Continuando a Navigare sulle “Nuvole” ...

Andrea Pasquinucci

Indice:

- Il Cloud: Veloce Riassunto
- Alcune Caratteristiche delle Nuvole
- Modelli di Nuvole e Gestione dei Rischi
- Conclusioni

Il Cloud: Veloce Riassunto

- Un tempo si parlava (ad esempio) di
  - Outsourcing
  - ASP (Application Service Provider)
  - Sistemi centralizzati (Mainframe)
  - Data Center remoti
  - ...
- Oggi si parla solo di

Cloud Computing

Principio 1

- Il "*Cloud* " è volutamente un concetto

"***Foggy*** "

  - Oggi quasi ogni implementazione IT sufficientemente avanzata tecnologicamente o per tipo di servizio, può essere classificata come un "Cloud" di qualche tipo

Principio 2

- Le "*Nuvole*" attuali sono dovute alla maturazione di alcune tecnologie:
  - Virtualizzazione (HW)
  - Web 2.0 (interattivo)
  - Calcolo distribuito (Grid)
  - Connettività (Mbps)
  - Architetture Applicative Distribuite (SOA)
  - ....

Classificazione delle Nuvole

- Modelli di servizio (NIST)
  - Infrastructure as a Service (IaaS): utilizzo della infrastruttura HW
  - Platform as a Service (PaaS): utilizzo del Sistema Operativo
  - Software as a Service (SaaS): utilizzo del Software Applicativo

Classificazione delle Nuvole - 2

- Modelli di erogazione (NIST)
  - **Pubblico**: fornitore di servizi via internet
  - **Privato**: servizio interno all'azienda
  - **Ibrido**: in parte Pubblico, in parte Privato
    - Esempio: ambienti di sviluppo e di test Pubblici, ambiente di produzione Privato
  - **Comunità**: servizio verticale riservato a / specializzato per una comunità
    - Esempi: medicale, applicazioni smartphone, ambienti sviluppo SW ...

Alcune Caratteristiche

- Virtualizzazione (OS gira su HW virtuale)
- Analogamente per Applicazioni su OS (Java)
- Web 1.0 : pagine statiche => Web 2.0 : pagine dinamiche
  - Aggiornamento dinamico **elementi** pagine
  - **I dati possono risiedere sul server**
    - Ritorno al principio: elaboratore centrale e terminale "stupido", non solo PC ma anche smartphone e quant'altro

Modello Pubblico

- Fornitore di servizi ***Nuvolosi*** via Internet
- Scalabilità, economicità servizi
- **CAPEX vs OPEX**

Outsourcing Virtuale

- **Chi gestisce Cosa ?**
  - Responsabilità di Fornitore e Cliente
- **Dove sono i miei dati ?**
  - Da qualche parte (replicati) in Internet
    - Il Garante della Privacy non sarà molto contento...
    - Compliance e Norme (PCI ...) ?

Dati e Pubblicità

- Quale è il rischio che miei dati diventino pubblici?
  - Sindrome **Facebook !!!**
- Quale controllo ho sulla gestione dei miei dati nelle nuvole?
  - **Nullo ?**
- Cifratura dei dati:
  - Del provider = meglio che niente
  - In casa = in teoria OK, in pratica costosa e di difficile implementazione

Cloud Storage

- Servizio Pubblico / Comunità
- Utilizzo per **Backup**
  - Cifratura dati solo in casa
  - Pba localizzazione ridotto
  - Pba garanzia disponibilità dei dati
- Utilizzo **Storage Condiviso**
  - Dati “pubblici” anche se cifrati?
  - Chi accede, come, quando ...?

Sicurezza ICT Tradizionale

- **DataCenter => Firewall => IPS/IDS/Proxy => LAN Segregation => .... => Server**
  - Protezione anche **fisica** delle risorse (applicazioni e dati)
- Esempio: una vulnerabilità applicativa può costituire un rischio minore se un FW / IPS la scherma
- E' sempre possibile (anche fisicamente) “staccare la spina”

Sicurezza ICT sulle Nuvole

- Accesso **diretto** alle risorse
  - I dati e le applicazioni sono sempre online
- Protezione solo **logica** delle risorse (applicazioni e dati)
- L'infrastruttura non è più uno strumento di controllo e sicurezza
  - E' solo uno strumento di comunicazione
  - Manca la fisicità e la localizzazione delle risorse
    - Come faccio a proteggerle dall'esterno? Non posso, devo proteggerle “dall'interno”

