consentire accesso straordinario in caso di emergenza?
- Il cliente ha un ruolo 'administrator'? Ad esempio, l'administrator del cliente ha un ruolo nel creare nuovi utenti (ma senza permettergli di cambiare lo storage sottostante!)?

Identity Provisioning

- Quali controlli sono eseguiti, all'atto della registrazione, sull'identità degli account utente? Viene seguito uno standard? Ad esempio, il "e-Government Interoperability Framework"?
- Esistono differenti livelli di controlli sull'identità in base alle risorse richieste?
- Quali processi sono implementati per il de-provisioning delle credenziali?
- Le credenziali sono fornite e revocate simultaneamente su tutto il sistema cloud, o esistono rischi nel revocarle tra siti multipli geograficamente distribituiti?

Gestione dei dati personali

- Quali controlli relativi allo storage dei dati e alla loro protezione si applicano ai servizi di directory utente (ad esempio, AD, LDAP) e al loro accesso?
- I dati dei servizi di user directory sono esportabili in un formato interoperabile?
- L'accesso ai dati del cliente nel cloud è basato sul need-to-know?

Gestione delle chiavi (di cifratura)

Per le chiavi (di cifratura) sotto il controllo del fornitore cloud:

- Sono implementati controlli di sicurezza per la lettura e la scrittura delle chiavi? Ad esempio, politiche di password forti, chiavi memorizzate in un sistema separato, moduli di sicurezza hardware (HSM) per le chiavi del certificato root, l'autenticazione basata su smart card e accesso diretto schermato allo storage, breve durata della chiave, ecc.
- Sono implementati controlli che usano quelle chiavi per la firma e la cifratura dei dati?
- Sono implementate procedure per la gestione della compromissione di una chiave? Ad esempio, liste di revoca delle chiavi.
- La revoca della chiave è simultanea su siti multipli?
- Le immagini dei sistemi del cliente sono protette o cifrate?

Cifratura

- La cifratura può essere utilizzata in molti posti – dove è utilizzata?
  - per i dati in transito
  - per i dati a riposo (statici)
  - per i dati nel processore o in memoria?
- Nomi utente e password?
- Esiste una ben definita politica che definisca cosa dovrebbe essere cifrato e cosa no?
- Chi custodisce le chiavi di accesso?
- Come sono protette le chiavi?

Autenticazione

- Quali forme di autenticazione sono utilizzate per le azioni che richiedono elevata sicurezza? Queste forme potrebbero includere l'accesso alle interfacce di gestione, la creazione delle chiavi, l'accesso ad account multi-utente, la configurazione dei firewall, l'accesso da remoto, ecc.

- E' utilizzata l'autenticazione a due fattori per la gestione dei componenti critici dell'infrastruttura, quali firewall, ecc.?

Compromissione o furto delle credenziali

- Viene fornita la funzionalità di rilevamento anomalie (la capacità di individuare traffico IP inusuale e potenzialmente malevolo e comportamenti analogamente malevoli degli utenti o del gruppo di supporto)? Ad esempio, l'analisi dei login riusciti e falliti, login in orari non usuali, login multipli, ecc.
- Quali disposizioni esistono nell'eventualità di furto delle credenziali utente (rilevazione, revoca, traccia di azioni eseguite)?

Sistemi di gestione dell'identità e dell'accesso offerti ai clienti cloud

Le domande seguenti sono valide per i sistemi di gestione dell'identità e dell'accesso che sono offerti dal fornitore cloud e utilizzati e controllati dal cliente cloud:

STRUTTURE PER LA GESTIONE DELL'IDENTITA'

- Il sistema consente di avere un'infrastruttura IDM federata interoperabile sia per elevata sicurezza (dove richiesto, sistemi OTP) che minore sicurezza (ad esempio, nome utente e password)?
- Il fornitore cloud è interoperabile con fornitori di identità terzi?
- Esiste la possibilità di integrare il single sign-on?

CONTROLLO ACCESSI

- Il sistema di credenziali del cliente consente la separazione di ruoli e responsabilità e i domini multipli (o utilizza una singola chiave per più domini, ruoli e responsabilità)?
- Come è gestito l'accesso alle immagini di sistema del cliente - e come sono messe in sicurezza le chiavi crittografiche e di autenticazione in esse contenute?

AUTENTICAZIONE

- Come identifica il fornitore cloud se stesso nei confronti dei clienti (ad esempio, utilizzo della mutua autenticazione)?
  - Quando il cliente invia comandi mediante API?
  - Quando il cliente accede ad una interfaccia di gestione?
- Viene supportato un meccanismo federato di autenticazione?

Gestione degli asset

È importante assicurarsi che il fornitore mantenga un elenco aggiornato degli asset hardware e software (le applicazioni) che ricadono nell'ambito di controllo dei fornitori cloud. Ciò permette di verificare che tutti i sistemi impieghino gli opportuni controlli, e che i sistemi stessi non possano essere utilizzati come backdoor per l'infrastruttura.

- Il fornitore ha un sistema di censimento automatizzato di tutti gli asset, che ne facilita l'adeguata gestione?
- C'è una lista degli asset che il cliente ha utilizzato in uno specifico lasso di tempo?

Le seguenti domande sono da utilizzarsi nel caso in cui il cliente finale stia implementando dati che richiedono protezioni aggiuntive (ad esempio, classificati come sensibili).

- Gli asset sono classificati in termini di sensibilità e criticità?
  - Se tale classificazione è implementata, il fornitore utilizza un'opportuna separazione tra sistemi con classificazione differente e nel caso di cliente singolo che ha sistemi con classificazioni differenti?

Portabilità dei dati e dei servizi

Questo insieme di domande dovrebbe essere preso in considerazione per comprendere i rischi connessi al lock-in (accordo in esclusiva) nei confronti del fornitore.

- Esistono procedure documentate e API per esportare i dati dal cloud?
- Il fornitore offre formati interoperabili per tutti i dati immagazzinati nel cloud?
- Nel caso di SaaS, le interfacce API utilizzate sono standardizzate?
- Esistono consegne per esportare in formato standard le applicazioni create dall'utente?
- Esistono processi per testare che i dati possano essere esportati verso un altro fornitore cloud – ad esempio, qualora il cliente volesse cambiare fornitore?
- Il cliente può effettuare l'estrazione dei propri dati per verificare che il formato sia universale e capace di essere migrato verso un altro fornitore cloud?

Gestione della continuità operativa

Per un'organizzazione è importante erogare servizi con continuità. Benché sia possibile definire a livello di accordi di servizio (SLA) accordi sull'ammontare minimo di tempo durante il quale i servizi sono disponibili, rimangono un certo numero di ulteriori considerazioni

- Il fornitore mantiene un metodo documentato che dettaglia l'impatto di un'interruzione di servizio?
  - Quali sono l'RPO (recovery point objective) e l'RTO (recovery time objective) per i servizi? I dettagli devono concordare con la criticità del servizio.
  - Nel processo di ripristino le attività volte alla sicurezza delle informazioni sono opportunamente indirizzate?
  - Quali sono le linee di comunicazione all'utente finale nell'eventualità di un disservizio?
  - I ruoli e le responsabilità dei gruppi (di supporto) sono chiaramente identificate in caso di disservizio?

- il fornitore ha classificato la priorità del recupero, e quale potrebbe essere la nostra priorità relativa (del cliente finale) di ripristino? Nota: questa può essere una categoria (ALTA/ MEDIA / BASSA).
- Quali dipendenze rilevanti per il processo di ripristino esistono? Inclusi fornitori e partner in outsourcing.
- Nel caso il sito primario sia non disponibile, qual è la distanza minima per la posizione del sito secondario?

Gestione degli incidenti (e della risposta)

La gestione degli incidenti (e della risposta) è una parte della gestione della business continuity. L'obiettivo di questo processo è quello di contenere ad un livello accettabile l'impatto di eventi inattesi e potenzialmente distruttivi per un'organizzazione.

Per valutare la capacità di un'organizzazione di minimizzare la probabilità di un evento o per ridurre l'impatto negativo di un incidente di sicurezza delle informazioni, le seguenti domande dovrebbero essere poste al fornitore cloud:

- Il fornitore implementa un processo formale per il rilevamento, l'identificazione, l'analisi e la risposta agli incidenti?
- Allo scopo di controllare che i processi di gestione degli incidenti siano efficaci, questo processo è provato? Il fornitore garantisce anche, durante la prova, che chiunque nell'organizzazione di supporto del fornitore sia a conoscenza dei processi e del proprio ruolo durante la gestione di un incidente (sia durante l'incidente che nella fase di post-analysis)?
- Come sono strutturate le funzionalità di rilevamento?
  - In che modo il cliente cloud può riferire al fornitore di anomalie ed eventi di sicurezza?
  - Quali strutture di terze parti selezionate dal cliente per intervenire sui sistemi (laddove appropriato) o per coordinare le funzionalità di risposta agli incidenti con il fornitore cloud, mette a disposizione il fornitore stesso?

  - E' implementato un controllo di sicurezza in real-time (RTSM)? Il servizio è appaltato all'esterno? Che tipo di parametri e servizi sono monitorati?
  - Viene fornito (su richiesta) un report periodico degli incidenti di sicurezza (ad esempio, in accordo con la definizione ITIL)?
  - Per quanto tempo sono conservati i log di sicurezza? Questi log sono conservati in modo sicuro? Chi ha accesso ai log?
  - E' possibile per il cliente realizzare un HIPS/HIDS nell'immagine della macchina virtuale? E' possibile integrare le informazioni raccolte dai sistemi di rilevamento e prevenzione delle intrusioni nel servizio RTSM del fornitore cloud o di una terza parte?
- Come sono definiti i livelli di severità?
- Come sono definite le procedure di escalation? Quando (se mai) è coinvolto il cliente cloud?
- Come sono documentati gli incidenti e raccolte le evidenze?
- Oltre all'autenticazione, all'accounting e all'audit, quali altri controlli sono implementati per prevenire (o minimizzare l'impatto di) attività malevole condotte da insiders?
- Il fornitore offre al cliente (su richiesta) un'immagine forense della macchina virtuale?
- Il fornitore raccoglie metriche e indicatori di incidente (ad esempio, numero di incidenti rilevati o segnalati per mese, numero di incidenti causati dai subappaltatori del fornitore cloud e numero totale di tali incidenti, tempo medio di risposta e risoluzione, ecc.)?
  - Cosa, tra quanto elencato, viene messo pubblicamente a disposizione dal fornitore (NB non tutti i report di incidenti possono essere resi pubblici poiché ciò potrebbe compromettere la confidenzialità del cliente e rivelare dati critici sulla sicurezza)?
- Quanto spesso il fornitore esegue test dei piani di disaster recovery e continuità operativa?
- Il fornitore raccoglie dati su tutti i livelli di soddisfazione rispetto agli SLA?

- Il fornitore conduce test di help desk? Ad esempio:
  - Test di impersonificazione (la persona che chiama per un reset della password è realmente chi asserisce di essere?), o cosiddetti attacchi di 'social engineering'.
- Il fornitore esegue test di intrusione (penetration test)? Con che frequenza? Cosa viene effettivamente testato durante i penetration test – ad esempio, viene verificata la sicurezza dell'isolamento di ogni immagine per assicurare che non sia possibile "evadere" da un'immagine in un'altra ed anche avere accesso all'infrastruttura host? I test dovrebbero anche controllare se è possibile avere accesso, tramite l'immagine virtuale, ai sistemi di gestione e supporto del fornitore (ad esempio, i sistemi di distribuzione e l'accesso amministrativo ai sistemi di controllo).
- Il fornitore esegue test di vulnerabilità? Con quale frequenza?
- Qual è il processo di rimedio alle vulnerabilità (aggiornamenti rapidi, riconfigurazioni, aggiornamento a nuove versioni del software, ecc.)?

Sicurezza fisica

Come per la sicurezza del personale, molte delle questioni potenziali sorgono perché l'infrastruttura IT è sotto controllo di una terza parte – come nell'outsourcing tradizionale, l'effetto di una breccia di sicurezza fisica può avere impatto su più clienti (organizzazioni).

- Quali garanzie possono essere fornite al cliente in relazione alla sicurezza fisica dei luoghi? Andrebbero forniti esempi, e indicazioni degli standard cui si aderisce, ad esempio Sezione 9 della ISO 27001/2.
  - Chi, oltre al personale IT autorizzato, ha accesso (fisico) non scortato all'infrastruttura IT?
    - Ad esempio, addetti alle pulizie, dirigenti, personale addetto alla 'sicurezza fisica', appaltatori, venditori, ecc.
  - Quanto sovente vengono rivisti i diritti di accesso?
    - Con che rapidità i diritti di accesso possono essere revocati?

- I rischi per la sicurezza e i perimetri vengono valutati su base regolare?
  - Con che frequenza?
- Vengono effettuate con regolarità valutazioni dei rischi che includano aspetti quali gli edifici vicini?
- C'è un controllo o un monitoraggio sul personale (incluso quello di terze parti) che accede ad aree sicure?
- Quali politiche o procedure sono implementate per il carico, scarico e installazione dell'equipaggiamento?
- I beni in consegna vengono ispezionati prima dell'installazione per evitare rischi?
- C'è un inventario aggiornato dei componenti fisici nel data centre?
- I cavi di rete sono stesi attraverso aree di pubblico accesso?
  - Si fa uso di cablaggi rinforzati o di condutture (canaline e passerelle passacavi)?
- Gli ambienti vengono ispezionati con regolarità alla ricerca di materiale non autorizzato?
- Esiste materiale fuori dal sito?
  - Come è protetto?
- Il personale utilizza equipaggiamento portatile (ad esempio, laptop, smartphones) che potrebbe consentire l'accesso al data centre?
  - Come è protetto questo equipaggiamento?
- Quali misure sono implementate per controllare i cartellini di accesso?
- Quali procedure o processi sono implementati per la distruzione dei sistemi o dei supporti obsoleti, quando se ne presenta la necessità?
  - Sovrascrittura dei dati?
  - Distruzione fisica?
- Quali processi autorizzativi sono implementati per lo spostamento dell'equipaggiamento da un sito ad un altro?
  - Come avviene l'identificazione del proprio personale (o appaltatori) autorizzato a tale attività?

