Paolo Giardini
STUDIO GIARDINI
Eucip Certified Informatics Professional
Direttore OPSI – Osservatorio Privacy e Sicurezza Informatica
Centro di Competenza Open Source Regione Umbria
GNU/LUG Perugia
AIP – OPSI – AIPSI - CLUSIT ISSA - FORMEZ

Privacy e sicurezza nel cloud.

Cosa tenere presente quando si sceglie un servizio

Chi sono? ;-)

- Direttore Osservatorio Privacy Sicurezza Informatica
- Privacy Officer Associazione Informatici Professionisti
- Consulente per la sicurezza delle informazioni
- Membro comitato esecutivo CCOS Regione Umbria
- Socio Fondatore GNU/LUG Perugia
- Partecipo a varie associazioni e community: Sikurezza.org, Italian Linux Society, CLUSIT, Information Systems Security Association, Associazione Italiana Professionisti Sicurezza Informatica, Giuristi Telematici, Hackers Corner, ...
- Ideatore ed organizzatore dell'hacker game *“Cracca al Tesoro”*

Di cosa parleremo

- Chiariamoci alcune idee sul “cloud computing”
- ...Tutto oro quello che luccica?
- Parliamo di Privacy
- e anche di Sicurezza
- Le cose da considerare al momento della scelta di un servizio cloud
- Conclusioni (che invece sono un inizio)

Cosa si intende con “Cloud”?

