Usare il Cloud in sicurezza: spunti tecnici

Cesare Gallotti

Milano, 24 gennaio 2012

Agenda

- Presentazione relatore
- Definizioni
- Elementi di sicurezza per il cloud
- Qualche dubbio

- Presentazione relatore
- Definizioni
- Elementi di sicurezza per il cloud
- Qualche dubbio

Cesare Gallotti

- Lead Auditor ISO/IEC 27001 (CEPAS), ISO 9001:2000 (IRCA), ISO/IEC 20000-1 (itSMF); ITIL Expert (Exin); CISA; Computer Forensics (Specializzazione Post Universitaria), CBCI (BCI)
- Esperienze pregresse
  - > Consulente, Responsabile di progetti e formatore in ambito ISMS e ITSMS per società di consulenza italiane (Securteam, Intesis, Quint)
  - > Lead Auditor e ICT Technical Responsible per DNV Italia (auditing, sviluppo tecnico degli schemi di certificazione collegati agli standard ISO 9001, ISO/IEC 27001 e ISO/IEC 20000-1; sviluppo della relativa formazione)
- Attualmente consulente libero professionista:
  - > Consulenza in ambito ISMS, QMS, ITSM, Risk Assessment e Privacy
  - > Auditor di terza parte per la sicurezza delle informazioni, qualità e altro
  - > Formatore per corsi LA ISO/IEC 27001, ITIL Foundation e Quality Assurance
  - > Attività in Europa, Africa and Asia per clienti di diversi settori di mercato

- Presentazione relatore
- Definizioni
- Elementi di sicurezza per il cloud
- Qualche dubbio

Cos'è il cloud computing

- Il cloud computing è un modello per fornire accesso via rete a risorse condivise con altri utenti, disponibili, convenienti e su richiesta
- Caratteristiche:
  - diffuso accesso via rete
  - rapida scalabilità
  - servizi misurabili
  - disponibilità su richiesta
  - gestione autonoma (self-service)
  - risorse aggregabili

Modelli di cloud

- Modelli di servizio:
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Modello di erogazione:
  - Pubblico
  - Privato
  - Ibrido

IaaS, PaaS; SaaS

- IaaS: le funzionalità offerte comprendono capacità computazionale, storage, connettività e altre componenti fondamentali con le quali un cliente può installare e gestire qualsiasi software, inclusi sistemi operativi e applicazioni. Il cliente non gestisce o controlla l'infrastruttura cloud sottostante, ma ha il controllo del sistema operativo, dello storage, delle applicazioni installate e un controllo limitato di alcune componenti di rete (es. firewall)
  - Solitamente sono forniti dei modelli di sistemi operativi da utilizzare.
- PaaS: le funzionalità offerte permettono al cliente di installare delle applicazioni, purché compatibili con la piattaforma. Il cliente non gestisce o controlla l'infrastruttura, ma le applicazioni installate e alcune configurazioni dell'ambiente operativo.
- SaaS: le funzionalità offerte sono quelle delle applicazioni, accessibili da diversi client (incluso un web browser, come ad esempio la web mail). Il cliente non gestisce o controlla l'infrastruttura sottostante e controlla solo alcune limitate configurazioni dell'applicazione.
  - tra le configurazioni controllabili dal cliente vi sono gli utenti e le autorizzazioni correlate

- Presentazione relatore
- Definizioni
- Elementi di sicurezza per il cloud
- Qualche dubbio

Dove si applica la sicurezza?

- Sicurezza contrattuale
- Sicurezza tecnica lato cliente
- Sicurezza tecnica lato fornitore (non trattata nel seguito)

- Ricordiamo i 3 assi della sicurezza:
  - prevenzione
  - rilevazione
  - recupero

I punti chiave

- Definire modalità di gestione dei contratti
- Condurre un'analisi dei rischi
- Definire modalità di valutazione dei fornitori (anche rispetto alla affidabilità e la durabilità; eventuale due diligence)
- Valutare (ed eventualmente migliorare) la disponibilità e le competenze del personale interno
- Definire (e successivamente attivare) modalità di controllo del servizio
- Prevedere, prima della migrazione verso cloud esterni, le modalità da seguire nel caso in cui si volesse, in futuro, cambiare fornitore o fare insourcing (anche se oggi potrebbe apparire improbabile)

Sicurezza contrattuale – Requisiti generali

- I requisiti contrattuali applicabili a tutti i contratti sono:
  - ruoli e responsabilità anche privacy
  - clausole di riservatezza
  - modalità di rescissione del contratto
  - diritto di audit (non solo verifiche, anche Vulnerability Assessment o Pen Test)
- E' opzionale il seguente requisito, da trattare con il dovuto rigore:
  - certificazioni sulle ultime versioni (secondo i regolamenti degli Organismi di Certificazione) ISO 9001, ISO/IEC 20000-1, ISO/IEC 27001, con ambito che copre i servizi cloud sui siti pertinenti (dove applicabile), rilasciato da un Organismo di Certificazione accreditato da un Ente membro degli EA MLA

Sui contratti

- I livelli di servizio e i requisiti devono essere stipulati contrattualmente
  - > contratti negoziabili
  - > contratti non negoziabili
- Il cliente è sempre tenuto ad amministrare tutte le configurazioni sotto il proprio controllo.
- Si ricordi che alcune attività operative possono essere trasferite ad altri, ma le responsabilità rimangono in carico al cliente.

