Volando nella Nebbia delle Nuvole

(ovvero Cloud e Sicurezza)

Sommario

Navigare nelle “Nuvole”, modo grazioso per indicare l'utilizzo di servizi ICT “Cloud”, è e diventerà sempre più comune e conveniente. Al contempo le problematiche di sicurezza, non solo relative agli aspetti più tecnici-informatici, ma in generale alla protezione delle informazioni personali ed aziendali, diventano e diventeranno sempre più complesse. E' necessario quindi comprendere chiaramente il significato della navigazione sulle “Nuvole” per evitare spiacevoli incidenti dovuti alle sempre più presenti “Nebbie”.

Ormai le “Nuvole” (“Cloud”) sono il paradigma dell'ICT innovativo, qualunque nuovo prodotto o servizio deve avere una qualche connotazione “Nuvolosa” per potersi presentare sul mercato.

Ma cosa sono le “Nuvole”?

In realtà nulla di nuovo, quelli che qualche tempo fa chiamavamo Outsourcing, ASP (Application Service Provider), sistemi centralizzati (mainframe), data-center remoti, sistemi client-server ecc. sono oggi accomunati in una unica sigla, le “Nuvole” appunto.

Quello che è cambiato è la tecnologia che oggi permette di fare quello che ieri solo si immaginava di fare:

- Virtualizzazione dell'Hardware (ieri solo su Mainframe, oggi su qualunque PC)
- Web 2.0 ovvero interattivo
- Calcolo distribuito (Grid)
- Connettività veloce (Mbps per tutti)
- Architetture Applicative Distribuite (SOA)

eccetera. Nulla di nuovo a livello di concetti fondamentali, molto di nuovo a livello di risultati pratici. Vale la pena di soffermarsi sullo strano percorso della capacità di calcolo e di archiviazione dei dati: dai sistemi terminale-server degli anni '80, ai PC degli anni '90 con lo spostamento di dati e calcolo sui terminali utente, al ritorno al modello client-server attuale, ove i dati e il calcolo sono appunto nelle “Nuvole” ed i terminali utente si limitano in pratica al rendering grafico (si pensi in particolare a tablet e smartphone).

Se è difficile dare una definizione chiara di cosa siano le “Nuvole”, vi sono comunque alcune caratteristiche comuni o ricorrenti che è importante ricordare:

- Accesso a reti a banda larga (anche LAN)
- Rapida elasticità (scalabilità)
- Misurabilità dei servizi
- Approvvigionamento Self Service
- Comunione delle risorse.

Dal punto di vista tecnico un punto è particolarmente interessante, il disaccoppiamento dei tre livelli:

- hardware
- sistema operativo
- applicazione.

L'idea di base è che possiamo

- virtualizzare l'hardware sul quale eseguire diversi sistemi operativi
- “virtualizzare” i sistemi operativi sui quali eseguire un'applicazione, ad esempio utilizzando linguaggi quali Java e la Java Virtual Machine
- “virtualizzare” le applicazioni fornendo un'interfaccia tipicamente Web che rende indipendente la fruizione dell'applicazione dall'istanza dell'applicazione stessa.

In parallelo a questo abbiamo gli ormai famosi tipi di servizi delle “Nuvole”:

- 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

ed i modelli di fruizione:

- 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 per smartphone, ambienti sviluppo SW.

Le Nuvole Pubbliche

Quando si parla di "Nuvole" comunemente si fa riferimento a servizi offerti e fruiti in Internet. Tralasciando di considerare gli aspetti tecnici che in questa sede non ci interessano più di tanto, ragioniamo sugli aspetti di servizio ed il significato che questi hanno per un'azienda od un privato cittadino. I più comuni lati positivi sono facili da individuare:

- risparmio economico
- approvvigionamento self-service o molto rapido
- facile e rapida scalabilità
- grande accessibilità.