- Con che frequenza sono condotti degli audit dell'equipaggiamento per verificare che non avvengano spostamenti non autorizzati?
- Con che frequenza vengono fatti controlli per assicurarsi che gli ambienti siano conformi a quanto richiesto dalle norme e leggi pertinenti?

Controlli ambientali

- Quali procedure o politiche sono implementate per assicurare che questioni ambientali non provochino interruzioni di servizio?
- Quali metodi sono utilizzati per la prevenzione incendi, allagamenti, terremoti, ecc.?
  - Nell'eventualità di un evento disastroso, quali misure di sicurezza aggiuntive sono implementate per proteggere l'accesso fisico?
  - Sia a livello di sito primario che di secondario?
- Temperatura ed umidità nel data centre sono monitorate?
  - Il condizionamento dell'aria è monitorato?
- Gli edifici sono protetti contro gli effetti del fulmine?
  - Incluse le linee elettriche e le linee dati?
- Sono installati e funzionanti generatori autonomi per far fronte a eventuali assenze di tensione?
  - Qual è la loro autonomia?
  - Sono disponibili scorte adeguate di carburante?
  - Ci sono generatori in failover?
  - Con che frequenza è controllato il gruppo di continuità (UPS)?
  - Con che frequenza sono controllati i generatori?
  - La fornitura di energia elettrica è ridondata?
- Le utilities (elettricità, acqua, ecc.) sono in grado di supportare i carichi?
  - Con che frequenza avviene la verifica di questa adeguatezza?
- L'impianto di condizionamento dell'aria è in grado di sopportare i carichi termici dell'ambiente specifico?
  - Con che frequenza è testato?

- Vengono rispettati le prescrizioni di manutenzione programmata raccomandate dai costruttori?
- Viene ammesso all'interno dell'edificio il solo personale autorizzato addetto alla manutenzione o riparazione?
  - Come viene verificata la sua identità?
- Quando l'equipaggiamento è inviato in riparazione, i dati sono preventivamente cancellati?
  - In che modo avviene la cancellazione preventiva?

REQUISITI LEGALI

Clienti e potenziali clienti di fornitori di servizi cloud dovrebbero prendere in considerazione i rispettivi obblighi nazionali e sovranazionali in materia di conformità con i quadri normativi e assicurarsi che tali obblighi siano adeguatamente rispettati.

Le domande chiave in ambito legale che il cliente dovrebbe porre al fornitore cloud sono:

- In quale nazione risiede il fornitore cloud?
- L'infrastruttura del fornitore cloud è nella stessa nazione o distribuita in più paesi?
- Il fornitore cloud utilizza altre aziende le cui infrastrutture sono localizzate al di fuori delle proprie?
- Dove saranno fisicamente localizzati i dati?
- La giurisdizione dei dati e quella dei termini contrattuali sono disgiunte?
- Quali tra i servizi del fornitore cloud sono subappaltati?
- Quali tra i servizi del fornitore cloud sono in dati in outsourcing?
- Come saranno raccolti, trattati e trasferiti i dati del cliente e dei suoi clienti?
- Cosa accade ai dati inviati al fornitore cloud dopo il termine del contratto?

RACCOMANDAZIONI DI NATURA LEGALE

Attualmente, la gran parte delle questioni di natura legale connesse al cloud computing vengono risolte all'atto della valutazione del contratto, dei Termini di Utilizzo (ToU), degli accordi di licenza (ULA) e degli SLA da parte del cliente. E' importante distinguere tra il caso della piccola e media organizzazione che si trova a scegliere tra i differenti contratti presenti sul mercato, e le organizzazioni più grandi, che sono nella posizione di poter negoziare le clausole contrattuali. Nell'analisi legale in questo documento, si assume la prospettiva di una piccola media organizzazione che stia valutando differenti

contratti, SLA, ecc. offerti sul mercato, poiché è questo il caso più comune. Ciò perché il modello di business del cloud computing è differente da quello dell'outsourcing: per fornire alcuni dei propri benefici ai clienti, il cloud computing si basa su economie di scala per distribuire servizi di tipo commodity a basso costo, molto differente da un servizio specificamente costruito sulle esigenze del cliente. Le organizzazioni più grandi possono però utilizzare le stesse considerazioni (dell'outsourcing) quando negoziano i contratti. Mentre le passate esperienze con tecnologie internet similari costituiscono una qualche guida che consente ai clienti e ai fornitori cloud di valutare i rischi di sicurezza connessi al cloud computing, è necessario per entrambi considerare la natura unica del cloud computing quando si valutano questi rischi.

Sebbene vi sia un ampio terreno comune, alcune clausole contrattuali standard potrebbero meritare una revisione ulteriore che tenga conto della natura del cloud computing. Particolare attenzione dovrebbe essere posta ai diritti e obblighi connessi alla comunicazione delle brecce di sicurezza, il trasferimento dei dati, la creazione di lavori derivati, il cambio del controllo, e l'accesso ai dati da parte delle forze dell'ordine. Poiché il cloud può essere utilizzato per porre in outsourcing infrastrutture critiche interne, e l'interruzione di una tale infrastruttura potrebbe avere effetti ad ampio raggio, dovrebbe essere posta attenzione a che le limitazioni standard di responsabilità o rappresentino adeguatamente la suddivisione delle responsabilità, stante l'utilizzo del cloud che ne fanno le parti, o una imputazione di responsabilità per l'infrastruttura [cfr. Suddivisione delle responsabilità].

Finché il precedente legale non chiarisce le questioni relative alla sicurezza dei dati che sono specifiche del cloud computing, i clienti ed allo stesso modo fornitori dovrebbero prestare attenzione ai termini dei propri contratti per gestire i rischi in modo efficace.

Quanto segue è una lista di aree cui il cliente dovrebbe prestare particolare attenzione nella valutazione degli SLA, Termini di Utilizzo, ULA e di altre clausole contrattuali per servizi cloud:

1. **Protezione dei dati**: si dovrebbe prestare attenzione a scegliere un data processor (nel senso di persona che tratta i dati) che fornisca sufficienti misure tecniche di sicurezza e misure organizzative che regolino i processi da attuare, e che assicurano la conformità con queste misure.
2. **Sicurezza dei dati**: si dovrebbe prestare attenzione alle misure obbligatorie di sicurezza per i dati, che potenzialmente rendono soggetti o il fornitore cloud o il cliente a misure regolatrici e giuridiche laddove il contratto non indichi questi obblighi.
3. **Trasferimento dei dati**: si dovrebbe prestare attenzione a quali informazioni siano fornite al cliente relativamente a come i dati sono trasferiti all'interno del cloud proprietario del fornitore, al suo esterno, e all'interno ed esterno dell'Area Economica Europea.
4. **Accesso delle Forze dell'Ordine ai dati**: ogni nazione ha le proprie restrizioni in merito a, e requisiti che prevedono di, accedere ai dati da parte delle forze dell'ordine. Il cliente dovrebbe prestare attenzione a che le informazioni rese disponibili dal fornitore in merito alle giurisdizioni nelle quali i dati potrebbero essere immagazzinati e trattati, e valutare ogni rischio da esse risultante che potrebbe essere pertinente.
5. **Confidenzialità e non divulgazione:** dovrebbero essere considerati i doveri e gli obblighi connessi a questi aspetti.
6. **Proprietà intellettuale**: nel caso di IaaS e PaaS, la proprietà intellettuale, inclusi i lavori originali creati utilizzando l'infrastruttura cloud, potrebbero essere conservati. Il cliente cloud dovrebbe accertarsi che il contratto rispetti per quanto possibile i suoi diritti su ogni proprietà intellettuale o lavoro originale, senza compromettere la qualità del servizio offerto (ad esempio, i backup potrebbero essere una parte necessaria di un'offerta con un buon livello di servizio).
7. **Assegnazione del rischio e limitazione della responsabilità**: quando si rivedono i rispettivi obblighi contrattuali, le parti dovrebbero sottolineare quegli obblighi che presentano un significativo rischio per esse, includendo clausole di risarcimento monetario, o obblighi di

indennizzo, a favore della parte non inadempiente. Inoltre, ogni clausola standard che riguardi limitazioni di responsabilità dovrebbe essere valutata con attenzione.

8. **Cambio di controllo:** (dovrebbe essere considerata) la trasparenza in relazione alla capacità del fornitore cloud di onorare con continuità i propri obblighi contrattuali sia in caso di cambiamento nel controllo (societario), sia in ogni eventualità di rescissione del contratto.

Le raccomandazioni di natura legale sono generalmente qui espresse dal punto di vista del cliente cloud.

RACCOMANDAZIONI DI NATURA LEGALE ALLA COMMISSIONE EUROPEA

Si raccomanda che la Commissione Europea studi o chiarisca quanto segue:

- Alcune questioni connesse alla Direttiva sulla Protezione dei Dati e alle raccomandazioni di cui all'Articolo 29 del Data Protection Working Party richiedono chiarimenti. In particolare:
- In quali circostanze il fornitore cloud potrebbe essere classificato come Joint Controller;
- L'applicazione della Sezione 25[2] (2) della Direttiva sulla Protezione dei Dati come applicata al trattamento dei dati in Paesi fuori dall'Area Economica Europea durante il trasferimento dei dati da un fornitore cloud all'altro, o all'interno del cloud aziendale.
- L'impatto del trasferimento dei dati da e verso Paesi esterni all'Area Economica Europea, se questi Paesi non assicurano un adeguato livello di protezione dei dati.
- Se il concetto di "trasferimento dei dati" dovrebbe essere riesaminato alla luce degli avanzamenti tecnologici da quando la direttiva è stata

[2] La direttiva ePrivacy, così come riveduta nel 2009 (http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf), richiede agli Stati Membri di introdurre uno schema di notifica di brecce di sicurezza. Si noti che un tale schema sarà applicabile a reti di comunicazione elettronica e a servizi di comunicazione elettronica e non a servizi di società dell'informazioni quali i servizi di cloud computing

originariamente concepita, particolarmente alla luce di un approccio legale basato sulla responsabilità (ad esempio, come proposto dal progetto Galway (51)).

- Se il fornitore cloud dovrebbe essere obbligato a notificare ai propri clienti le brecce di sicurezza, e quali informazioni questi clienti dovrebbero essere tenuti a girare alla propria clientela. Ciò si potrebbe ottenere attraverso clausole contrattuali e perciò dovrebbe essere compreso quali mezzi siano maggiormente efficaci. Ad esempio, la legislazione sulla segnalazione delle brecce di sicurezza potrebbe essere di difficile applicazione e potrebbe persino agire come disincentivo alla trasparenza.
- Se sia necessario che gli Stati Membri chiariscano come si applicano ai fornitori cloud le esenzioni di responsabilità dell'intermediario secondo la Direttiva sull'eCommerce (articoli 12-15).
- Le differenze tra Stati Membri concernenti le leggi che regolano le richieste coercitive effettuate dalle varie autorità pubbliche per i dati conservati nel cloud, in particolare con uno sguardo a valutare le differenze del livello di protezione rispetto alle richieste governative di dati personali memorizzati su un sistema privato (casalingo o lavorativo), e di dati personali immagazzinati nel cloud

Come sia il miglior supporto per gli standard minimi di protezione dei dati e gli schemi di certificazione della privacy, basati sui concetti di responsabilità che sono comuni a livello globale o almeno comuni a tutti gli Stati Membri dell'EU.

Maggiori dettagli sulle cinque questioni di natura legale possono essere reperite nell'ALLEGATO I.

RACCOMANDAZIONI IN AMBITO RICERCA

Nel seguito si raccomandano alcune aree prioritarie di ricerca volte al miglioramento della sicurezza delle tecnologie del cloud computing:

COSTRUIRE LA FIDUCIA NEL CLOUD

- Processi di certificazione e standard per il cloud: più in generale, standard inerenti il ciclo di vita delle sicurezza nel cloud computing che possano essere certificati rispetto a disposizioni specifiche degli standard di governance - – COBIT(52), ITIL (53), ecc.
- Metriche per la sicurezza nel cloud computing
- Ritorno sugli investimenti in sicurezza (ROSI): quali misure il cloud computing può abilitare per migliorare l'accuratezza del ROI per la sicurezza;
- Gli effetti delle differenti forme di rendicontazione delle brecce di sicurezza;
- Tecniche per aumentare la trasparenza mantenendo adeguati livelli di sicurezza:
  - Etichettatura (tagging), ad esempio, tagging della località, tagging del tipo di dati, tagging secondo politiche
  - Salvaguardare la privacy relativa alla provenienza dei dati, ad esempio, tracciamento all'indietro dei dati attraverso i sistemi;
- Confidenzialità End-to-end dei dati nel cloud ed oltre:
  - Ricerca cifrata (sul lungo termine)
  - Schemi di elaborazione cifrati (sul lungo termine)
  - Strumenti per la cifratura e la confidenzialità per applicazioni social nel cloud
  - Trusted computing nel cloud, ad esempio, sequenze fidate di boot per stack di macchine virtuali;
- Cloud a elevata sicurezza, cloud privati virtuali, ecc.;

- Estensione del trust basato sul cloud ai dati e alle applicazioni basate presso il cliente

PROTEZIONE DEI DATI IN SISTEMI DI GRANDE SCALA CROSS-ORGANIZZAZIONALI

Le seguenti aree richiedono ulteriore ricerca nell'ambito del cloud computing:

- Distruzione dei dati e gestione del loro ciclo di vita
- Verifica di integrità – dei backup e degli archivi nel cloud e loro gestione delle versioni
- Analisi forense e tecniche di raccolta dei mezzi di prova
- Gestione degli incidenti – monitoraggio e tracciabilità
- Risoluzione delle dispute e disciplina dei mezzi prova
- Differenze internazionali nelle normative attinenti, incluse la privacy e la protezione dei dati
- Mezzi legali per facilitare il buon funzionamento delle infrastrutture cloud internazionali
- Mezzi automatizzati per la mitigazione di problemi con giurisdizioni differenti.

