Il contratto e gli SLA con il cloud service provider

E-privacy
Firenze 3 giugno 2011

Lucilla Mancini
Business-e-Security Consulting Manager
&
SALVI SAPONARA CIMINO & GIANNI

BUSINESS e
drive your e-success

Definizione

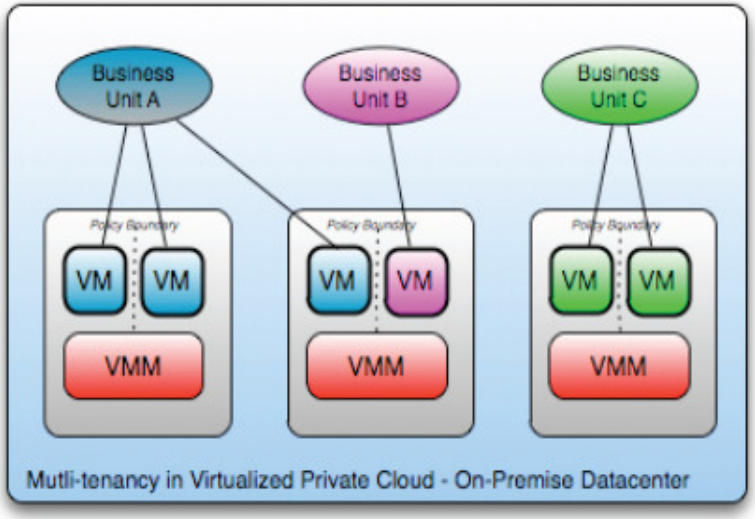
Cloud computing è un nuovo modo di fornire risorse, non una nuova tecnologia!

Teorici Svantaggi

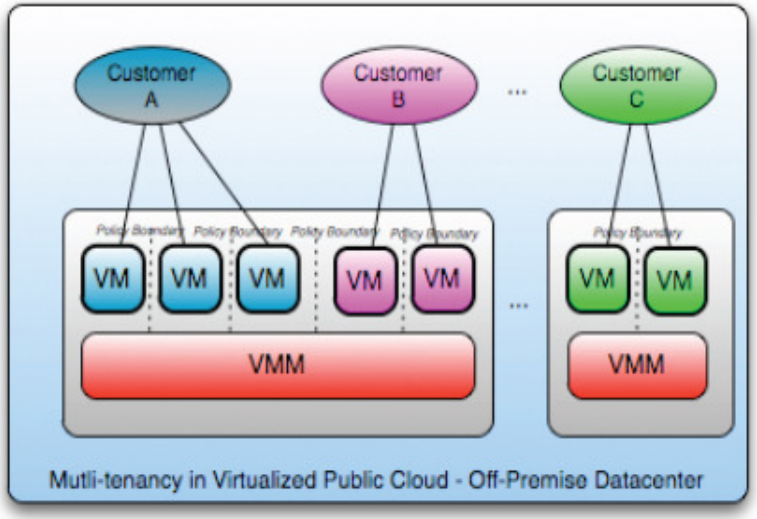
- **Problematiche che derivano dalla dipendenza da Terze Parti**
  - Costi, tempi di risoluzione problematiche di sicurezza etc..
- **Lock-In**
  - non essendo ancora stato definito uno standard migrare da un provider ad un altro potrebbe essere complicato.
- **Compliance Risks**
  - L'investimento nell'ottenere certificazioni può essere messo a rischio dalla migrazione al Cloud (es. PCI-DSS)

Rischi

- **Multi-tenancy : condivisione dello stesso hardware e software - Multi-Tenancy significa, in parole semplici, che non viene messa a disposizione per ciascun cliente un'infrastruttura separata dedicata (single-tenant), ma che tutti gli utenti operano sulla stessa piattaforma**
  - un problema di sicurezza per un Cliente in un ambiente