Per un'azienda vi è un altro punto di grande interesse, il fatto di imputare i costi come OPEX, ovvero spese operative, senza CAPEX, ovvero investimenti di capitale. In questo modo l'utilizzo di un servizio diventa molto più semplice visto che basta pagare quanto si consuma senza dover fare degli investimenti, che in realtà fa il fornitore di servizi invece dell'azienda. Il fatto che il fornitore fornisca lo stesso servizio a molti clienti, riduce i costi per i fruitori a seguito delle economie di scala.
Fin qui nulla di nuovo nel modello di business, un tempo lo si chiamava Outsourcing.
Come nei contratti di Outsourcing è quindi necessario capire le responsabilità ed i doveri di cliente e fornitore. Molti progetti di Outsourcing sono risultati dei veri fallimenti proprio a causa della mancata chiarificazione del "chi fa cosa" e "chi è responsabile di cosa".

Nel caso di servizi “Nuvolosi” il rischio è ancora più grande vista la facilità di accedere ai servizi: il più delle volte basta un “click” di mouse, e nessuno legge le clausole di servizio scritte in piccolo visto che poi si paga con la carta di credito (qualunque cosa questo voglia dire). Nei casi di Outsourcing tradizionale almeno c'era un contratto cartaceo che qualcuno doveva leggere e firmare, magari passando prima per un'opinione dell'ufficio legale. E' inevitabile quindi che le clausole contrattuali proteggano in maniera particolare il fornitore del servizio e che vi siano delle clausole generiche a protezione dei clienti, che sono spesso diversi e con diverse esigenze. In questo caso al più verrà garantito ai fruitori il minimo comune di interesse tra i potenziali clienti del fornitore.
L'utilizzo di un servizio “Nuvoloso” Pubblico parte quindi con una gran dose di rischio già a livello contrattuale, ma questo è solo l'inizio.

I miei dati ed il Garante per la Privacy

Tralasciando gli aspetti unicamente contrattuali di un servizio “Nuvoloso” Pubblico, la prima cosa che in pratica succede è che dati aziendali (o personali) vengono trattati, gestiti, archiviati dal servizio e sui sistemi del fornitore. In fondo è proprio quello che si vuole fare, quindi non possiamo meravigliarcene. Il punto principale è che dati che prima risiedevano esclusivamente sui sistemi aziendali (o personali) ora sono presenti sui sistemi del fornitore. Nel caso di un servizio tradizionale di Outsourcing, i sistemi esterni ove risiedono i dati sono in una località vicina, alla quale si ha accesso e che si è visitata, ed il tragitto dei dati tra la sede aziendale e quella del fornitore è noto.
Per un servizio “Nuvoloso” Pubblico tutto questo non vale: tipicamente il fornitore del servizio applicativo a sua volta usufruisce di servizi “Nuvolosi” Pubblici per l'infrastruttura, da SaaS a PaaS a IaaS, ognuno dei quali utilizza data-center e server ridondati più volte per garantire l'alta affidabilità nelle sedi economicamente più convenienti.
In conclusione i dati aziendali tipicamente vengono trattati, gestiti, archiviati su sistemi di molteplici fornitori di servizi (spesso non conosciuti dal cliente) e distribuiti in tutto il mondo.

Questa realtà è quella che permette di ottenere servizi a basso costo ed alte prestazioni, ma al contempo sicuramente da dei grattacapi, e non piccoli, con le norme per la gestione dei dati personali secondo il Garante della Privacy. Questa problematica è ben nota, al punto che alcuni tra i più grandi fornitori di servizi "Nuvolosi" Pubblici permettono di scegliere in quale continente e secondo quale legislazione gestire i dati. Al contempo stanno nascendo servizi "Nuvolosi" localizzati, sia per rispondere a delle esigenze localizzate di servizi che per rispettare le normative di ogni singola nazione sul trattamento delle informazioni.
Una scelta oculata del fornitore potrebbe quindi, a scapito del risparmio economico, garantire il rispetto delle norme di legge sul trattamento delle informazioni e dei dati personali.