INGEGNERIA DEI GRANDI SISTEMI DI CALCOLO

- La sicurezza approfondita nei grandi sistemi distribuiti di calcolo;
- Servizi di sicurezza nel cloud – de-perimetrizzazione delle tecnologie di sicurezza e adattamento al cloud delle tecnologie tradizionali di sicurezza perimetrale, ad esempio: HSMs, filtri web, firewall, IDSs, ecc;
- Meccanismi di isolamento delle risorse – dati, elaborazione, memoria, logs, ecc.;
- Interoperabilità tra fornitori cloud;
- Portabilità delle VM, dei dati e impostazioni di sicurezza per le VM, da un fornitore cloud all'altro (per evitare il lock-in sul fornitore), e mantenimento di stato e sessione nei backup delle VM e migrazione live a lunga distanza di macchine virtuali;

- Standardizzazione delle interfacce per inviare dati, applicazioni e interi sistemi verso il cloud – così che ogni OS possa sviluppare la corrispondente interfaccia client;
- Approvvigionamento delle risorse (ampiezza di banda e CPU, ecc.) e loro allocazione secondo la scala (elasticità);
- Gestione scalabile della sicurezza (politiche e procedure operative) nelle piattaforme cloud:
  - applicazione automatica di politiche di protezione e sicurezza dei dati
  - processi operativi sicuri dei fornitori – l'implementazione dei processi di governance;
- resilienza del cloud computing – come migliorare la resilienza nel cloud:
  - utilizzo di architetture cloud lato client (edge networks, p2p, ecc.)
    - aggregazione di più reti client
    - ridondanza e backup client-based;
  - cloud bursting e resilienza su scala globale nel cloud.

Un'altra utile fonte di informazioni relativamente alle raccomandazioni in ambito ricerca sarà il report PROCENT (Priorities of Research on Current & Emerging Network Technologies), che dovrebbe essere pubblicato nel Dicembre 2009. Si invita a consultare il seguente link: http://www.enisa.europa.eu/act/res/technologies/procent

GLOSSARIO E ABBREVIAZIONI

AAA	Authentication, authorization and accounting
AD	Active directory
API	Application programming interface – specifica di interfaccia pubblicata dal fornitore di software
ARP	Address resolution protocol (2)
Asset	Nell'analisi di sicurezza è ciò che deve essere protetto (Ndt: il bene da proteggere)
Availability	La proporzione di tempo durante il quale un sistema può svolgere le proprie funzioni. Ndt: Disponibilità.
BS	British Standard
CA	Certification authority. Ndt: Autorità di certificazione
CC	Common Criteria (standard)
Confidentiality	Garantire che l'informazione sia accessibile solo agli autorizzati ad aver accesso. (ISO 17799). Ndt: Confidenzialità.
Co-residence	Condivisione di risorse hardware o software da parte di clienti cloud
CP	Cloud provider
CRL	Certificate revocation list. Ndt: Lista dei certificati revocati
CRM	Gestione della relazione con la clientela
Data controller	La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento dei dati personali; quando le finalità ed i mezzi del trattamento sono determinati da leggi nazionali o comunitarie o da regolamenti, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario.
Titolare del Trattamento	Una persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento.
Data subject	Persona fisica identificata o identificabile (si veda EU Directive 95/46/EC) Dalla quale sono raccolti i dati e/o della quali sono processati quei dati
DDoS	Negazione di servizio distribuita Ndt: Distributed denial of service
De-provision	Il processo che applica la rimozione di una risorsa dall'utilizzo oppure ne disabilita l'uso da parte di un insieme di utenti
Edge network	In questo contesto, una rete di computer che è in grado di trattare e immagazzinare dati per distribuirli in prossimità della destinazione finale

EDoS	Negazione del servizio di natura economica Ndt:Economic denial of service
Escrow	La conservazione di una risorsa da parte di un terzo che ha accesso a tale risorsa, quando alcune ben definite condizioni sono soddisfatte
FIM	Federated Identity Management. Gestione dell'identità federata
Guest OS	Un sistema operativo nel controllo del cliente cloud, che viene eseguito in un ambiente virtuale
Host OS	Il sistema operativo del fornitore cloud che esegue molteplici sistemi operativi guest
HSM	Hardware Security Module. Ndt:Modulo hardware di sicurezza
Https	Connessione HTTP che utilizza TLS o SSL
Hypervisor	Computer software o piattaforma software di virtualizzazione dell'hardware che consente l'esecuzione contemporanea di più sistemi operativi su un computer host
IDS	Intrusion detection system. Sistema di rilevamento intrusioni
Integrity	Proprietà per la quale i dati non sono stati intenzionalmente o accidentalmente alterati durante la conservazione o la trasmissione. Integrità
IP	Internet Protocol. Ndt: Protocollo internet
IPS	Intrusion Protection System. Ndt: Sistema di protezione dalle intrusioni
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control (indirizzo ethernet di un nodo di rete nel protocollo IP)
MITM	Man In The Middle (una forma di attacco)
MSS	Servizi di sicurezza gestiti. Ndt:Managed Security Services
NIS	Sicurezze delle reti e delle informazioni Ndt: Network and Information Security
NIST	National Institute of Standards and Technology (US)
Non-repudiation	Proprietà per la quale una delle parti della controversia non può ripudiare o confutare la validità di una dichiarazione o di un contratto (Ndt: non ripudio)
OCSP	Online Certificate Status Protocol
OS	Sistema Operativo
OTP	One-Time Password (tipo di token di autenticazione)

OVF	Open Virtualisation Format
Perimeterisation	Il controllo dell'acccesso a un bene o a un gruppo di beni. Ndt: perimetrizzazione
Port scan	Il sondare un host di rete per determinare quali porte siano aperte e quali servizi offra
Protection profile	Documento che specifica i criteri di valutazione di sicurezza per comprovare le affermazioni dei venditori per una data famiglia di prodotti di sistemi informativi (termine utilizzato nei Common Criteria). Ndt: profilo di protezione
Provision	Il rilascio di una risorsa
PV LAN	Private VLAN
QoS	Quality of service. Ndt: Qualità del Servizio
RBAC	Role-Based Access Control
Resilience	La capacità di un sistema di fornire e mantenere un livello di servizio accettabile a fronte di guasto (non intenzionale, intenzionale, o per cause naturali). Ndt: resilienza
ROI	Return On Investment. Ndt: ritorno dell'investimento
ROSI	Return On Security Investment. Ndt: ritorno dell'investimento in sicurezza
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTSM	Real Time Security Monitoring. Ndt: Monitoraggio di sicurezza in tempo reale.
Security target	Documento che specifica i criteri di valutazione di sicurezza per comprovare le affermazioni dei venditori riguardo alle proprietà di sicurezza del prodotto (termine usato nei Common Criteria).
Service engine	Il sistema responsabile per la fornitura dei servizi cloud. Motore del servizio
Side channel attack	Ogni attacco basato su informazioni acquisite dalla realizzazione fisica di un sistema, ad esempio, informazioni di tempo, consumo, perdite elettromagnetiche o persino suono possono fornire una ulteriore fonte di informazioni che può essere sfruttata per aver ragione del sistema.
SLA	Service level agreement. Ndt: Livelli di servizio
SSL	Secure Sockets Layer (utilizzato per cifrare il traffico tra i web server e i browser)
Subpoena	In questo contesto, un'autorità giudiziaria che confisca delle prove
TLS	Transport Layer Security (utilizzato per cifrare il traffico tra web server e browser)

ToU	Terms of Use. Ndt: Termini di Utilizzo
UPS	Uninterruptable Power Supply. Sorgente di potenza ininterrompibile.
VLAN	Virtual local area network
VM	Virtual machine. Ndt: Macchina virtuale
VPC	Virtual private cloud. Ndt: Cloud privato virtuale
VPN	Virtual private network. Ndt: Rete privata virtuale
Vulnerability	Qualsiasi circostanza o evento potenzialmente in grado di avere impatto negativo su un'attività, attraverso l'accesso non autorizzato, la distruzione, la divulgazione, la modifica dei dati, e / o la negazione del servizio. Vulnerabilità
XML	Extensible Mark-up Language

BIBLIOGRAFIA

(1) **IDC** *Cloud Computing 2010 - An IDC Update,* Frank Gens, Robert P Mahowald, Richard L Villars, Sep 2009 - Doc # TB20090929, 2009

(2) — Western European Software-as-a-Service Forecast, 2009–2013, David Bradshaw, Apr 2009 - Doc # LT02R9, 2009

(3) General Services Administration US - GSA [Online] http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=-24825&P=&contentId=28477&contentType=GSA_BASIC

(4) PCI Security Standards Council [Online] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

(5) NIST [Online] http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

(6) Wikipedia [Online] http://en.wikipedia.org/wiki/Cloud_computing

(7) Craig Balding *cloudsecurity.org.* [Online] http://cloudsecurity.org/2008/07/21/assessing-the-security-benefits-of-cloud-computing

(8) SUN - Project Kenai [Online] http://kenai.com/projects/suncloudapis/pages/HelloCloud#Examining_the_Virtual_Data_Center

(9) EC - European Commission [Online] http://ec.europa.eu/enterprise/policies/sme/small-business-act/index.htm

(10) ISO/IEC. ISO/IEC 27001:2008 *Information technology - Security Techniques - Information security risk management; Annex E: Information security risks assessment approaches,* 2008

(11) Wikipedia [Online] http://en.wikipedia.org/wiki/Open_Virtualization_Format

(12) MITRE [Online] http://cwe.mitre.org/data/definitions/400.html

(13) **BBC** [Online] http://news.bbc.co.uk/2/hi/uk_news/scotland/glasgow_and_west/6089736.stm

(14) www.retailresearch.org [Online] http://www.retailresearch.org/reports/fightinternalfraud.php

(15) **NY Daily News** [Online] 15. http://www.nydailynews.com/gossip/2009/08/23/2009-0823_outted_blogger_rosemary_port_blames_model_liskula_cohen_for_skank_stink.html

(16) **Enterprise Storage Forum** [Online] http://www.enterprisestorageforum.com/continuity/news/article.php/3800226

(17) **Electronic Discovery Navigator** [Online] http://www.ediscoverynavigator.com/statutesrules/

(18) **Find Law** http://technology.findlaw.com [Online] http://technology.findlaw.com/articles/01059/011253.html

(19) **CBS 11 TV** [Online] http://cbs11tv.com/local/Core.IP.Networks.2.974706.html

(20) **WIRED** www.wired.com/ [Online] http://www.wired.com/threatlevel/2009/04/company-caught/

(21) **Samuel T King, Peter M Chen, Yi-Min Wang, Chad Verbowsk, Helen J Wang, Jacob R Lorch** *SubVirt: Implementing malware with virtual machines.* 2006

(22) **Secunia** [Online] http://secunia.com/advisories/37081/

(23) — [Online] http://secunia.com/advisories/36389/

(24) **Kortchinsky, Kostya** http://www.immunityinc.com [Online] http://www.immunityinc.com/documentation/cloudburst-vista.html

(25) **Ormandy, Tavis** [Online] http://taviso.decsystem.org/virtsec.pdf

(26) **Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage** [Online] http://people.csail.mit.edu/tromer/papers/cloudsec.pdf

(27) **Gentry, Craig** [Online] http://delivery.acm.org/10.1145/1540000/1536440/p169-gentry.pdf?key1=1536440&key2=6166986521&coll=GUIDE&dl=GUIDE&CFID=60359435&CFTOKEN=10086693

(28) **Schneier, Bruce** [Online] http://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html

(29) www.spywarewarrior.com [Online] http://www.spywarewarrior.com/uiuc/ss/revoke/pgp- revoke.htm

(30) RSA Laboratories, PKCS#11 [Online] http://www.rsa.com/rsalabs/node.asp?id=2133

(31) Jun Zhou, Mingxing He [Online] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4716141

(32) Clulow, Tyler Moore and Jolyon [Online] http://people.seas.harvard.edu/~tmoore/ifipsec-pres.pdf

(33) Andrew Bechere, Alex Stamos, Nathan Wilcox [Online] http://www.slideshare.net/astamos/cloud-computing-security

(34) **Wikipedia** [Online] http://en.wikipedia.org/wiki/Token_bucket

(35) — [Online] http://en.wikipedia.org/wiki/Fair_queuing

(36) — [Online] http://en.wikipedia.org/wiki/Class-based_queueing

(37) Devera, Martin [Online] http://luxik.cdi.cz/~devik/qos/htb/old/htbtheory.htm

(38) Open Source Xen Community [Online] http://xen.org/

(39) Common Criteria Recognition Agreement (CCRA) [Online] http://www.commoncriteriaportal.org/

(40) **OWASP** [Online] http://www.owasp.org/index.php/OWASP_Top_Ten_Project

(41) — [Online] http://www.owasp.org/index.php/Category:OWASP_Guide_Project

(42) 27001:2005, ISO/IEC *Information technology -- Security techniques -- Information security management systems – Requirements*

(43) 27002:2005, ISO/IEC *Information technology -- Security techniques -- Code of practice for information security management*

(44) Group, BSI *BS 25999 Business Continuity*

(45) NIST *Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information* Systems

(46) OWASP [Online] http://www.owasp.org/index.php/Main_Page

(47) SANS Institute [Online] http://www.sans.org/reading_room/whitepapers/securecode/a_security_checklist_for_web_application_design_1389?show=1389.php&cat=securecode

(48) Software Assurance Forum for Excellence in Code (SAFECode) [Online] http://www.safecode.org

(49) IEEE Standards Association [Online] http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

(50) The European Privacy Seal [Online] https://www.european-privacy-seal.eu/

(51) EDRI - European Digital Rights [Online] http://www.edri.org/edri-gram/number7.2/international-standards-data-protection

(52) ISACA [Online] http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/COBIT_Publications/COBIT_Products.htm

(53) Office of Government Commerce (OGC) [Online] http://www.itil-officialsite.com/home/home.asp

(54) Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, Maik Lindner *A Break in the Clouds: Towards a Cloud Definitio*

(55) Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

(56) Jericho Forum, *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, April 2009,* http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

(57) Gartner, *Assessing the Security Risks of Cloud Computing,* June 2008, http://www.gartner.com/DisplayDocument?id=685308

(58) **Data Liberation Front**, Google, http://www.dataliberation.org/

ALLEGATO I – CLOUD COMPUTING – QUESTIONI GIURIDICHE

I. Sono state individuate cinque questioni giuridiche comuni a tutti gli scenari:

1. Protezione dei dati

    a. disponibilità ed integrità

    b. standard minimo o garanzia

2. confidenzialità

3. proprietà intellettuale

4. negligenza professionale

5. servizi in outsourcing e cambiamenti negli assetti societari

II. La maggior parte delle questioni individuate in questa disamina non riguarda solo il cloud computing. Infatti, i clienti di servizi di cloud computing possono trovare utile usare l'analisi giuridica applicata ad altri servizi Internet come base per la loro analisi giuridica dei rischi di sicurezza sollevati dal cloud computing. Per evitare di ripetere un'analisi preliminare, ci siamo concentrati su quegli aspetti della sicurezza del cloud computing che riteniamo attuali nuove sfide giuridiche o variazioni sostanziali all'analisi applicata alle tecnologie Internet precedenti.