Alcuni Rischi

- Sicurezza dei dati
  - Controllo e Sicurezza degli Accessi (anche Admin)
    - Piattaforma condivisa => valutazione attacchi esterni e/o interni anche in riferimento agli altri clienti
  - Segmentazione di Infrastruttura e Dati
  - Accesso ai dati da parte dei Sub-contractors
  - Data Ownership
  - E-discovery
  - Filtri sui contenuti
  - Cifratura dati e comunicazioni
  - Backup e restore

Alcuni Rischi - 2

- Disponibilità e Provisioning dei Servizi
  - Degradazione dei servizi
  - Interruzione dei servizi
  - Gestione del Change dei servizi
  - Modifica dei piani tariffari
  - Procedure di enrollment e dis-enrollment
    - Affidabilità del fornitore, cambio fornitore
    - Inter-operabilità tra fornitori

Alcuni Rischi - 3

- Compliance
  - Reporting e Audit dei sistemi sia dei clienti che delle piattaforme del fornitore
  - Gestione dello storage dei dati
  - Procedure di Audit dei clienti e terze parti
  - Compliance con standard e normative
  - Gestione degli incidenti e notifiche di attacchi riusciti e non riusciti

Modello Privato

- Tipicamente IaaS (cioè Infrastruttura HW)
- Trade-off: costi <=> dim. scala <=> prestazioni
  - Conveniente solo se il sistema è di dimensioni sufficientemente ampie
- Introduzione di un ulteriore livello SW da gestire
- "*Nuove*" tecnologie, richiedono personale specializzato per gestirle
- **Affidabilità** dei sistemi e architetture HW/SW
- **Compatibilità** tra Vendor diversi (mancanza Standard)

Modello Ibrido

- Nuvola Privata e Pubblica
- Rischio **commistione** dati: **dati privati => nuvola pubblica**
  - Costi
  - Disponibilità
  - Semplicità
  - Eccezioni
  - Difficoltà di controlli

Modello Comunità

- Applicazioni specializzate
  - Molto utile
- Aspetti tecnici fanno sottovalutare i rischi
  - Leaking informazioni
  - Condivisione dati con competitor
  - Dati di produzione in ambiente di sviluppo
  - Minori controlli visto che si tratta di “campo tecnologico”

Cosa Fare?

- Aspetti contrattuali e legali
  - vedi Outsourcing
- Scelta applicazioni da far Veleggiare
  - Valutazione modalità di utilizzo, sicurezza accessi e manutenzione
- Valutazione rischi dei dati sulle nuvole
  - Scenario della perdita completa dei dati o accesso pubblico ai dati e applicazioni
- Valutazione reale di costi, risparmi ed innovazioni tecnologiche

Conclusioni

- Le “*Nuvole*” sono una rinascita di un vecchio paradigma IT rivisto con nuove teconologie
- Le “*Nuvole*” sono qui per restare
- Le nuove “*Nuvole*” sono ancora giovani
  - se danno problemi, si rischia di scottarsi al sole
- Affidare a qualcun altro i propri problemi non vuol dire risolverli (attenzione a non fare gli “struzzi”)

Riferimenti

- *Cloud Computing Security Risk Assessment: Benefits, Risks and Recommendations for Information Security*, ENISA, 2009
- *Top Threats to Cloud Computing*, Cloud Security Alliance (CSA) 2010
- *The NIST Definition of Cloud Computing*, NIST, 800-145, 2011
- *Cloud Computing Synopsis and Recommendation*, NIST, 800-146, 2011
- *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, 800-144, 2011
- *Cloud Computing Risks*, R. Mosher, ISSA Journal July 2011

Riferimenti

- *Cloud? Si, grazie, ma senza Fog*, R. D'Alessandro, Information Security n° 3, 2011
- *IT Governance and the Cloud*, R. Speed, ISACA Journal vol. 5, 2011
- *Cloud Computing Risk Assessment*, S. Gadia, ISACA Journal vol. 4, 2011
- *Cloud Computing as an Integral Part of a Modern IT Strategy*, KU. Ruhse, M. Baturova, ISACA Journal vol. 3, 2012
- *Securing Hybrid Cloud Applications*, C. Sweet, ISACA Journal vol. 4, 2012
- *Cloud Risk – 10 Principles and a Framework for Assessment*, D. Vohradsky, ISACA Journal vol. 5, 2012

Copyright e Licenza

Grazie

Andrea Pasquinucci

pasquinucci-At-ucci.it www.ucci.it