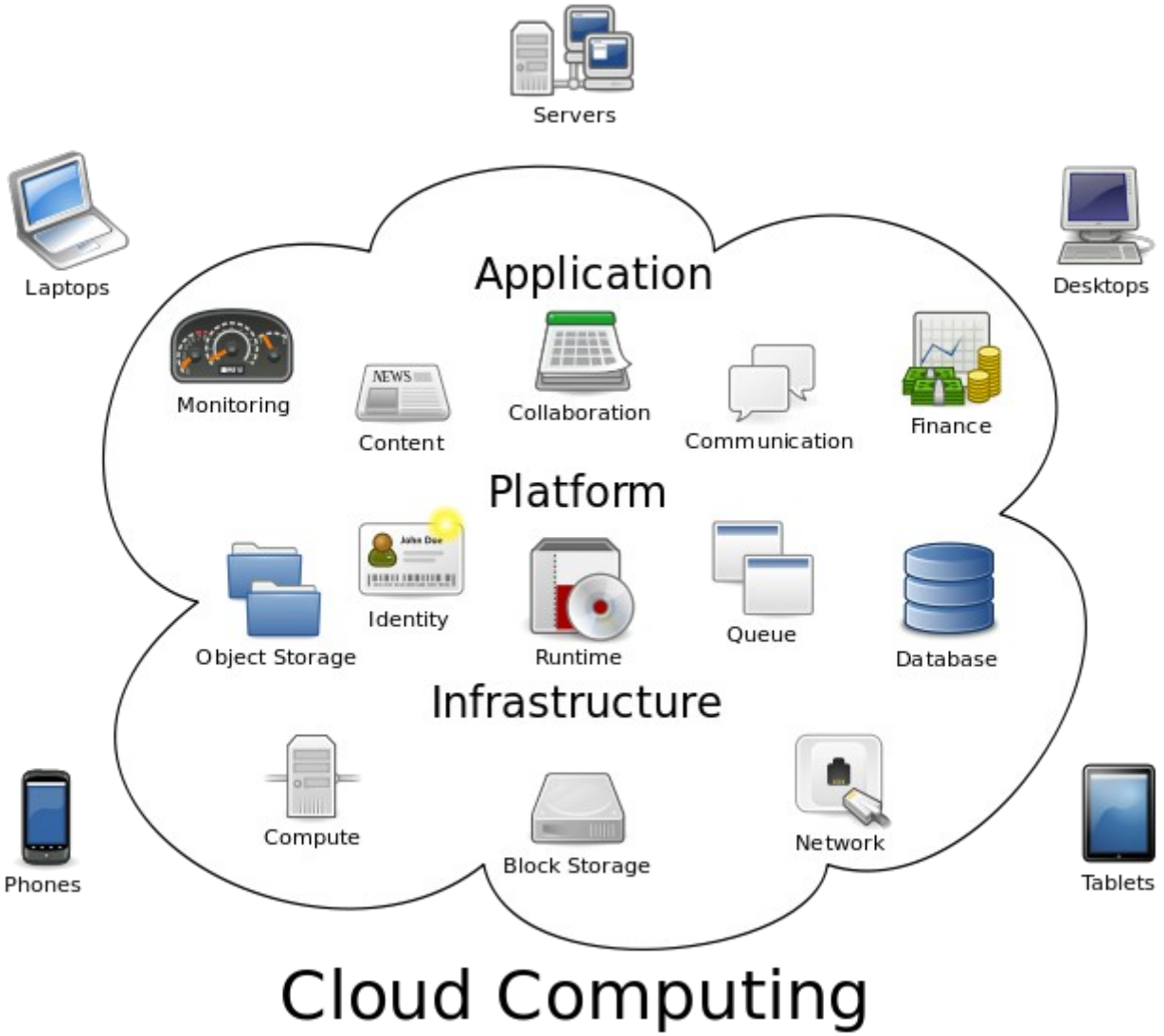


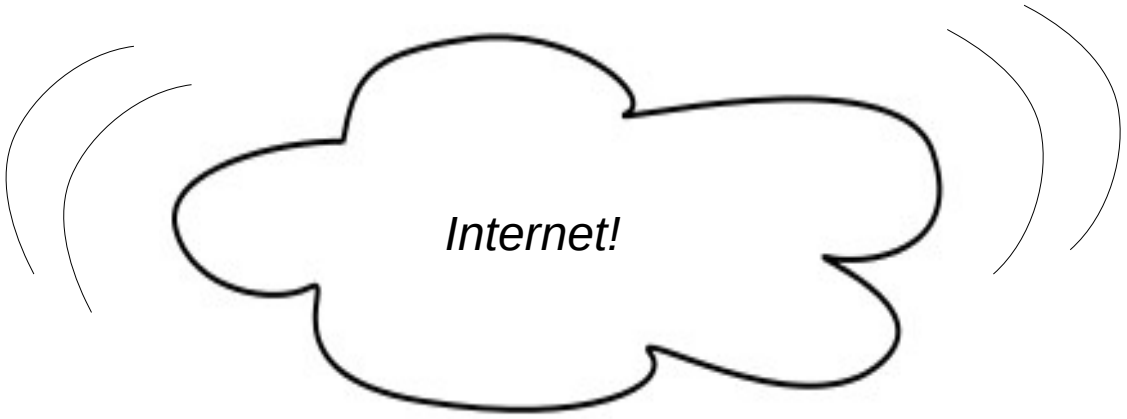
Immagine tratta da Wikipedia

Cloud, ovvero: ...

- Una definizione semplicistica è: qualunque servizio offerto via internet
- In questa definizione rientrerebbe qualunque Data Center!

Cloud, ovvero: nuvola!

- Il nome deriva dal simbolo della “nuvoletta” usato nei diagrammi di flusso per indicare “internet”
- In realtà un cloud “vero” impiega un “mix” di varie tecnologie al fine di offrire riconosciuti vantaggi agli utenti