Gestione del contratto e del servizio

- A livello di contratto, prevedere e successivamente attuare in fase di erogazione del servizio:
  - incontri periodici di riesame report e servizio
  - controllo dei change da parte dei fornitori, che prevedano il preavviso al cliente
  - rilascio di reportistica (a livello di granularità opportuna) su disponibilità, trattamento ticket, incidenti
  - scelta del sistema di ticketing e definizione delle modalità di comunicazione degli incidenti
  - definizione di SLAs sui tempi di gestione e di soluzione dei ticket
  - specifiche di BCM (anche organizzativo, considerando il Service Desk)
  - disponibilità di manualistica aggiornata
  - modalità di conduzione di vulnerability assessment

SLAs di disponibilità

- Disponibilità
  - > SLAs di disponibilità a livello di singolo servizio e di singola componente (non solo tecnologica); la disponibilità deve essere calcolata end-to-end, dopo aver definito il perimetro del fornitore (p.e: router di frontiera del cliente)
  - > modalità di backup e di ripristino
  - > tempi di ripristino a fronte di eventi straordinari (da verificarne la coerenza con le proprie esigenze)
  - > modalità (e costi...) di gestione dei test di ripristino

Requisiti per tutti i servizi IT

- Applicabile a tutti i servizi IT:
  - termini di proprietà del software e dei dati installati
  - localizzazione dei server (se necessaria, soprattutto se si trattano dati personali)
- Importante, per tutti i servizi:
  - sicurezza dei canali di comunicazione (cifratura, gestione utenze e password)
  - chi può accedere ai dati (lato fornitore)
  - possibilità di cifratura dei dati (da valutare con attenzione)

Requisiti per alcuni servizi IT

- Sicurezza della rete (applicabile a IaaS e PaaS):
  - > tipologia di meccanismi di sicurezza di rete (firewall, IDS, segmentazione interna)
- Classificazione e trattamento delle informazioni (applicabile a SaaS)
  - > se sono in vigore presso il cliente delle procedure di classificazione e trattamento e controllo delle informazioni, verificare se il servizio è compatibile con esse

Misure di sicurezza facoltative

- Non è sempre necessario richiedere al fornitore le seguenti misure:
  - descrizione delle specifiche di sicurezza fisica delle sale server (accesso limitato, presenza sistema antincendio, presenza aria condizionata con temperatura controllata)
  - presenza e utilizzo di UPS e generatori ridondati (con ovvia doppia alimentazione delle macchine)
  - duplicazione delle linee di connessione e dei POP