III. Noi crediamo che una delle preoccupazioni dei potenziali clienti dei servizi di cloud sarà relativa alla protezione dei dati. Di conseguenza, in questa analisi giuridica ci siamo concentrati su questi temi in modo più dettagliato rispetto ad altri.

IV. Sebbene questo documento fissi cinque principali questioni giuridiche, un tema trasversale a tutti gli scenari e a tutte le discussioni sul cloud computing è la necessità, per i fornitori di cloud computing, di avere contratti estremamente dettagliati e per prodotti specifici nonché altri accordi e informazioni integrative, e per i clienti di esaminare attentamente tali contratti o la relativa documentazione. Entrambe le parti devono anche prestare

attenzione al Service Level Agreements (SLAs), senza ritenere che una molteplicità di problematiche legali associate al cloud computing, sia risolta o mitigata dagli SLAs.

V. Prima di entrare nei dettagli giuridici, vale la pena notare che i clienti cloud provider possono variare nel tipo (da privati a enti pubblici) e nelle dimensioni (dalle PMI alle grandi imprese) e, quindi, nella misura in cui essi sono in grado di negoziare. Questo è molto rilevante dal punto di vista giuridico, perché il rapporto tra i fornitori cloud e i loro clienti sarà per lo più regolato attraverso i contratti. A causa della mancanza di normative specifiche, gli obblighi e i doveri reciproci sono sia determinati in termini e condizioni generali standard, unilateralmente predisposti dal fornitore cloud, e verranno (più comunemente) semplicemente accettati dai clienti senza modifiche o negoziati in specifici accordi.

VI. La tabella seguente riassume le tre possibilità in termini di negoziazione dei contratti e degli accordi tra il cliente e il fornitore cloud.

FORNITORE CLOUD	**CLIENTE**
A) Grande azienda – **forte capacità di negoziare clausole contrattuali**	PMI – **Scarsa o assente capacità di negoziare clausole contrattuali**
B) Sia il cliente che il fornitore **sono in grado di negoziare clausole contrattuali**	
C) PMI – **Scarsa capacità di negoziare clausole contrattuali**	Grande azienda o pubblica amministrazione – **possono negoziare clausole contrattuali**

A seconda del caso particolare (se si tratta di A, B o C), il modo di affrontare le questioni individuate nel comma I possono differire in modo significativo.

VII. E' importante distinguere tra il caso di una piccola o media organizzazione, che debba scegliere tra i vari contratti offerti sul mercato, e un'organizzazione più grande, che sarebbe in grado di negoziare le clausole. E' prevedibile che il principale vantaggio commerciale del cloud computing sarà che il cloud computing diverrà probabilmente un servizio di massa, o merce, che può essere acquistato a breve termine o sulla base del pay-per use (ad esempio, il caso A: un grosso fornitore cloud – un cliente PMI). Ciò presuppone

la standardizzazione dei servizi e quindi delle condizioni giuridiche. Pertanto, nell'analisi giuridica in questo documento, vengono descritti in primo luogo i problemi dal punto di vista delle piccole e medie imprese che valutino i diversi contratti, SLA, ecc., offerti sul mercato.

Tuttavia, ci possono essere situazioni in cui i servizi di cloud computing saranno su misura per clienti di grandi dimensioni, cioè, grandi aziende e amministrazioni pubbliche (ad esempio, caso B). Questo presuppone specifici, contratti su misura. Il caso C è probabile che sia meno comune. In questo caso, ci sarà spazio per i negoziati, come nel caso B. Le organizzazioni più grandi possono tuttavia utilizzare le stesse considerazioni nella negoziazione dei contratti. Per questo motivo abbiamo inserito una disamina di raccomandazioni per la negoziazione, ove ciò sia possibile.

E' anche interessante notare che anche quando un cliente non può negoziare i termini di un contratto con un provider specifico, *egli è ancora libero di scegliere tra offerte alternative sul mercato. Nel caso di una PMI, quindi, le raccomandazioni per specifiche clausole contrattuali devono essere inteso in termini di preferenze tra le offerte presenti sul mercato*.

VIII. L'analisi che segue coglie ed evidenzia come queste cinque principali questioni giuridiche possono essere affrontate attraverso i tre diversi scenari di contrattazione di cui al paragrafo VI.

1. Protezione dei dati

Questa sezione si occupa di questioni giuridiche di protezione dei dati che spesso sorgono con l'uso di un servizio di cloud computing, e mira a fornire indicazioni in base alla formulazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 sulla protezione delle persone con riguardo al trattamento dei dati personali e sulla libera circolazione di tali Dati[3] (in prosieguo: la " "Data Protection Directive"). Tuttavia, poiché tali questioni saranno direttamente governate da leggi nazionali di attuazione della direttiva

3 Il testo ufficiale della Direttiva 95/46/EC e lo stato dell'implementazione è disponibile a http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

sulla protezione dei dati, i clienti di servizi di cloud computing sono invitati a riesaminare tali questioni sulla base all'applicazione del diritto nazionale.

Glossario

Le seguenti definizioni sono contenute nella *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati* (di seguito: la 'direttiva protezione dati').

Dati personali: qualsiasi informazione concernente una persona fisica identificata o identificabile ('persona interessata'); una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più fattori specifici alla sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare la salute e la vita sessuale.

Trattamento dei dati personali (Processing): si intende qualsiasi operazione o insieme di operazioni compiute su dati personali, con o senza l'ausilio di processi automatizzati, come la raccolta, registrazione, organizzazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, blocco, cancellazione o distruzione.

Titolare: la persona fisica o giuridica, autorità pubblica, di servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali, dove le finalità dei mezzi del trattamento sono determinati da leggi nazionali o comunitari o regolamentari,

il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario.

Incaricato: una persona fisica o giuridica, autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del titolare.

Definizione dei problemi

1.1. Considerando che i servizi forniti da provider di cloud consistono generalmente in email, messaggistica, desktop, gestione progetti, buste paga, contabilità e finanza, CRM, gestione delle vendite, sviluppo di applicazioni personalizzate, applicazioni personalizzate, telemedicina, e fatturazione dei clienti, saranno trattati dati personali (inclusi i dati sensibili). Questi dati possono appartenere a un numero di persone (persone interessate), ad esempio, dipendenti, clienti, fornitori, pazienti e, più in generale, i partner commerciali.

1.2 Dato per scontato che vengano trattati dati personali, è importante però capire esattamente quando applicare la Direttiva sulla Protezione dei Dati. La Sezione 4 recita: '1. Ciascuno Stato membro applicherà le disposizioni nazionali in conformità alla presente Direttiva al trattamento di dati personali laddove: (a) il trattamento è effettuato nel contesto delle attività di un'azienda del responsabile del trattamento nel territorio dello Stato Membro; qualora uno stesso titolare del trattamento insiste nel territorio di diversi Stati Membri, esso deve adottare le misure necessarie per assicurare che ciascuna delle aziende sia aderente agli obblighi derivanti dal diritto Nazionale. (b) il titolare non è stabilito nel territorio dello Stato Membro, ma in un luogo dove si applichi il diritto nazionale in virtù del diritto pubblico internazionale; (c) il titolare non dimora nel territorio comunitario e, ai fini del trattamento di dati personali, fa uso di strumenti, automatizzati o non automatizzati, situati nel territorio dello Stato Membro, a meno che queste (attrezzature) non siano utilizzate solo ai fini di transito attraverso il territorio della Comunità.'

1.3 Da un'analisi della sezione 4 della Direttiva sulla protezione dei dati, ne consegue che:

a) il luogo in cui è stabilito il titolare è rilevante ai fini dell'applicazione della Direttiva sulla protezione dei dati
b) ciò che non è rilevante per l'applicazione della Direttiva sulla protezione dei dati è il luogo di trattamento dei dati personali o la residenza della persona interessata.

1.4 La Direttiva sulla protezione dei dati sarà quindi applicata sia se il titolare è stabilito nell'UE, sia se il titolare non è stabilito nella UE, ma utilizza attrezzature situate nella UE per il trattamento dei dati personali (ad esempio, i centri di dati per la memorizzazione e l'elaborazione remota dei dati personali situato nel territorio di uno Stato Membro, calcolatori, terminali, server), a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità[4].

1.5 Una volta stabilito che la Direttiva per la protezione dei dati viene applicata, la domanda successiva è: chi è il titolare e chi l' incaricato? Se il cliente del fornitore cloud determina le finalità e gli strumenti del trattamento di dati personali è il controller e, se il fornitore cloud elabora dati personali per conto del suo cliente, è un Incaricato esterno[5]. Infatti, la qualificazione di un Incaricato o Titolare è molto diversa per quanto riguarda i doveri e gli obblighi di conformità e le relative responsabilità. Nella nostra analisi si assume che il cliente del fornitore cloud è il titolare e il fornitore cloud è un incaricato esterno.

4 Per un'ulteriore guida alla costituzione e uso di strumenti e fattori determinanti l'applicabilità della Direttiva Protezione Dati, si veda l' Articolo 29 di Data Protection Working Party's opinions on online social networking and search engines – rispettivamente Opinion 5/2009 on online social networking; Opinion 1/2008 on data protection issues related to search engines; disponibili a: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm.

5 Esterno perché nel caso specifico il Processor è un soggetto esterno all'organizzazione/azienda del Controller.

1.6 Le funzioni principali e gli obblighi per il Titolare previsti nella Direttiva sulla protezione dei dati sono i seguenti:

a) trattamento dei dati personali secondo i principi di correttezza, liceità, finalità, adeguatezza, proporzionalità, necessità e "minimazione" dei dati (art. 6 della Direttiva sulla protezione dei dati);

b) Ottenimento del consenso inequivocabile dell'interessato, di cui al comma a. dell'articolo 7 del 95/46[6];

c) trattamento dei dati personali dopo aver fornito agli interessati le necessarie informazioni (art. 10 della Direttiva sulla protezione dei dati);

d) garantire alla persona interessata il diritto di cui alla sezione 12 della Direttiva sulla protezione dei dati - ad esempio, per ottenere la conferma dell'esistenza o meno di dati relativi alla persona interessata in fase di elaborazione, per ottenere informazioni sulle finalità del trattamento, le categorie di dati interessati, i destinatari o le categorie di destinatari a cui vengono comunicati i dati; per rettificare, cancellare o il bloccare i dati trattati in un modo che non è conforme alle disposizioni della direttiva; ecc - (art. 12 della protezione dei dati Direttiva);

6 L'Articolo 7 della Direttiva 95/46 directive recita: gli Stati Membri faranno in modo che i dati personali possano essere trattati solo se:

(a) Il soggetto dei dati ha fornito il proprio consenso in modo non ambiguo; oppure

(b) il trattamento è necessario per l'esecuzione di un contratto di cui il soggetto dei dati è parte o al fine di adottare le misure richieste dalla persona interessata prima della conclusione del contratto; oppure

(c) il trattamento è necessario per adempiere a obblighi legali ai quali il titolare è assoggettato; oppure

(d) il trattamento è necessario al fine di proteggere gli interessi vitali della persona interessata; oppure

(e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti al responsabile del trattamento o di una terza parte a cui vengono comunicati i dati; oppure

(f) il trattamento sia necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da terze parti o soggetti cui vengono comunicati i dati, a meno che tali interessi non vengano scavalcati da interessi relativi a diritti e libertà fondamentali della persona interessata che richiedono tutela ai sensi dell'articolo 1 (1).

e) attuare misure di sicurezza tecniche e organizzative per proteggere i dati personali contro la perdita accidentale, alterazione, divulgazione o accesso non autorizzati e contro tutte le altre forme di trattamento illecito (art. 17 della direttiva sulla protezione dei dati);

f) scegliere un incaricato che offra garanzie sufficienti per quanto riguarda le misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare, e garantire il rispetto di tali misure;

g) il trasferimento di dati personali a paesi terzi che non garantiscono un livello di protezione adeguato ai sensi della Sezione 25 (2) della Direttiva sulla protezione dei dati solo nel caso in cui la persona interessata abbia dato il previo consenso in maniera inequivocabile al trasferimento previsto o sotto la condizione che altre procedure siano messe in atto ai sensi dell'articolo 26 (per esempio, 'clausole contrattuali tipo' o - se i dati sono trasferiti negli Stati Uniti -'Safe Harbor Principles').