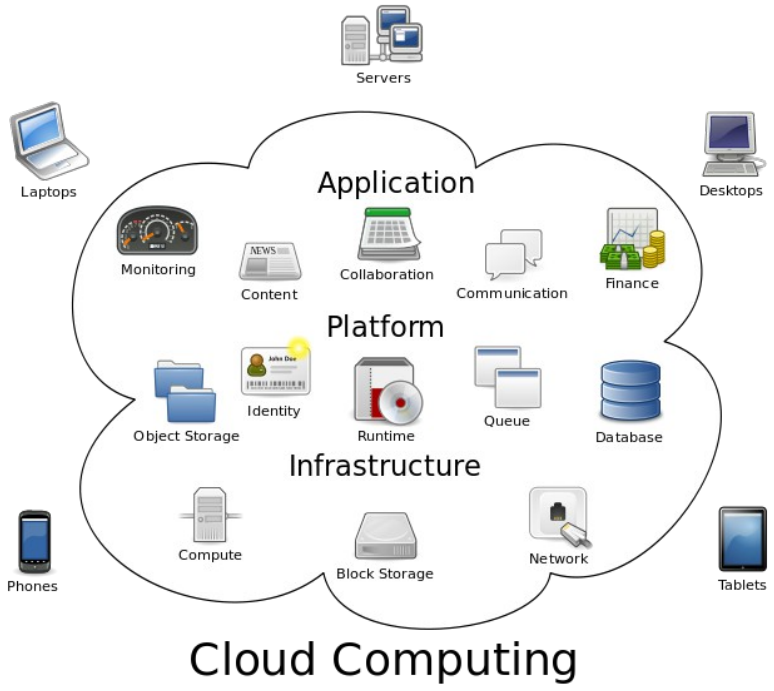


Tipi di cloud

- Private cloud
  - L'infrastruttura è localizzata presso l'utente che ne dispone totalmente e la gestisce in piena autonomia, in proprio o tramite terzi, sfruttandone i vantaggi tecnologici (ottimizzazione, scalabilità,...)
  - I dati restano presso la struttura dell'utente
- Public cloud
  - L'infrastruttura di proprietà di un fornitore mette a disposizione dei clienti (multipli) i propri servizi tramite internet
  - Il controllo dei dati è in parte ceduto al gestore del cloud
- Altri cloud
  - Soluzioni miste (hybrid cloud) o condivise (community cloud)

Modelli di servizi Cloud

- Software as a Service (SaaS)
  - Sono messe a disposizione applicazioni (es. Mail, suite per ufficio...)
- Platform as a Service (PaaS)
  - Sistemi e servizi per lo sviluppo di applicazioni (da rivendere)
- Infrastructure as a Service (IaaS)
  - Vengono messi a disposizione sistemi virtualizzati HW e SW (server, sistemi per il backup..)