I miei dati e la sindrome di Facebook

Ma il principale rischio nell'utilizzo di servizi "Nuvolosi" Pubblici è che la presenza dei propri dati sui sistemi altrui in data-center e server anche in svariati paesi esteri, rende plausibile la possibilità di accesso e divulgazione dei dati da/a terzi. Forse il corretto punto di approccio è quindi quello della sindrome di Facebook, ovvero "all your data belong to us".
E' necessario valutare come realistico il seguente scenario: per un qualunque motivo tutti i dati aziendali presenti nei servizi "Nuvolosi" Pubblici sono ad un certo momento resi veramente pubblici, ovvero chiunque ne ha accesso via internet, con una molto limitata responsabilità del fornitore dei servizi, oppure sono utilizzati da altri senza che l'azienda possa opporsi.
Quali conseguenze avrebbe questo evento per l'azienda?
Questa domanda è cruciale e non solo deve essere posta, ma bisogna anche darle le opportune risposte. Per rendere più preciso lo scenario, bisogna aggiungere alcune informazioni.
La più importante decisione da prendere è quella su quali dati aziendali sono presenti e gestiti dal servizio "Nuvoloso" Pubblico. E' ovvio che il valore dei dati è la variabile più importante per poter dare risposta alla domanda precedente. Ad esempio, se i dati presenti sul servizio "Nuvoloso" Pubblico fossero tutti e soli dati rappresentanti informazioni già pubbliche, dalle brochure pubblicitarie ai listini prezzi al pubblico, nulla succederebbe. Se invece i dati fossero il segreto industriale sul quale si base il futuro dell'azienda, le conseguenze sarebbero catastrofiche.
L'azienda (od il privato cittadino) deve quindi scegliere molto accuratamente i dati e le informazioni trattate dal servizio "Nuvoloso" Pubblico ed essere pronto all'evenienza che queste possano diventare pubbliche.

Purtroppo questo è fatto molto raramente perché ci si affida sul fatto che il fornitore garantisca in maniera assoluta la protezione dei dati e che li gestisca secondo i principi di ogni singola azienda o persona. In realtà, come le ben note vicissitudini di Facebook ci insegnano, è esattamente il contrario: i dati e le informazioni sono di solito gestiti secondo le procedure, i principi e la convenienza del fornitore sino ai casi estremi ove i dati stessi diventano proprietà del fornitore che li può quindi utilizzare a proprio piacimento.

La protezione dei dati

Se da un lato bisogna valutare realisticamente l'evento di divulgazione o utilizzo dei dati a/da altri, dall'altro quello che è possibile fare è ridurre la probabilità della sua evenienza, ovvero proteggere i dati.

Anche in questo caso la situazione è più complessa e pericolosa rispetto al caso tradizionale di Outsourcing. Per inquadrare il problema, ricordiamo come la sicurezza ICT è stata implementata in pratica sino ad oggi. L'approccio è quello della protezione esterna ai dati ed alle applicazioni: abbiamo firewall, segmentazione di reti, proxy, IPS, protezioni fisiche ecc. Ben poco, se non nulla, è fatto a livello dei dati stessi.

Ora nel caso di servizi “Nuvolosi”, tutte queste misure di sicurezza non sono disponibili, o meglio sono utilizzate dal fornitore di servizi per proteggere i propri assets, la sua infrastruttura e le sue applicazioni, ma non per proteggere i dati dei clienti. Combinando questo con la delocalizzazione dei dati e servizi, l'utilizzo comune delle risorse da parte di molti clienti anch'essi delocalizzati, ne consegue che non è possibile proteggere i dati dall'esterno ma che questi devono essere protetti “dall'interno”.

Nella lista dei rischi, bisogna anche tenere conto del fatto che non solo i dati potrebbero essere accessibili a tutti da internet, ma che anche altri clienti dello stesso servizio potrebbero accedervi e che sicuramente vi accedono i sistemisti e il personale tecnico del fornitore e di tutti i suoi sub-contractor.

A parte la problematica della nomina ad amministratore di sistema secondo i provvedimenti del Garante della Privacy di tutto questo personale difficilmente identificabile, questo rende improponibile una protezione esterna dei dati.