1.7 Il titolare del trattamento (in questa analisi, il cliente cloud) dovrebbe fornire agli interessati (utenti finali del cliente cloud) tutte le informazioni obbligatorie relative al trattamento dei dati. Il cliente cloud dovrà, ai sensi della Direttiva sulla protezione dei dati, informare i loro clienti circa le circostanze del trasferimento al provider cloud, la qualità del fornitore cloud (cioè, processore esterno), e le finalità del trasferimento. In realtà, esternalizzare i servizi di cui sopra al punto 1.1 implica necessariamente la comunicazione e il trasferimento di tali dati a terzi parti[7] (cioè, i fornitori di cloud),[8]che possono trovarsi in Europa, ma anche nei paesi al di fuori dello Spazio economico europeo (terzi-paesi). Questi paesi potrebbero non offrire un adeguato livello di protezione dei dati personali ai sensi della Sezione 25 della

7 Si noti che in qualche legislazione nazionale (ad es. nel Data Protection Act tedesco) i termini “trasferimento” e “terze parti” vengono definiti *termini legali* i quali comportano specifiche implicazioni legali. L'uso di questi termini qui non significa comportare tali implicazioni.

8 Sfortunatamente non sembra esserci una definizione ufficiale di trasferimento dei dati. In ogni caso dalla Sezione 4 della Direttiva 95/46/EC è possibile dedurre che il transito di dati attraverso i territori non è rilevante dal punto di vista giuridico. Per esempio, se i dati sono trasferiti dalla Gran Bretagna agli USA, in ogni caso il flusso dei dati attraverso i link di rete che corrono lungo Islanda, Groenlandia e Canada sembra essere irrilevante sotto il profilo giuridico.

Direttiva sulla protezione dei dati. E' fondamentale che coloro che raccolgono dati soggetti alla Direttiva sulla protezione dei dati comprendano l'applicazione della Direttiva per l'uso e il trasferimento di tali dati. A questo proposito, ai titolari non attualmente coinvolti nel cloud computing si consiglia di chiedere il consenso informato degli interessati al trattamento dei dati per il trasferimento al di fuori dello Spazio economico europeo. A coloro che attualmente sono impegnati in cloud computing si consiglia di assicurare che questo consenso sia in loro possesso e che descriva in modo adeguato la natura e la portata del trattamento e il trasferimento. L'alternativa sarebbe quella di disporre di una delle procedure di cui alla Sezione 26 (ad esempio, "clausole contrattuali tipo Safe Harbor Principles" - se i dati sono trasferiti negli Stati Uniti e il provider cloud partecipa a tale programma). In realtà, la seconda modalità presenta alcuni vantaggi in quanto il consenso, sul trasferimento, può essere ritirato in qualsiasi momento dal soggetto interessato.

1.8 Si raccomanda che la Commissione chiarisca l'applicazione della sezione 25 (2) della Direttiva per quanto attiene al possibile trattamento di dati in paesi al di fuori dello Spazio economico europeo durante il suo trasferimento da un provider di cloud computing ad un altro, o all'interno di una determinata società Cloud, qualora quel Cloud si trovasse in molteplici giurisdizioni, ma con una giurisdizione al di fuori dello Spazio economico europeo.

1.9 Tutte le parti coinvolte nel trattamento dei dati (dati, soggetti titolari e incaricati) dovrebbero conoscere i loro rispettivi diritti e obblighi relativi al trattamento dei dati, ai sensi della Direttiva sulla protezione dei dati e dei relativi strumenti di legge con i quali la Direttiva è stata attuata nei vari Stati membri dell'UE[9]. Inoltre, quei soggetti dovrebbero anche comprendere il diritto per il rispetto della vita privata di cui all'articolo 8 della Convenzione Europea dei diritti fondamentali dell'uomo e delle libertà di cui i Paesi coinvolti sono

9

Si veda "Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data", consultabile a http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#italy.

firmatari o che hanno sottoscritto nella propria legislazione. Per applicare la Direttiva sulla protezione dei dati in modo adeguato, è fondamentale avere la disponibilità e l'integrità dei dati, e questo fa nascere l'analisi sulle misure di sicurezza dei dati. Ciò porta a inevitabili compromessi. Più sicurezza dei dati rischia di portare a ridurre la disponibilità. Il cliente può quindi voler dare un'occhiata da vicino alle misure di sicurezza che il cloud provider ha in atto e alla garanzia della disponibilità dei dati. Si deve tener presente che nella maggior parte dei paesi europei ci sono requisiti obbligatori in materia di sicurezza dei dati. Il cliente dovrà assicurarsi che tali misure siano rispettate. In alcuni casi (eHealth e, possibilmente, elasticità, quando i dati sensibili e dati finanziari vengono elaborati) il cliente può anche voler maggiori garanzie sulle misure di sicurezza per la memorizzazione di dati, la comunicazione o il trasferimento, disaster recovery dei dati e poi trasferimento.

1.10. Deve essere chiaro a questo punto che il cliente - se classificato come unico titolare del trattamento - sarà l'entità responsabile del trattamento dei dati personali delle persone interessate. Il cliente sarà inoltre responsabile di questi dati quando tale trattamento è effettuato dal provider di servizi cloud nel ruolo di incaricato esterno. Il mancato rispetto della Direttiva sulla protezione dei dati può portare a sanzioni amministrative, civili e anche penali, che variano da paese a paese, per il titolare del trattamento. Tali sanzioni sono per lo più individuate in rilevati strumenti normativi con i quali la Direttiva 95/46/CE è stata attuata nei vari Stati membri dell'UE.

Affrontare le questioni

1.11. Tutti i temi sopra evidenziati possono essere trattati contrattualmente. Oltre a garantire la raccolta di tutti i dati personali nel rispetto delle sezioni 7 e 10 della Direttiva sulla protezione dei dati, ad esempio avendo precedentemente informato gli interessati ed aver ottenuto il loro consenso (se richiesto dalla sezione 7), il cliente cloud dovrebbe verificare la presenza di una clausola di protezione dei dati nel contratto tra lui stesso ed il fornitore di cloud. Questa clausola dovrebbe esporre i doveri e gli obblighi delle parti interessate. Il cliente cloud dovrebbe considerare quanto segue nella valutazione di tali clausole:

a. Tenendo presente che il cliente Cloud è classificato come un titolare di dati ai sensi della normativa UE sulla protezione dei dati ed è anche legalmente responsabile per la correttezza, liceità, finalità, ecc., dovrebbero essere ricercate delle clausole che sostengono la conformità del cliente con i principi della Direttiva sulla Protezione dei Dati.

b. Il provider cloud dovrebbe collaborare con il titolare, al fine di assicurare che quest'ultimo possa effettivamente garantire i diritti della persona interessata conformemente alla Sezione 12 della Data Protection Directive.

c. Il cloud provider dovrebbe disporre di adeguate misure di sicurezza ai sensi dell'articolo 17 e il provider di servizi cloud dovrebbe avvertire tempestivamente il titolare di qualsiasi violazione della sicurezza dei dati e cooperare per risolvere rapidamente il problema.

d. I trasferimenti di dati personali, verso paesi terzi, che non garantiscano un livello di protezione adeguato ai sensi della Sezione 25(2) della Direttiva, dovrebbero essere preventivamente autorizzati dall'interessato, in conformità con la Sezione 26 (per esempio 'clausole contrattuali tipo' o 'Safe Harbor Principles "- se i dati sono trasferiti negli Stati Uniti ed il fornitore cloud partecipa a tale programma). E' importante ricordare che il cloud computing può avere a oggetto il trasferimento di dati. Questo problema non è facile da risolvere contrattualmente. Si raccomanda alla Commissione Europea che venga affrontata la questione.

1.12. **Si noti che nel caso A** (*cfr.* Introduzione, paragrafo VI), il contratto, compresa la clausola di protezione dei dati, viene elaborato dal cloud provider per l'impossibilità di negoziazione contrattuali tra un provider di grandi dimensioni e numerosi piccoli clienti. Quindi, il potenziale cliente dovrebbe analizzare con attenzione quanto prescritto, per determinare se la clausola fornisce al cliente garanzie sufficienti in merito al trattamento dei dati da parte del cloud provider, e preveda rimedi adeguati per danni contrattuali.

1.13. **Nei casi B e C** (*cfr.* Introduzione, paragrafo VI), la clausola di protezione dei dati sarà oggetto di trattativa. Inoltre, le misure di sicurezza possono essere trattate negli allegati e nello SLA. Nell'affrontare questioni di sicurezza,

le parti dovrebbero tenere a mente che possono non essere in grado di descrivere dettagliatamente tutte le misure di sicurezza da affrontare. Poiché la sicurezza IT è una continua corsa nell'affrontare nuove problematiche, i termini contrattuali devono essere liberi di seguire quest'evoluzione.

1.14. **Nei casi B e C (negoziazione di appalti di valore elevato)**, può anche essere opportuno per il cliente negoziare soluzioni adeguate per i danni contrattuali qualora venisse disattesa la clausola relativa alla protezione dei dati. In ultimo, ma non di minor importanza, se la violazione del fornitore cloud è significativo, può essere inclusa nella lista dei casi che portano alla risoluzione unilaterale del contratto.

1.15. Se il fornitore cloud si trova in un paese al di fuori dello Spazio economico europeo e questo paese non offre un adeguato livello di protezione dei dati, è consigliabile mettere in atto procedure in conformità con la Sezione 26 (ad esempio, 'clausole contrattuali tipo sicurezza Harbor Principles' - se i dati sono trasferiti negli Stati Uniti e il fornitore cloud partecipa a questo programma), anziché basare il trasferimento sul consenso della persona interessata (per il motivo indicato in 1.7). Tuttavia, va sottolineato che il trasferimento dei dati all'interno del territorio degli Stati membri non è scevro da problemi. Infatti, nonostante i dati personali possano circolare liberamente all'interno degli Stati membri, le leggi non sono coerenti tra paesi. Tale incoerenza crea delle difficoltà evidenti nel rispetto (della legislazione) e, quindi, nelle questioni di responsabilità. Si auspica che la Commissione prenda provvedimenti verso la standardizzazione dei requisiti minimi di protezione dei dati in Europa. Ciò è particolarmente importante in considerazione del fatto che la Direttiva sulla protezione dei dati è attualmente oggetto di revisione. Inoltre, una certificazione basata sulle norme minime di protezione dei dati, che siano comuni in tutti gli Stati membri, può essere estremamente utile.

2. Riservatezza

Definizione delle problematiche

2.1. Preoccupazioni sulla riservatezza vengono sollevate anche dagli scenari considerati dal presente documento. In effetti, informazioni riservate e 'know-how' possono essere trattati nel Cloud. Ogni perdita di informazioni causata da comunicazione volontaria del fornitore Cloud all'interno del proprio Cloud violando la sicurezza può compromettere l'operatività/i servizi del cliente. NB in questo contesto è fondamentale distinguere tra trattamento dei dati nelle operazioni di elaborazione, e la conservazione o la trasmissione dei dati senza alterazioni, in quanto la trasformazione, in questo senso, richiede di solito che i dati siano in forma non cifrata.
2.2. Può essere utile approfondire il concetto di know-how e di come proteggerlo.

Know-how è definito come un insieme di informazioni segrete, sostanziali ed identificate, in ogni appropriata forma[10]. Il termine "segreto" implica che il know-how, considerato globalmente o nella precisa configurazione e composizione dei suoi componenti, non è generalmente noto, né facilmente accessibile. Il termine "identificato" intende che il know-how è descritto o registrato in modo tale da consentire di verificare se risponde ai criteri di segretezza e di sostanzialità. A questo scopo "sostanziale" significa che il know-how include informazioni che sono importanti per la totalità o una parte significativa di:

i un processo produttivo, o

ii un prodotto o servizio, o

iii importante per lo sviluppo in sé ed esclude informazioni ovvie

10 Si veda *Commission Regulation (EC) No 772/2004 del 27 April 2004 sull'applicazione dell'Articolo 81(3) del Trattato delle categorie di accordi al trasferimento di tecnologie*

2.3. Non sembrano esistere normativi Europee applicabili a tali scenari. Le normative europee in materia di know-how, di cui alla precedente definizione, si applicano essenzialmente a licenze e attività che riguardano il trasferimento e lo sfruttamento delle informazioni.

Affrontare le questioni

2.4. Tenendo a mente le normative, e al fine di preservare il valore economico del know-how e di informazioni segrete, in generale, compresi risultati della ricerca, e informazioni relative al progetto e a clienti, è consigliabile che i clienti cerchino condizioni contrattuali che coprano questi problemi. In realtà, parte dei doveri e degli obblighi da preservare come valore devono essere specificamente affrontati in una "clausola di riservatezza/non divulgazione". Particolare attenzione dovrebbe essere prestata ai confini delle responsabilità delle parti e alle relative passività. Gli allegati tecnici possono essere di aiuto nel risolvere questo aspetto.

2.5. **Nel caso A**, il potenziale cliente del provider cloud dovrebbe analizzare con attenzione la clausola di riservatezza/non-divulgazione per determinare se il fornitore cloud offre garanzie sufficienti per proteggere le informazioni segrete del cliente e il know-how che circolano nel cloud.

2.6. **Nei casi B e C**, si consiglia che le parti negozino una disposizione che rifletta il danno che una parte dovrebbe sostenere se le informazioni riservate venissero divulgate. Se la comunicazione è importante, tale violazione può essere inclusa nella lista dei casi che consentono alla società di rescindere unilateralmente il contratto.