Modelli di servizi Cloud

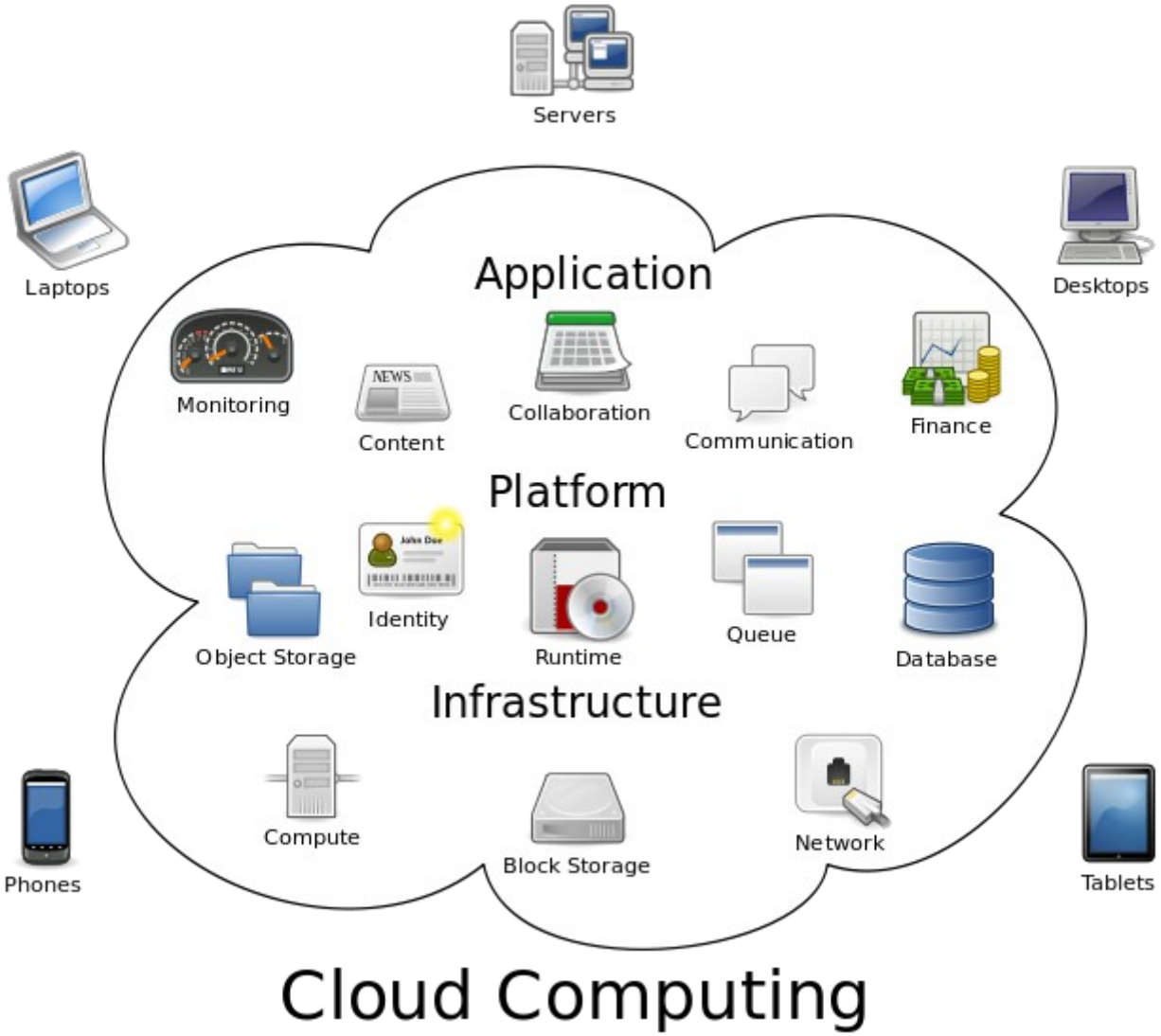


Immagine tratta da Wikipedia

alcuni servizi che sfruttano il cloud

aruba CLOUD.it COMPUTING

iCloud

amazon web services

Picasa

Dropbox

SCALITY

tiscali:

cloud drive

SkyDrive

La Nuvola Italiana.

TELECOM ITALIA

pulse

BEST BUY

gigya

claritics

DNAnexus

Opinioni diverse

- Per alcuni è un innegabile vantaggio
- Per altri è un nuovo nome inventato dal marketing per servizi già conosciuti
- E' pur vero che alcuni fornitori potrebbero spacciare per “cloud” il vecchio servizio di data center
- Un “cloud vero” può effettivamente offrire vantaggi importanti, se il progetto è ben pensato!

Alcuni vantaggi del Cloud

- Riduzione dei costi per l'implementazione della infrastruttura
- Minore richiesta di risorse interne per personale specializzato
- Scalabilità della soluzione al crescere delle esigenze
- Indipendenza dalla locazione geografica dell'utente
- Riduzione dei costi di gestione e manutenzione

Alcune problematiche

- Minore controllo sui dati, essendo localizzati presso le strutture del provider (dove?)
- Dipendenza da terze parti (il provider), difficoltà nella migrazione e interoperabilità (tecnologie proprietarie)
- Privacy e confidenzialità dei dati riservati (perdita della riservatezza dei dati, distruzione, furto di informazioni sensibili, ad esempio brevetti, contabilità, contratti,..)
- Sicurezza (sicurezza presso il provider, hijacking delle comunicazioni, sicurezza presso l'utente, affidabilità operatori, ...)
- Compliance Normativa e contrattuale (norme privacy europee, clausole contrattuali con clienti, certificazioni – p.e. PCI DSS - Payment Card Industry Data Security Standard)
- Contratto con il provider (gestione dei dati nel cloud, uptime e disponibilità, migrazione, assistenza, ...)
- Infrastruttura lato client (connessione sempre disponibile, veloce ed affidabile, sicura... ADSL!?)