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

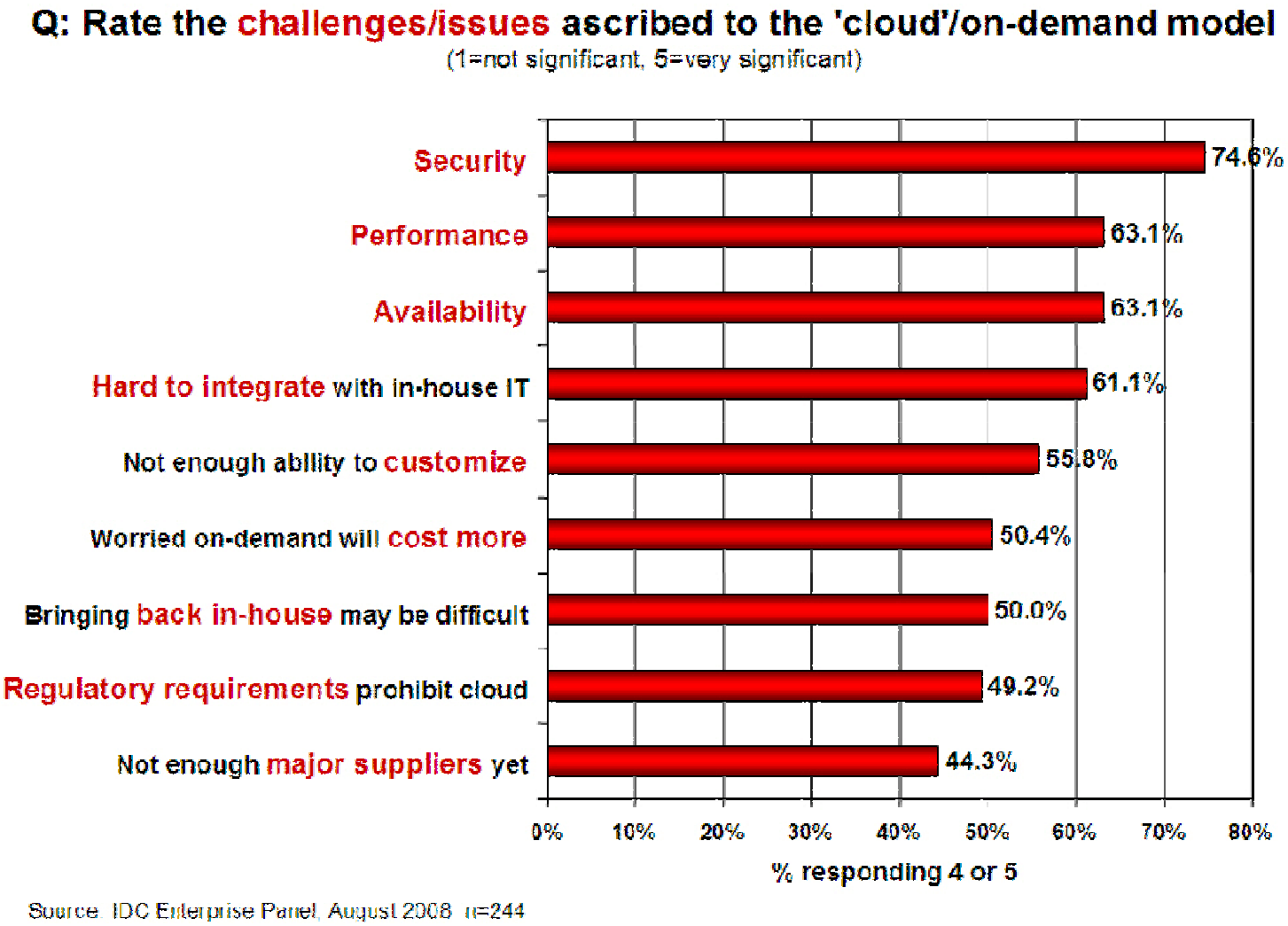
Rischi

- **Perdita di Governance**
  - Il Cliente cede il controllo al Cloud Provider su problematiche che possono aver effetto sulla sicurezza.

- **Data Protection**
  - In alcuni casi, può essere difficile per il Cliente controllare efficacemente le modalità di trattamento dei dati del Cloud Provider per essere sicuri che i dati siano trattati in modo lecito e conforme alle policy.

Cloud Computing Security

La sicurezza è il problema maggiore



Cosa si intende con "Security" nel cloud

- I controlli di sicurezza per il cloud computing non differiscono molto dai controlli di sicurezza necessari in generale nel mondo IT per la protezione delle informazioni.