3. Proprietà intellettuale

Definizione dei problemi

3.1 La proprietà intellettuale può essere a rischio anche in uno scenario di Cloud Computing.

3.2 Sebbene un'entità che affida dei servizi in outsourcing a un fornitore cloud possa proteggere e far valere i propri diritti di proprietà intellettuale mediante la normativa, che è simile in tutti gli Stati Membri Europei, una violazione dei diritti di proprietà intellettuale può provocare danni immediati, che non saranno mai completamente risarciti in un procedimento legale.

3.3 Inoltre, vi è il caso improbabile che le interazioni tra il cliente e il fornitore cloud, ad esempio, in fase di negoziazione, che sarà possibile nel caso B o C - possano dar luogo a risultati comuni che possono essere oggetto di diritti di proprietà intellettuale (per esempio, migliori tecniche per la gestione dei dati). Pertanto, è opportuno stabilire chi sarà il proprietario di tali diritti prima di impegnarsi in attività di cloud computing, e in seguito determinare l'uso dei diritti tra le parti.

Affrontare le questioni

3.4 I diritti di proprietà intellettuale dovrebbero essere disciplinati attraverso apposite clausole contrattuali: "clausola di Proprietà Intellettuale" e "Riservatezza / clausola di non divulgazione"[11].

3.5 **Nel caso A**, il potenziale cliente del fornitore cloud dovrebbe valutare attentamente il valore della sua proprietà intellettuale e i rischi derivanti da servizi di cloud computing. Dopo averlo fatto, il cliente deve esaminare attentamente tutte le clausole che regolano la proprietà intellettuale per determinare se il fornitore cloud offra sufficienti garanzie e permetta ai clienti l'utilizzo di strumenti adeguati per proteggere le proprie informazioni (ad esempio, attraverso la crittografia dei dati), per proteggere i beni del cliente. Il cliente Cloud dovrebbe accertarsi che il contratto rispetti i suoi diritti di

[11] *Per quanto riguarda la "Riservatezza / clausola di non divulgazione", si applica quanto al precedente 2.4*

proprietà intellettuale, per quanto possibile senza compromettere la qualità del servizio offerto (ad esempio la creazione di copie di backup può essere una parte necessaria dell'offerta di un buon livello di servizio).

3.6 **Nei casi B e C**, la "clausola di proprietà intellettuale" deve contenere dettagliatamente le norme stabilite per affrontare le questioni di cui al precedente 3.3. Inoltre, è consigliabile che il cliente negozi una clausola in cui il fornitore cloud venga penalizzato se le disposizioni in materia di proprietà intellettuale vengano violate. La sostanziale violazione da parte del fornitore cloud può essere uno degli elementi inclusi nella lista dei casi che consentono alla società di rescindere unilateralmente il contratto.

4. Negligenza professionale

Definizione delle problematiche

4.1 Errori nei servizi di outsourcing da parte del cloud provider possono causare un impatto significativo sulle capacità del cliente di soddisfare obblighi e doveri nei confronti dei propri clienti. Il cliente può così essere esposto a responsabilità contrattuali sulla base di negligenza nei confronti dei propri clienti

4.2. Errori da parte del cloud provider comportano anche la responsabilità da parte del cliente nei confronti dei propri dipendenti. Poiché il cliente affida in outsourcing tecnologie che forniscono e sostengono funzioni interne critiche, quali posta elettronica, messaggistica, applicazioni da ufficio, gestione dei progetti e delle paghe, dall'insufficienza del fornitore cloud ne consegue l'impossibilità da parte dei dipendenti di accedere a queste funzioni o ai dati da loro stessi elaborati, comportando responsabilità del cliente nei confronti dei propri dipendenti.

4.3. Un problema collegato è se i termini contrattuali attribuiscono delle responsabilità al cliente per eventuali atti illegali svolti autenticandosi con le credenziali del cliente, in un account non correntemente gestito dal cliente stesso.

Affrontare le questioni

4.4. **Nel caso A**, il cliente deve esaminare attentamente e verificare la sostenibilità degli (standard) di limitazione/esclusione della clausola di responsabilità in favore del fornitore cloud.

4.5. **Nei casi B e C (ovvero, nel caso raro in cui sono negoziati contratti di valore elevato)**, si raccomanda che il cliente sposti la sua responsabilità per le questioni di cui sopra, per quanto possibile, verso il fornitore cloud, possibilmente senza incorrere in costi più elevati. Ciò può essere conseguito con clausole del tipo "Limitazione di responsabilità" e "indennizzo". Sostanzialmente questo tipo di violazione da parte del fornitore

cloud può essere incluso nella lista delle istanze che consentono al cliente la rescissione unilaterale del contratto. Va notato, tuttavia, che il titolare rimane sempre legalmente responsabile, in base alle disposizioni della Direttiva Protezione Dati (1) (1), indipendentemente da eventuali clausole contrattuali, per eventuali i danni alle persone interessate.

4.6. Si raccomanda che la Comunità Europea rediga un chiarimento su come si applichino le deroghe di responsabilità per l'intermediario al caso dei fornitori cloud.

5. Servizi di outsourcing e cambiamenti nel controllo (societario)

Definizione delle problematiche

5.1 L'accordo tra l'azienda e il fornitore cloud può essere definito come un contratto *intuitu personae*. Un *intuitu personae* è un contratto che le parti scelgono di stipulare basandosi sulle qualità uniche dell'azienda. Ad esempio, un cliente può scegliere un determinato fornitore di servizi Cloud in base alla sua offerta, alla sua reputazione e professionalità, o per le sue competenze tecniche. Come risultato, il cliente potrebbe essere restio ad accettare che tutto o parte di quei servizi vengano, a loro volta, affidati in outsourcing ad altri dal fornitore cloud.

5.2 Il controllo (societario) del fornitore cloud può anche cambiare e, di conseguenza, anche i termini e le condizioni dei servizi forniti.

Affrontare le questioni

5.3 **Nel caso A**, si raccomanda che il cliente determini se il fornitore cloud affidi servizi in outsourcing e se il fornitore cloud fornisca garanzie e assicurazioni in relazione alle prestazioni di tali servizi dati in outsourcing. Tuttavia, non è consigliabile che il cliente sia in grado di limitare il ricorso all'outsourcing da parte del fornitore cloud. Si raccomanda inoltre che il contratto venga riesaminato per determinare come il fornitore cloud provider debba comunicare i cambiamenti al cliente. Il cliente può anche prendere in considerazione che il contratto preveda il diritto di recesso in caso si verifichi un cambiamento nella catena di controllo.

5.4 **Nei casi B e C**, il cliente *può* scegliere di richiedere che il ricorso all'outsourcing da parte del fornitore cloud sia soggetto ad autorizzazione preventiva da parte del cliente stesso. Per prendere tali decisioni, il cliente dovrà essere informato sul tipo di servizi che il fornitore cloud intende affidare in outsourcing e verso quale società ciò sarà effettuato. Anche se il cliente accetta il ricorso all'outsourcing, potrebbe volere che il fornitore cloud fornisca

delle assicurazioni o garanzie connesse alle prestazioni dei servizi affidati in outsourcing. Sulla stessa linea di ragionamento, il cliente può anche voler avere la possibilità di approvare una modifica del controllo (societario) o di annullare o rinegoziare il contratto in caso di cambiamento nel controllo (societario) del fornitore cloud. Tali opzioni possono essere attentamente specificate nel contratto tra l'azienda e il fornitore cloud per mezzo di un 'third-party outsourcing', una clausola 'garanzie e indennizzi', una 'cambio di controllo', o una clausola di 'risoluzione del contratto ' - sempre a seconda del potere contrattuale delle parti.

Conclusioni

Tutte le clausole contrattuali dalla sezione 1 alla sezione 3 possono essere adattate per la standardizzazione, ad eccezione delle relative penali, che dipendono dal potere contrattuale delle parti. Considerando che il contenuto recondito delle clausole contrattuali di cui ai punti 4 e 5 dipende dal potere contrattuale delle parti, queste sono meno adatte per la standardizzazione.

ALLEGATO II – SCENARIO DI CASO D'USO PMI

PROSPETTIVA DELLA PICCOLA E MEDIA IMPRESA SUL CLOUD COMPUTING

Valutazione del rischio di sicurezza del cloud computing di ENISA

Questo scenario è stato usato come base per l'analisi dei rischi pubblicata nel rapporto.

Limiti e ipotesi

Questo scenario si basa parzialmente sui risultati del sondaggio: delle PMI in prospettiva del Cloud Computing [REF]. Lo scenario NON vuole essere una road map per una società che sta valutando, pianificando o eseguendo progetti e investimenti di cloud computing.

La scelta di utilizzare un'azienda di medie dimensioni è stata fatta per garantire la valutazione di un livello elevato di complessità in termini di IT, legali e commerciali. L'obiettivo era quello di esporre tutti i possibili rischi di sicurezza. Alcuni di questi rischi sono specifici per medie imprese, altri sono rischi generali che ogni impresa micro, piccola o media che sia, deve affrontare quando avviene la migrazione a un ambiente di cloud computing.

Lo scenario NON è destinato a essere completamente realistico per una singola organizzazione, ma tutti gli elementi dello scenario è probabile che si verifichino di frequente in molte organizzazioni; attualmente non vi è alcun provider unico sul mercato che può coprire l'ampiezza dei servizi descritti nello scenario, ma i servizi sono coperti da diversi provider. L'assegnazione di applicazioni per ogni livello (IaaS, PaaS, SaaS) è arbitraria ed è fatta per scopi puramente illustrativi e NON è una raccomandazione.

Scenario

L'azienda CleanFuture opera nel settore fotovoltaico. L'azienda produce e fornisce sistemi e componenti chiave per sistemi solari, fotovoltaici e di riscaldamento. La società è stata fondata nel 1999 in Germania, dove si trova il principale sito produttivo. Da allora CleanFuture è un'azienda in rapida crescita e il fatturato è aumentato in media del 20% l'anno.

Nel 2003, è stata aperta una filiale in Spagna e, nel 2004, sono stati aperti nuovi uffici in Italia. Nel corso del 2005, è stata presa la decisione di spostare la linea di business di produzione vetro antiriflesso solare in Polonia, dove a partire da giugno 2006 si iniziano a produrre i primi prodotti. L'azienda prevede inoltre di esplorare il mercato USA.

CleanFuture impiega 93 persone:

- 50 in Germania (2 siti differenti: sede principale (include il sito di produzione, laboratorio e 1 ufficio periferico)
- 34 in Polonia
- 5 in Spagna
- 4 in Italia

La società ha anche un numero variabile di appaltatori (da 10 a 30 agenti intermedi, rappresentanti, consulenti, tirocinanti, ecc.)

A causa della pressione della concorrenza e della crisi economica e finanziaria del 2008-2009, CleanFuture ha avviato una strategia a breve termine per ridurre i costi e aumentare la produttività. I servizi IT sono stati identificati come un settore cruciale, con un ampio margine di miglioramento.

L'analisi effettuata sui requisiti di sicurezza IT ha portato alle seguenti conclusioni:

1. Sono necessarie maggiore flessibilità e scalabilità per rispondere alle esigenze variabili dei servizi IT (un numero variabile di dipendenti nel

corso dell'anno, un numero variabile di partner e fornitori che devono essere trattati, i cambiamenti improvvisi nel panorama del mercato, la possibile cooperazione con un centro di ricerca e università, la possibile apertura di filiali e ampliamento della forza vendita, ecc.)

2. La società richiede un'alta qualità dei servizi IT (in termini di efficacia e performance) e un alto livello di Information Security (in termini di disponibilità, integrità e riservatezza). Tuttavia, al fine di fornire risorse interne (IT Dept) con tali alti livelli di servizio, sono necessarie competenze specifiche assieme a investimenti in hardware, software, assistenza e in sicurezza.
3. Devono essere migliorate la Business continuity e il disaster recovery.
4. Sarebbe estremamente importante dal punto di vista di efficienza del business e della capacità di innovazione avere un banco di prova per la valutazione di nuove applicazioni a supporto del business, nonché un ambiente di cooperazione in cui gli sviluppatori possono lavorare insieme con i partner verso nuove soluzioni e progetti.
5. Un progetto di migrazione da fisico a virtuale (phisical-to-virtual (P2V)) darebbe un feedback importante in termini di affidabilità ed efficienza con finalità di set-up.

I servizi e le applicazioni che saranno influenzati da questo nuovo approccio sono:

- posta elettronica e messaggistica
- desktop (applicazioni da ufficio)
- gestione progetti
- paghe
- CRM e gestione delle vendite
- contabilità e finanza
- hosting o esecuzione di applicazioni personalizzate, e sviluppo di applicazioni personalizzate
- gestione dell'identità.

Il gruppo di lavoro interno, supportato da un consulente esterno, propone la tecnologia del cloud computing come una possibile soluzione per le esigenze di CleanFuture.

Come passo successivo è stato effettuato uno studio di fattibilità sul cloud computing. E' stato consegnato al consiglio di amministrazione della società il report: 'CleanFuture - Uno studio di fattibilità sul Cloud Computing: una possibile strategia di implementazione e i connessi problemi di business, legali e di sicurezza'.

Sulla base dell'analisi ad hoc del gruppo di lavoro, il rapporto propone che i servizi IT individuati e le applicazioni siano affidati in outsourcing ad almeno tre fornitori di cloud. Nel lungo periodo i tre provider potrebbero costituire un cosiddetto "federation cloud", ma per il momento è consigliabile utilizzare, per ragioni di semplicità, tre provider indipendenti collegati in una soluzione di "gestione federata delle identità".