Privacy e Cloud

- Che tipo di dati andrò a trattare? (ovvero: quali tipi di dati andrò a trasferire sul cloud)?
  - Sono dati personali?
  - Sono dati sensibili?
- Dove saranno effettivamente localizzati?
  - Su sistemi all'interno dell'Unione Europea?
  - Fuori Europa? Il paese ospitante ha una normativa equivalente a quella Europea o vi sono particolari accordi (Es. Safe Harbor con gli USA)?
- Chi avrà la possibilità di trattare I miei dati?
  - Posso nominarlo Responsabile Esterno del trattamento?
  - In quale modo potrò esercitare l'obbligo di controllo previsto dalla normativa sulla Protezione dei Dati Personali (privacy)?

Privacy e Cloud

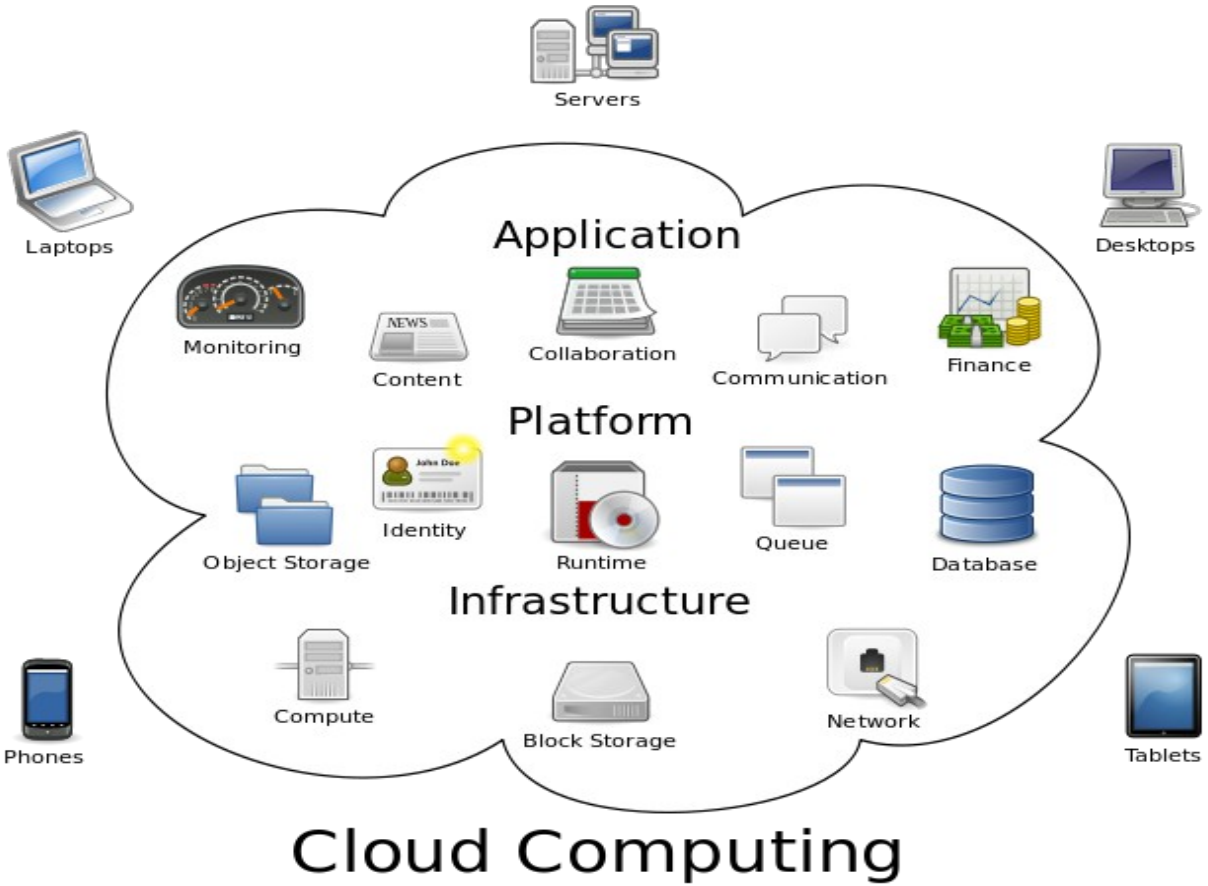
- Il vademecum del Garante Privacy focalizza alcuni punti da tenere presenti al momento di decidere sull'utilizzo di servizi cloud
- Con il nuovo Regolamento Europeo arrivano novità importanti
  - Privacy by design
  - Privacy Impact Assessment
  - Data Protection Officer