Ma proteggere i dati dall'interno non è facile e non abbiamo oggi molti strumenti per farlo. In realtà l'unico approccio è quello di cifrare i dati, ma questo non sempre è possibile sia in teoria che in pratica.

In teoria la cifratura dei dati può impedire il trattamento e l'elaborazione dei dati stessi: se il servizio deve elaborare i dati e non solo conservarli, i dati devono essere accessibili al servizio stesso in modalità non cifrata. Si può immaginare che i dati siano decifrati solo per il tempo necessario alla loro elaborazione e poi immediatamente cifrati nuovamente, ma questo tipicamente richiede riscrivere buona parte delle nostre applicazioni. Inoltre, tecnicamente la soluzione deve fare in modo che la chiave di cifratura/decifrazione dei dati sia ignota al fornitore di servizi e nota solo al cliente finale.

In teoria la procedura dovrebbe essere la seguente: cifratura dei dati presso la sede del cliente prima dell'invio al fornitore, trasporto dei dati cifrati sui sistemi del fornitore, decifrazione dei dati sui sistemi del fornitore per il solo tempo necessario alla loro elaborazione ed in modo tale da non poter essere acceduti dal fornitore stesso, ri-cifratura dei dati elaborati.

Se il servizio è quello di backup remoto nel quale non è necessaria alcuna elaborazione e quindi decifrazione sui sistemi del fornitore, questa procedura è implementabile ed è stata implementata, altrimenti oggi è difficilmente realizzabile.

Quello che in pratica si può fare oggi per proteggere i dati è:

- selezionare accuratamente i dati
- cifrare (od almeno far cifrare dal fornitore) i dati quando possibile e soprattutto quando sono archiviati o su disco
- “mascherare” i dati particolarmente sensibili mantenendo il dato reale in azienda ed inviando al fornitore solo parte dei dati, quelli strettamente necessari all'elaborazione il più possibile in forma “anonima”.

Concludendo

L'utilizzo di servizi “Nuvolosi” è sicuramente non solo economicamente conveniente, ma anche utile a migliorare il proprio modo di lavorare e fornire nuove possibilità di sviluppo e accesso a nuovi mercati. E' inevitabile che i servizi sulle “Nuvole” divengano sempre più parte fondamentale del modo di fare ICT nel prossimo futuro, ma questi strumenti devono essere affrontati ed utilizzati nel modo corretto.

I rischi di utilizzo di servizi "Nuvolosi" Pubblici sono molti, quelli descritti precedentemente sono solo i più ovvi ed immediati. Nelle tre tabelle che seguono ne indichiamo alcuni altri che sicuramente devono essere valutati ma che sono solo degli spunti per una completa valutazione del rischio.
Altri modi di utilizzo delle "Nuvole" sono possibili, in primo luogo le "Nuvole" Private, in pratica l'approccio opposto a quello Pubblico. In questo caso i problemi di sicurezza dei dati sono risolti a priori, ma le problematiche che sorgono sono ad esempio sul costo e la funzionalità dell'infrastruttura stessa.
Le "Nuvole" sono un vecchio approccio declinato al presente e sicuramente valido per il futuro: sono qui per restare e dobbiamo imparare a sfruttare al meglio le grandi possibilità che ci offrono, legate non solo al risparmio economico ma forse e soprattutto alla possibilità di astrarre i servizi ICT sia dal luogo che dalla modalità di produzione e fruizione.

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
- *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

Controllo e Sicurezza degli Accessi (anche Admin)
Condivisione piattaforma (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

Tabella 1. Alcuni rischi relativi alla sicurezza dei dati

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 del fornitore • Inter-operabilità tra fornitori

Tabella 2. Alcuni rischi relativi alla disponibilità e provisioning dei servizi

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

Tabella 3. Alcuni rischi relativi alla compliance

Andrea Pasquinucci (PhD CISA CISSP, socio AIEA) è un consulente freelance in sicurezza informatica. Si occupa prevalentemente di progetti di sicurezza ICT, audit, compliance, governance e formazione ICT per il management ed il personale tecnico. In particolare è esperto di sicurezza delle reti e dei servizi web, dei sistemi operativi e di crittografia.