1. Fornitore Cloud # 1: offrirà un servizio basato su cloud hosting per posta elettronica, messaggistica, ambienti desktop, gestione del progetto e del servizio di buste paga (vale a dire, un 'software as a service' (SaaS) modello di cloud computing). Contrattualmente, i dati possono essere localizzati e trattati in luoghi diversi a livello mondiale, tra cui Asia, Europa e Stati Uniti.
2. Fornitore Cloud # 2: offrirà una piattaforma cloud-based per le applicazioni personalizzate di hosting, spesso definito come il modello 'platform as a service' (PaaS) del cloud computing. Questa applicazione personalizzata consiste in un 'simulatore' che aiuta i clienti ad auto-configurare un impianto fotovoltaico, a calcolare la produzione di energia (in base alla loro posizione geografica) e il ROI (secondo l'incentivo del paese in cui l'impianto sarà fatto).
3. Fornitore Cloud # 3: offrirà una infrastruttura cloud-based per le risorse umane, contabilità e finanza, CRM e la gestione delle vendite e sviluppo di applicazioni personalizzate (cioè il modello 'Infrastructure as a Service' (IaaS) del cloud computing).

Nel breve periodo (due anni), CleanFuture si occuperà di business continuity e disaster recovery di dati e servizi in outsourcing per PaaS e fornitori di IaaS. Questo sarà possibile utilizzando l'infrastruttura esistente. Il provider SaaS si assume la responsabilità per le esigenze di backup e business continuity per i servizi che fornisce. In entrambi i casi, il servizio di backup verrà fornito dal fornitore e dal CleanFuture per un periodo di due anni.

Il piano strategico a medio termine per il disaster recovery è ancora da definire. Sono da confrontare le due opzioni seguenti:

I. individuare un partner commerciale con cui creare un piccolo cloud privato e condividere le capacità e il costo di tale infrastruttura;
II. acquistare servizi di business continuity e disaster recovery da ogni provider cloud.

La decisione sarà presa entro due anni, allorquando l'infrastruttura IT attuale sarà obsoleta. Fino ad allora, CleanFuture userà la propria tecnologia in-house e on-site hosting per le proprie esigenze di continuità e di recovery.

Gestione dell'identità

La relazione riconosce la gestione dell'identità come un componente che interessa tutti gli aspetti della migrazione. Per motivi di affidabilità e scalabilità, CleanFuture NON dovrebbe fare affidamento a lungo termine su un elenco aziendale interno (directory) per l'autenticazione dell'utente e la gestione degli account. Una soluzione scalabile, flessibile e a prova di futuro deve fornire:

a) single sign-on
b) single sign-off
c) una directory unica per tutti i servizi
d) una sola applicazione per l'assegnazione e la revoca dell'identità
e) gestione sicura di ogni chiave crittografica utilizzata per l'autenticazione e la firma
f) implementazione delle politiche di controllo (ad esempio, utilizzando XACML). Una soluzione che garantisca che tutti gli utenti (collaboratori,

partner, fornitori) siano conformi ai requisiti di sicurezza di base dell'azienda. Questi requisiti sono stabiliti in base alle caratteristiche del profilo utente e di autorizzazione. I requisiti minimi stabiliti dovrebbero essere: antivirus aggiornato, con aggiornamento del sistema operativo.

Il rapporto raccomanda di passare a una soluzione di gestione federata delle identità che separi i vari account necessari per i diversi fornitori di soluzioni, da quelli dei fornitori delle identità e della gestione dei servizi. Un breve sondaggio mostra che poche soluzioni di cloud esistenti forniscono le interfacce necessarie per una soluzione completa FIM. Questo porta a una serie di importanti requisiti di migrazione:

1. I servizi selezionati dovrebbero supportare l'autenticazione tramite un selezionato framework FIM (implementazione mediante Liberty/Cardspace + SAML 2.0).
2. Prima di migrare tutti i servizi e le applicazioni al cloud, CleanFuture dovrebbe implementare un single-sign-on per tutte le applicazioni, tra cui l'autenticazione di partner esterni.
3. Le proprietà di trust di qualsiasi componente dell'infrastruttura di gestione dovrebbero essere accuratamente verificate.
4. Dovrebbe essere definito un livello di sicurezza di base per tutti i client che accedono a tutti i servizi.

Progetto	Fase 1 – 2008	Fase 2 – 2009	Fase 3 –2010	Fase 4 –2011	Fase 5 - 2012
Migrazione da Fisico a Virtuale (P2V)	Adozione di una piattaforma di virtualizzazione in azienda, esecuzione di migrazione da fisico a virtuale (P2V) delle seguenti applicazioni: CRM Gestione vendite, applicazioni personalizzate, HR	Verifica dell'affidabilità e prestazioni della soluzione di cui alla fase 1 Migrazione P2V delle seguenti applicazioni: contabilità e finanza Selezione del FIM e della soluzione di gestione chiavi	Verifica dell'affidabilità e prestazioni della soluzione di cui alla fase 2 Migrazione alla soluzione SSO FIM e alla soluzione per la gestione delle chiavi		
Migrazione al fornitore di cloud: PROVIDER #1 - SaaS			Selezione delle applicazioni cloud (SaaS) e migrazione delle seguenti applicazioni: gestione progetti *	Migrazione delle seguenti applicazioni e servizi: Posta elettronica *, messaggistica *, applicazioni da ufficio *, paghe *	
Migrazione al fornitore di cloud: PROVIDER #2 - PaaS			Selezione del fornitore cloud (PaaS) e migrazione delle seguenti applicazioni: CRM e gestione delle vendite	Verifica dell'affidabilità e prestazioni del fornitore PaaS Migrazione delle seguenti applicazioni: Applicazioni personalizzate, Contabilità e finanza, HR	Verifica dell'affidabilità e prestazioni del fornitore PaaS Migrazione delle seguenti applicazioni: Sviluppo di applicazioni personalizzate
Sviluppo di un cloud privato in partnership per DR e BC			Individuazione del partner Definizione dei requisiti di progetto	Definizione del progetto esecutivo	Avvio del cloud privato

* Si noti che queste applicazioni o servizi sono stati affidati in out-sourcing a fornitori cloud senza che sia effettuata una migrazione interna da fisico a virtuale.

Controlli di sicurezza esistenti

Il fornitore # 1 (SaaS) e il # 2 (PaaS) asseriscono di attuare una serie di controlli di sicurezza standard che includono:

- firewall
- IDS/IPS (Network and Host based)
- system hardening e in-house penetration testing
- gestione degli incidenti e degli aggiornamenti conforme a ITIL

Non sono forniti ulteriori dettagli. La selezione dei fornitori è eseguita da Future Clean sulla base della buona reputazione di Fornitore # 1 e Fornitore # 2.

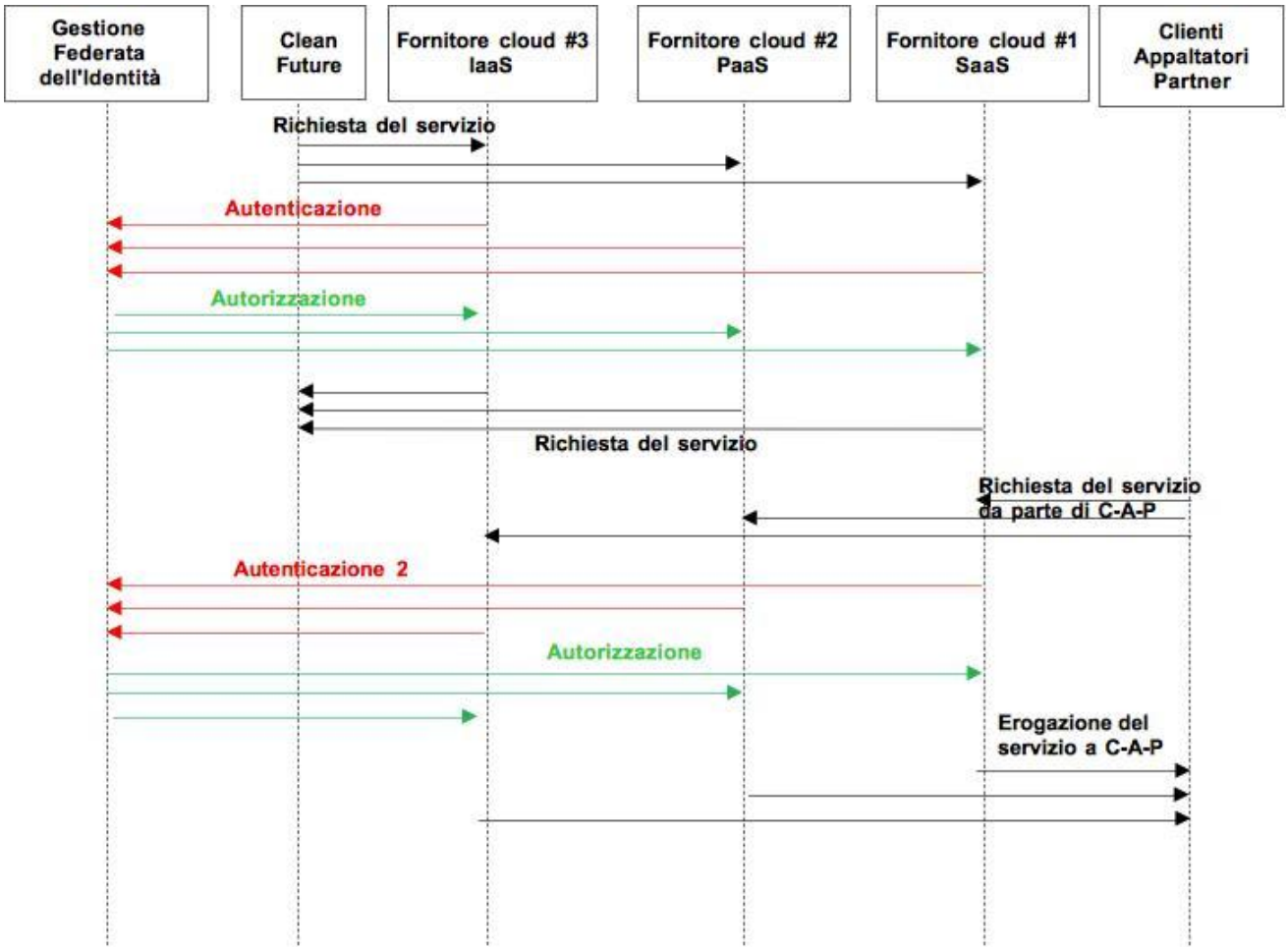
Fornitore # 3 (IaaS) offre le istanze VM pre-configurate in varie configurazioni standard. Esse, tuttavia, non offrono istanze pre-hardenizzate di default, cioè, il cliente è interamente responsabile di tutte le misure di sicurezza sulle istanze di macchine virtuali, incluso l'esame di tutte le impostazioni predefinite. Fornitore # 3 specifica che esegue un controllo di fondo su tutti i dipendenti (con alcune limitazioni in base alle leggi locali), che il controllo di accesso fisico è basato su smart-card biometriche e le politiche di controllo accesso ai dati sono basati sul principio del 'need-to-know'.

Tutti i collegamenti (IaaS, PaaS, SaaS, IDM, ecc.), ECCETTO quelli con i clienti (ad esempio, utilizzando l'applicazione di configurazione), sono cifrati (via VPN o SSH).

Tutti i fornitori sono certificati ISO 27001, ma nessuno di loro dichiara l'esatto ambito di applicazione della certificazione. Lo SLA con ogni provider comprende una clausola di notifica delle violazioni di sicurezza (breach notification). Tutti i fornitori offrono come extra (a pagamento), funzioni di reportistica di sicurezza. Tale reportistica può includere: violazioni fallite (degli asset del cliente), attacchi contro obiettivi specifici (per ogni utente aziendale, per ogni applicazione specifica, per ogni macchina fisica specifica, rapporto di attacchi interni rispetto agli attacchi esterni, ecc), le tendenze e le statistiche.

La soglia di segnalazione per i tentativi falliti e la scala di gravità degli incidenti sono personalizzati in base alle esigenze specifiche del cliente.

Flusso dei dati



ALLEGATO III – SCENARI DI ALTRI CASI D'USO

Nel seguito si trova un breve riassunto degli scenari di resilienza e di eHealth che sono stati utilizzati nella nostra analisi del rischio.

SCENARIO DI RESILIENZA

Questo scenario evidenzia come l'uso del cloud computing influenza la resilienza dei servizi a fronte di:

- improvvisi aumenti nella domanda da parte del cliente (ad esempio, in periodi di crisi finanziaria)
- attacchi finalizzati all'interruzione del servizio (denial of service)
- catastrofi naturali
- catastrofi localizzate
- uso improprio delle infrastrutture come piattaforma d'attacco
- fughe di dati (utente interno negligente o con intenti malevoli o processo difettoso)

L'anno è il 2012. XK-Ord fornisce e-commerce in tempo reale attraverso una interfaccia web-service, insieme a soluzioni per la fornitura di contenuti sotto forma di widget, che possono essere incorporati nei portali di acquisto. Casi d'uso tipici sono:

- dati e grafici in tempo reale di prezzi per le merci nei portali di acquisto.
- dati storici da utilizzare per la previsione di prezzi e di analisi
- storicizzazione degli ordini e resoconti di gestione del magazzino per le aziende
- conversione valuta in tempo reale e storicizzazione FX
- resoconti SOX & anti-monopolio UE aggiornati
- dati finanziari per applicazioni più complesse.

Inoltre, XK-Ord offre una piattaforma per la gestione dei vari servizi e per la combinazione di essi in applicazioni personalizzate. Data la loro offerta di servizi, XK-Ord richiede alta resilienza per:

- latenza - ritardi nella trasmissione dei dati possono portare alla perdita di contratti ad alto valore;
- adempimento alla richiesta - ad esempio, altamente affidabile:
  - richieste al database e presentazione dei risultati
  - web server in grado di gestire adeguatamente le richieste HTTP
  - infrastruttura TCP/IP;
- integrità dei dati - errori nei dati possono portare a perdite finanziarie;
- riservatezza e segnalazione - il dato ha un valore finanziario - quindi, se divulgato a clienti che non hanno pagato, rappresenta una perdita finanziaria per XK-Ord;
- integrità dell'applicazione e vulnerabilità.