Cloud e sicurezza

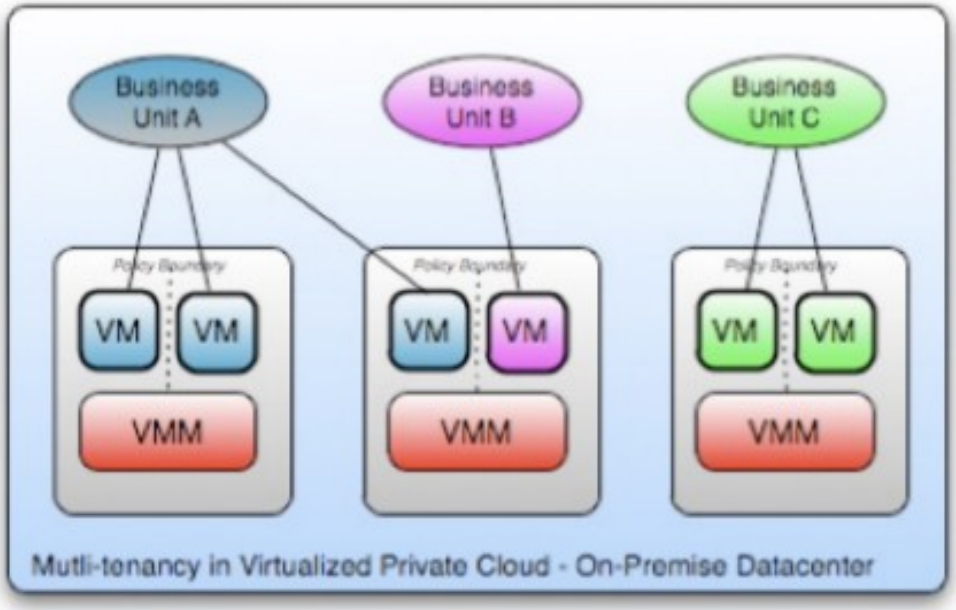
- L'adozione di sistemi cloud nella propria organizzazione non elimina i problemi di sicurezza
  - Le problematiche di sicurezza “locali” rimangono tali e quali
  - Vengono invece aggiunti nuovi livelli da tenere in considerazione

Livelli di (in)Sicurezza cloud

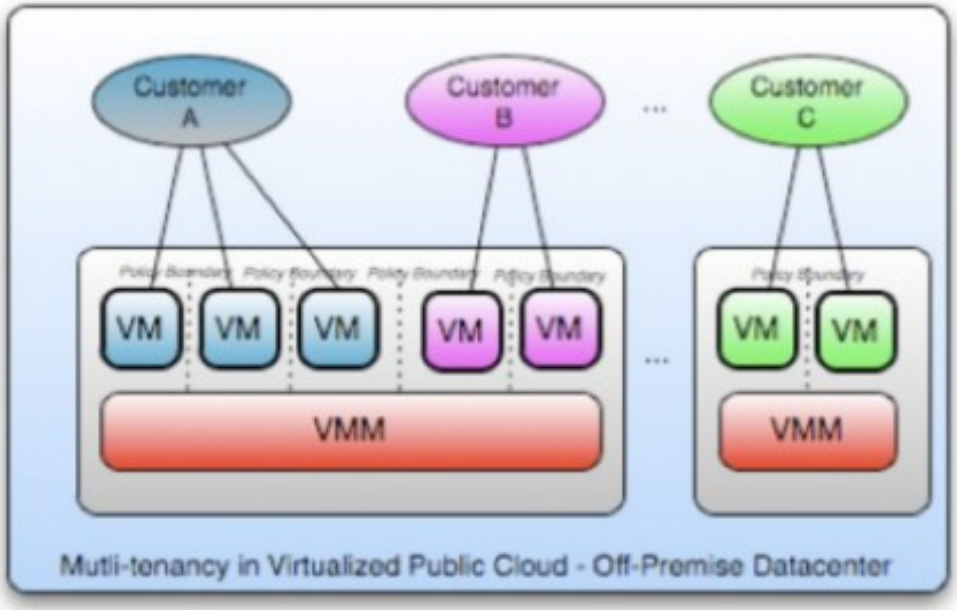
- Potete acquistare un servizio Public Cloud, ma non l'infrastruttura, ed almeno parte di essa è condivisa con altri (multi-tenancy)
- Ricordate i tre livelli di servizi cloud?