Cosa deve fare il cliente – IaaS e PaaS

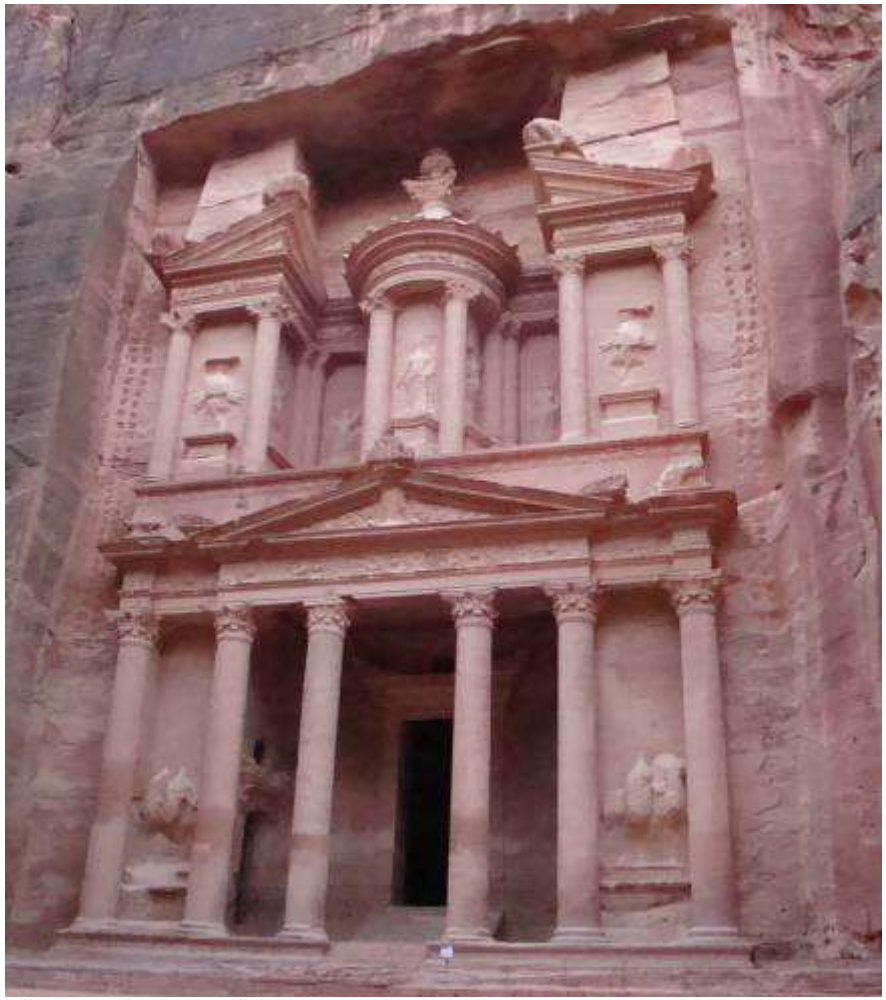
- Verificare le configurazioni dei sistemi installati o template offerti (IaaS)
  - servizi inutili
  - utenze inutili
  - opzioni di default
  - eventuali backdoor del fornitore
- Installare dei sistemi di monitoraggio delle prestazioni del sistema (capacità CPU, RAM, memoria, banda di rete)

Cosa deve fare il cliente – SaaS

- Accertarsi della sicurezza applicativa garantita dai servizi SaaS.
- Alcuni metodi sono i seguenti:
  - verificare documentazione basata sull'Annex A della ISO/IEC 27001
  - verificare il protection profile applicato conforme alla ISO/IEC 15408 (Common Criteria)
  - condurre dei Penetration Test o dei Code Review
- Altri punti da verificare:
  - modalità di controllo accessi
  - ruoli e profili disponibili
- Alcune di queste tecniche potrebbero essere seguite anche per validare gli strumenti utilizzati dagli operatori, in caso di IaaS o PaaS

Cosa deve fare il cliente – Backup

- Attivare un sistema di backup, senza basarsi su quello offerto dal fornitore (il sistema di backup deve essere dimensionato a seconda delle prestazioni offerte dal fornitore e deve essere testato)
  - > può essere complesso per i SaaS, ma dovrebbe essere verificato



Cosa deve fare il fornitore - Organizzazione

- Politica per la sicurezza e direzione aziendale
  - il rigore, entro certi limiti, paga
  - è la Direzione che guida l'impresa
- Ruoli e responsabilità
  - non solo privacy
- Formazione
  - sulle tecnologie specifiche
  - costi che poi si ripagano
- Relazioni tra vendita e produzione
  - evitare di vendere servizi non sostenibili
- Relazioni fornitore – cliente
  - ruoli (non solo privacy)
  - contratto

Cosa deve fare il fornitore – Tecnologie e non solo

- Oltre alle "solite" best practices (sicurezza fisica e logica)
- Scegliere attentamente i prodotti (non i produttori!)
- CMDB e discovery
  - > evitare la proliferazione delle macchine
- Standardizzare
  - > può sembrare noioso, ma è fondamentale
  - > non irrigidirsi
- Procedure tecniche e di processo
  - > stabilire chiaramente chi fa cosa
  - > garantire la ripetibilità (p.e. delle configurazioni)
- Gestire i change in modo controllato
  - > anche se richiede tempo: la frenesia non paga
- Attenzione ai processi di Business Continuity, Incident e Problem Management

- Presentazione relatore
- Definizioni
- Elementi di sicurezza per il cloud
- Qualche dubbio

I dubbi

- Quanto abbiamo detto del IaaS non è applicabile ai servizi di housing su hardware del fornitore stesso?
- Quanto abbiamo detto del PaaS non è applicabile ai servizi di hosting?
- Quanto abbiamo detto del SaaS non è applicabile a servizi quali gestione del mail server?

Domande finali

- E’ il caso di parlare di “cloud security”?
- Non è il caso di parlare di “sicurezza dei fornitori dei servizi IT”?
- Perché il Cloud Security Alliance non cambia nome in “IT Service Outsourcing Security Alliance?

Grazie!

- Cesare Gallotti
  cesaregallotti@cesaregallotti.it
  http://www.cesaregallotti.it
  http://blog.cesaregallotti.it
  PEC: cesaregallotti@mailcert.it