Infrastruttura

Nel 2011, XK-Ord ha migrato, per ragioni di costi, flessibilità e affidabilità, verso un'infrastruttura in cloud. XK-Ord utilizza i sistemi di CumuloNimbus, un cloud provider che offre soluzioni IaaS per la fornitura dei contenuti.

- I dati sono memorizzati utilizzando un modello DaaS (database as a service).
- CRM e gestione degli account dei clienti di XK-Ord, tra cui la fatturazione, sono gestiti da un secondo cloud provider, Stratocumulus. Le credenziali vengono rilasciate e verificate da XK-Ord utilizzando questo servizio, mentre il controllo di accesso al contenuto è fornito da risorse di CumuloNimbus, vale a dire, Stratocumulus funge da fornitore di identità federata fornendo un'unica autenticazione (single sign-on).
- Le risorse umane di XK-Ord, le buste paga, le applicazioni desktop da ufficio e sistemi di Ricerca e Sviluppo sono gestiti direttamente da XK-Ord e ospitate sul sito da XK-Ord.

Rete

Rispetto all'utilizzo di un data center, le infrastrutture del cloud provider offrono dei notevoli miglioramenti in termini di larghezza di banda totale, elaborazione, memoria e spazio di archiviazione, nonché la possibilità di scalare velocemente i limiti. Ad esempio, i router situati vicino ai luoghi di distribuzione di contenuti utilizzano memoria virtuale scalabile, Risorse per la registrazione degli eventi e per il filtraggio dei pacchetti. IPSec è implementato in parti della rete. Queste caratteristiche migliorano notevolmente la resistenza contro gli attacchi DDoS.

Gestione delle risorse

- La distribuzione dei contenuti è a carico di XK-Ord sulla base della singola richiesta HTTP. I costi sono limitati in base ad una scelta di policy offerte da CumuloNimbus. I clienti di XK-Ord pagano in base al numero di richieste HTTP a ogni servizio, secondo uno schema diverso.
- Il provider gestisce le risorse in co-locazione insieme ad altri clienti (non necessariamente similari) sulla loro intera infrastruttura. Ciò significa che l'isolamento tra le risorse utilizzate da clienti diversi deve essere forte. XK-Ord ha la possibilità di pagare una piccola quota per riservare le risorse in anticipo, il che aumenta l'affidabilità complessiva per il fornitore di servizi e per la XK-Ord.
- La crescita nel breve termine nell'ambito delle risorse disponibili è più veloce rispetto a tipiche infrastrutture non-cloud. L'aggiunta di risorse di espansione (per esempio, più hardware in quanto il provider cloud è lento). Le difese DDoS in particolare devono scalare in modo rapido e le implicazioni sui costi e l'utilizzo delle risorse dovrebbero essere ben definite.
- Vengono utilizzati SLA standardizzati ed API standard per facilitare la migrazione tra cloud.

Servizi di sicurezza

XK utilizza un provider di servizi di sicurezza, BorealisSec, per il monitoraggio in tempo reale della sicurezza (RTM), la valutazione della vulnerabilità e la gestione dei dispositivi.

- Il personale di BorealisSec gestisce i sistemi di XK ospitati su CumuloNimbus utilizzando una connessione VPN.
- I log sono raccolti da CumuloNimbus e inviati automaticamente alla piattaforma SIEM (Gestione delle informazioni di sicurezza e degli eventi) di BorealisSec via VPN, per l'analisi. XK utilizza un fornitore di servizi di sicurezza, BorealisSec, per il monitoraggio in tempo reale della sicurezza (RTM), il vulnerability assessment e la gestione degli apparati.

Nell'eventualità che dovesse accadere un incidente di sicurezza:

- Un amministratore di BorealisSec si occuperà direttamente dell'incidente (automaticamente o manualmente), o
- essi apriranno un ticket verso Cumulonimbus per risolvere il problema.

In ogni caso, la risposta agli incidenti sarà contrattualmente concordata con XK, in base alla gravità.

I seguenti altri punti sono degni di nota:

- La valutazione della vulnerabilità può essere eseguita solo su una installazione di prova in quanto il ToU di CumuloNimbus vieta test di sicurezza pro-attiva.
- BorealisSec fornisce report di conformità e di controllo per quanto possibile all'interno del ToU di Cumulonimbus.
- BorealisSec è responsabile della gestione degli aggiornamenti software al di fuori della sfera di competenza del fornitore cloud.

SLA: XK-Ord -> clienti

XK-Ord offre un accordo sui livelli di servizio (Service Level Agreement - SLA) ai suoi clienti al fine di competere con altre società finanziarie che offrono certi SLA. Vale la pena notare che lo SLA di XK può offrire livelli più alti di affidabilità rispetto CumuloNimbus, nonostante la dipendenza tra i due. Ciò può essere dovuto al fatto che XK è disposto ad accettare un livello di rischio più elevato.

SCENARIO E-HEALTH

Obiettivo	KPI	Valore	Penali
Disponibilità del servizio	% tempo di funzionamento al mese	99.99	Fattura ridotta del 20% per ogni fattore di 10
Latenza (NB questo è il tempo da quando il mercato azionario pubblica i dati)	Tempo medio di risposta su 100 richieste in un giorno	1 secondo	Fattura ridotta del 5% per ogni violazione
Amministrazione	Tempo per rispondere ad una richiesta in minuti	60 minuti	Fattura ridotta del 5% per ogni violazione
Allarmi	Minuti per avvisare il cliente di una violazione di servizio (escluso questo...)	5 minuti	Fattura ridotta del 5% per ogni violazione
Tempo di ripristino dall'interruzione	Ore	2 ore	Fattura ridotta del 5% per ogni violazione

Questo scenario esplora l'uso del cloud computing da parte di organismi governativi di grandi dimensioni che devono soddisfare severi requisiti normativi e sono molto sensibili alla percezione negativa dell'opinione pubblica. Una considerazione fondamentale - quando si utilizzano i servizi cloud – è che possa esserci da parte dell'opinione pubblica la percezione che potenzialmente ci sia stata una mancanza di attenzione ai problemi di sicurezza o di privacy. Questo sarebbe particolarmente vero nel caso venissero utilizzati servizi cloud "pubblici".

EuropeanHealth rappresenta un importante servizio sanitario pubblico in Europa, *ma non raffigura alcun servizio sanitario nazionale specifico*. EuropeanHealth è composto da enti pubblici e fornitori privati che forniscono servizi di eHealth. Si tratta di un'organizzazione molto grande sparsa in diversi

siti e si rivolge a 60 milioni di cittadini. Prima di utilizzare qualsiasi tipo di infrastruttura cloud, ha oltre 20 fornitori di servizi IT e più di 50 data center.

Scenario specifico

Questo scenario specifico prevede una piattaforma di eHealth, che fornisce assistenza e monitoraggio dei pazienti affetti da malattie croniche nelle loro case. Questo processo generale è descritto in maggior dettaglio come segue:

1. Un centro di monitoraggio utilizza una piattaforma internet indipendente per la distribuzione a domicilio di sensori per monitorare e interagire con i pazienti più anziani a casa.
2. Le variabili monitorate sono analizzate rispetto ad anomalie che si discostano da un profilo base. Un centro di monitoraggio decide quando sono necessari servizi più specialistici (medici, infermieri, ecc.).
3. I pazienti possono anche scegliere di rendere disponibili le informazioni a fornitori esterni di servizi di eHealth. Tali informazioni private sono fornite tramite un database centralizzato.
4. I servizi sono forniti ai pazienti anziani a casa utilizzando una interfaccia multimodale che si adatta alle capacità degli anziani. Possono essere utilizzati personificazione e sintesi vocale.

I dati monitorati sono a disposizione di medici e ospedali attraverso l'esclusivo servizio di cartella clinica del paziente. Si può accedere alle informazioni del paziente attraverso un identificatore unico del paziente. Questo servizio fornisce una documentazione della storia clinica del paziente e della cura.

Gov-cloud

Per fornire tali servizi utilizzando un'infrastruttura cloud, EuropeanHealth utilizza ***Gov-Cloud***, un servizio cloud fornito dai governi nazionali per i servizi pubblici nel loro complesso. Si tratta di un cloud ibrido privato-partner, in quanto è utilizzato esclusivamente da partner fidati e soltanto le organizzazioni governative hanno accesso amministrativo (ad esempio, pubblica amministrazione, sanità). Esso utilizza un’infrastruttura di rete dedicata, che è

fisicamente indipendente dall'Internet pubblico. Il Gov-cloud è ospitato in diverse località geografiche, ma le macchine virtuali possono essere trasferite da un sito all'altro.

Tutti i servizi nel nostro scenario specifico girano sul Gov-Cloud con le proprietà di sicurezza descritte di seguito.

Ad esempio:

- alcuni dei servizi in esecuzione internamente sono in esecuzione sul cloud utilizzando IaaS;
- i servizi in esecuzione presso il centro di monitoraggio sono in esecuzione sul cloud utilizzando IaaS;
- i dati monitorati vengono anche memorizzati nel cloud utilizzando DaaS (database as a service).

Gov-Cloud fornisce, inoltre, un mezzo per trasferire in modo sicuro i dati dei pazienti (in precedenza era abbastanza difficile) con un servizio di posta elettronica personalizzato per medici e infermieri. Questo servizio è fornito da una terza parte, ma progettato da EuropeanHealth.

Protezione dei dati

Tutti i dati raccolti da EuropeanHealth devono soddisfare i seguenti requisiti:

- I dati (comprese le informazioni personali sensibili) devono essere cifrati in transito e a riposo, dove sono potenzialmente a rischio (ad esempio, su dispositivi mobili).
- Il trattamento dei dati deve soddisfare la legge Europea di protezione dei dati (ad esempio, la definizione di 'elaboratore di dati' per tutte le operazioni).
- La legislazione nazionale applica alcune restrizioni in materia di trattamento dei dati (ad esempio, i dati non dovrebbero lasciare il paese d'origine della raccolta in qualsiasi momento).

- La sicurezza clinica deve essere fondamentale per alcune applicazioni, il che significa che l'integrità e la disponibilità devono essere 'garantite' in alcuni casi.
- I dati sensibili devono essere distrutti in un dato momento nel loro ciclo di vita (ad esempio, con la distruzione degli hard disk `alla fine della vita ' delle apparecchiature).
- devono essere adeguatamente garantiti dei controlli di sicurezza fisici nei data center in cui sono memorizzati i dati (alcuni di questi aspetti sono attualmente coperti attraverso l'osservanza alle ISO27001 da parte dei fornitori).
- Al personale dirigente è affidata la responsabilità speciale per la riservatezza delle 'informazioni del paziente e dell'utente del servizio'.

Conformità a leggi, regolamenti e buone norme (best practice)

- Tutti i fornitori devono dimostrare la conformità con ISO27001. Essi NON sono tenuti a essere accreditati, ma la conformità è dimostrata attraverso una verifica di presentazione annuale del loro sistema di gestione della sicurezza delle informazioni e dei documenti collegati.
- Ulteriori certificazioni e accreditamenti assistono le organizzazioni EuropeanHealth nella scelta di fornitori adeguati, ad esempio, ISO20000 (Service Management), ISO 9001 (Qualità), ecc, ma questi non sono richiesti.
- In termini di verifiche e conformità alle normative o agli standard nominati, da parte del fornitore di servizi, i fornitori di servizi di cloud computing devono garantire di essere in grado e disposti a consentire il diritto di verificare le loro policy, processi, sistemi e servizi.

Governance

Un insieme di controlli base di sicurezza è fornita da Gov-Cloud e controlli aggiuntivi sono eventualmente forniti dai servizi di gestione o da gestione in-house per ogni utente del Gov-Cloud (come EuropeanHealth). Vengono utilizzati standard di governance, come ad esempio ITIL.

EuropeanHealth non può imporre ai reparti interni di adottare tecnologie specifiche, ma solo raccomandare le tecnologie da adottare. I dipartimenti di EuropeanHealth restano liberi di applicare la tecnologia che meglio soddisfa le loro esigenze.

EuropeanHealth può richiedere alle organizzazioni partecipanti di fornire documentazione che dimostri che le loro raccomandazioni sono state seguite, per esempio, la prova che tutti i dati sui laptop siano cifrati. Per i fornitori esterni, ci sono requisiti specifici per le organizzazioni per connettersi alla rete EuropeanHealth e rimanere connessi.

Controllo degli accessi e verifiche delle tracce

EuropeanHealth fornisce Single Sign On (SSO) per le sue applicazioni e servizi utilizzando le smart card come token di autenticazione. Le organizzazioni EuropeanHealth possono utilizzare molte altre forme di autenticazione o forme multiple per diversi scopi (ad esempio, singolo fattore, due fattori, biometrici e così via). I fornitori di terze parti di Gov-Cloud si interfacciano con la PKI di EuropeanHealth utilizzando smart card.

Ci sono requisiti assoluti in termini di controllo per garantire che sia chiaro chi ha avuto accesso a quali dati personali o a quali dati personali sensibili e per quali scopi.

Accordi sui livelli di servizio (SLA)

Gli SLA dovrebbero essere di natura contrattuale ed inseriti all'interno di qualsiasi servizio cloud offerto alle organizzazioni EuropeanHealth. La chiave sarà probabilmente la disponibilità 24/7 (ma dipendente dal tipo di servizio, dall'applicazione o dai dati che vengono ospitati).

- Una preoccupazione per le organizzazioni EuropeanHealth sarà la potenziale perdita di controllo che percepiranno (ad esempio, delle infrastrutture, dei servizi, dei dati e del provisioning, ecc.). La capacità

dei fornitori di servizi cloud nel dimostrare che 'non' c'è perdita di controllo sarà un fattore chiave per acquisire il cliente.