Livelli di (in)Sicurezza cloud



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

Fonte: Cloud Security Alliance Italy

- Per ognuno di essi sono possibili specifiche vulnerabilità relative al fattore di condivisione di risorse HW, applicazioni, connessioni, librerie, database,...

Non solo *"hackers"*

CSA (Cloud Security Alliance) ha pubblicato in febbraio un rapporto nel quale si evidenziano le 9 maggiori minacce per la sicurezza del cloud computing

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Malicious Insiders
6. Abuse of Cloud Services
7. Insufficient Due Diligence
8. Shared Technology Issues
9. Denial of Service

Alcune delle domande da porsi

- La propria infrastruttura è adeguata?
- La connessione Internet supporta il carico previsto?
- Quali possibilità ho in caso di fault locale per continuare a lavorare?
- Gli operatori sono adeguatamente formati?
- Quali modalità di ripristino in caso di fault del provider? (attacchi informatici, disastri naturali, fallimento...)

Contratti cloud

- E' difficile poter contrattare clausole particolari specie se si è una piccola azienda
- Esaminare bene il contratto, obblighi e garanzie
- Selezionare più fornitori che offrano il servizio richiesto e confrontare non solo i costi
- A proposito: attenzione ai costi nascosti!

Clausole contrattuali

- SLA, Service Level Agreement
- Gelocalizzazione dei dati
- Garanzia di accesso e di riservatezza
- Cancellazione sicura dei dati
- Responsabilità e modalità di backup e disaster recovery
- Modalità di audit e di valutazione delle certificazioni
- Possibilità e supporto a migrazione ed interoperabilità
- Distruzione dei dati dopo la cessazione del rapporto
- E' il caso di pensare ad una assicurazione? (trasferimento del rischio)
- Che di pensate di penali per eventuali inadempienze?
- Individuare eventuali terzi che partecipino alla fornitura del servizio

Riepiloghiamo!

- Esistono vari livelli di problematiche da affrontare
  - Sicurezza locale → non cambia molto. Va curata particolarmente la formazione degli operatori
  - Compliance privacy → si devono valutare normative e altri obblighi in rapporto ai dati trattati
  - Comunicazioni → deve essere garantita la sicurezza e la affidabilità delle connessioni
  - Sicurezza lato cloud → valutare bene il fornitore, si dovrà lavorare sulla parte contrattuale

Conclusioni

- Esistono molte soluzioni possibili sul mercato
- L'importante è effettuare una buona analisi preventiva sui dati da trattare e sulle necessità
- E' necessario definire ed applicare delle valide policy di sicurezza
- Scegliere un prodotto valutando anche le policy e le clausole contrattuali e non solo il lato economico
- Valutare se richiedere specifiche clausole

GRAZIE PER L'ATTENZIONE

paolo.giardini@solution.it

Link di approfondimento sull'argomento

https://en.wikipedia.org/wiki/Cloud_computing – http://www.garanteprivacy.it
http://www.cloudsecurityalliance.it - http://opsi.aipnet.it - http://www.aipnet.it http://www.solution.it
http://blog.solution.it - http://www.enterthecloud.it