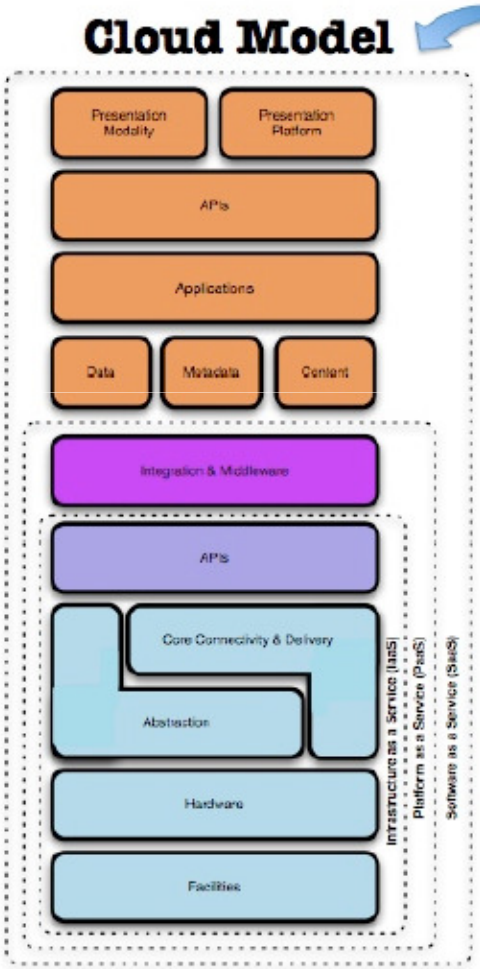
- Va invece sottolineato che, a causa dei diversi modelli di servizio, delle tecnologie usate etc… sono diversi i **rischi** da considerare e le responsabilità.

Sicurezza come Market Differentiator

La sicurezza è una preoccupazione prioritaria per i clienti del Cloud, molti di loro faranno le scelte d'acquisto sulla base della reputazione in merito a confidenzialità, integrità e disponibilità, ed i servizi di sicurezza offerti da un provider.

Questo è un forte "*driver*" per i fornitori di Cloud per migliorare le pratiche di sicurezza!

Cloud – security - compliance



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

- PCI
  - Firewalls
  - Code Review
  - WAF
  - Encryption
  - Unique User IDs
  - Anti-Virus
  - Monitoring/IDS/IPS
  - Patch/Vulnerability Management
  - Physical Access Control
  - Two-Factor Authentication...
- HIPAA
- GLBA
- SOX

ISO27002

La ISO/IEC 27002, sezione 6.2, “External Parties” sancisce :

“…la sicurezza delle informazioni nell’ambito di una organizzazione non deve essere mai ridotta dall’introduzione di servizi e prodotti di terze parti”

Principali benefici in termini di sicurezza

Economie di scala:

tutte le misure di sicurezza sono più economiche quando vengono implementate su larga scala. Ciò include patch management, hardening delle macchine virtuali, etc. Altri benefici sono relativi alla presenza di più location, e gestione più vicina alla destinazione finale), tempestività, etc…

Principali benefici in termini di sicurezza

Risorse velocemente ed efficacemente scalabili: la capacità dei cloud provider di riallocare dinamicamente le risorse per il filtering, l'autenticazione, l'encryption, etc, verso misure di difesa (e.g., DDoS attacks) ha l'evidente vantaggio della resilienza (capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati).

Aggiornamenti più efficaci, efficienti e con migliori tempistiche per i defaults: aggiornamenti e patch in un ambiente virtuale possono essere gestiti meglio; le API di un IaaS cloud service consentono di avere una foto dell'infrastruttura virtuale che può essere costantemente confrontata con la baseline.

Gli aggiornamenti possono essere distribuiti molte più volte ed in maniera più efficace in una piattaforma omogenea che non in un ambiente client-based che si appoggia sul modello del patching.

Benefici della concentrazione di risorse: sebbene la concentrazione di risorse sia uno svantaggio per la sicurezza, esiste l'indubbio vantaggio di un ridotto perimetro per accesso fisico (per unità) e quindi una più facile e economica di implementazione di processi di sicurezza.

Governance and Enterprise Risk Management

- Una corretta governance e gestione dei rischi nel mondo Cloud comporta processi e programmi per la gestione della sicurezza delle informazioni che siano scalabili, misurabili, ripetibili, misurabili, migliorabili etc.

- E' importante, come per ogni processo, seguire le best practice per il risk management. Le practice devono essere proporzionate all'utilizzo che l'azienda fa dei servizi cloud, che può andare da un semplice data processing all'affidamento di processi critici per il business con dati sensibili.

Suggerimenti per la governance

- I soldi “risparmiati” attraverso i servizi cloud devono essere investiti per migliorare il controllo delle capacità in termini di sicurezza del provider attraverso assessment ed audit frequenti.
- Sia i clienti che i fornitori di servizi cloud devono implementare robuste policy e una forte governance della sicurezza, collaborando insieme al fine di raggiungere gli obiettivi che supportino sia il business che la compliance.

Risk Management

- A causa dello scarso controllo fisico sull'infrastruttura nei servizi cloud, risultano di fondamentale importanza gli SLA, i contratti e la documentazione fornita dal provider.

- A causa degli aspetti legati al multi-tenant del Cloud Computing, le forme tradizionali di audit potrebbero non essere consentite: ad esempio attività quali i vulnerability assessments ed i penetration test potrebbero non essere consentiti, così come la raccolta degli audit log; a tale scopo è bene valutare il provider corretto o trovare metodi alternativi di verifica.

Il Rischio Legale: Un contratto standard…

…che non prevede, o meglio, gestisce i rischi operativi, tecnici ecc.:

1. **Illicit Cloud Use and Common Platform Attacks**
2. **Insecure Cloud Application Programming Interface Access**
3. **Malicious Insiders**
4. **Shared Infrastructure**
5. **Data Theft and Loss**
6. **Account Hijacking**
7. **Unknown Risk**

Requisiti legali

Ogni cliente o potenziale cliente di servizi cloud deve tenere in considerazione gli obblighi derivanti da requisiti di legge nazionali o sovranazionali al fine di avere garanzia della conformità al cogente.

I punti di attenzione sono:

- **In quale paese si trova il cloud provider?**
- **L'infrastruttura è nello stesso paese o altrove?**
- **Il cloud provider utilizza altre aziende le cui infrastrutture sono locate fuori dallo stato del cloud provider?**
- **Dove risiederanno fisicamente i dati?**
- **Come saranno raccolti, processati e trasferiti i dati del cliente e dei suoi clienti?**
- **Che accade ai dati inviati al cloud provider una volta che il contratto è concluso?**

Gestione del rischio legale

3 “zone” contrattuali: sicurezza, performance, exit

E’ fondamentale distinguere il caso delle piccole/medie imprese che sceglieranno tra i diversi contratti offerti dal mercato, con il caso di grandi organizzazioni che invece sono nella posizione di negoziare un contratto ad hoc.

“Due Diligence” sul Provider

Temi Legali: Clausole contrattuali

1. Privacy/Confidentiality: normative, ID Theft, User Privacy
2. Sicurezza dei dati; "Location" dei dati
3. Responsabilità di utenti finali
4. Uso/Accesso non autorizzato
5. Diritti di sospendere "user accounts"
6. Sospensione del servizio "in caso di emergenza"
7. Proprietario dei dati; proprietà intellettuale
8. Pubblicità
9. SLA
10. Disclaimer
11. Indennizzo (dal cliente/dal vendor)
12. Rinnovo tacito
13. Incorporazione di "URL Terms"
14. Modifiche al contratto
15. Normativa applicabile

Altri argomenti da valutare

1. **e.discovery: sopratutto per le banche/investitori istituzionali**
2. **Computer Forensics: i server spun down?**
3. **Audit Logging**
4. **Law enforcement access**

Un contratto dovrebbe avere i seguenti capitoli:

The Services
Modifications to this Agreement
Term, Termination and Suspension
Authorization and License to Use the Services
    Permitted Uses Generally
    Restricted Uses Generally
    Accounts and Keys
Acceptable Use Policy and Service Terms
License to Use Properties
Downtime and Service Suspensions; Security
Fees
Confidentiality
Intellectual Property
Representations and Warranties; Disclaimers; Limitations of Liability
Indemnification
Government License Rights; Import and Export Compliance
Disputes
Notices
Miscellaneous Provisions

Grazie dell'attenzione

BUSINESSe
drive your e-success