UNIVERSITÁ DEGLI STUDI DI TERAMO

Cloud e strumenti collaborativi

Roberto Salvatori
Università di Teramo

Cloud Computing: Aspetti di sicurezza Terza parte

III. Considerazioni di Sicurezza

Aspetti caratterizzanti un servizio di Cloud Storage

- Sicurezza:
  - Crittazione dei dati sul server di storage
  - Crittazione dei dati lato client
  - Coinvolgimento di risorse storage di terze parti (Amazon S3)
  - Terms of Services / SLA / PLA
  - Modalità di rilascio credenziali AAI (chiavi, password,

- Protocolli Supportati lato Risorsa di Storage inclusa:
  - Amazon S3
  - WebDAV
  - CIFS
  - http(s)
  - Sftp/sshfs
  - Fuse
  - Local mounted filesystem (ext3, ntfs,..)
  - glusterFS
  - XtreemFS
  - NFS
  - ftp

- Protocolli lato Client
  - http / WebDAV
  - Mobile / Android , iOS
  - Fuse
  - PC-client (Win, Linux, MacOS..) di sincronizzazione

Cosa determina complessivamente la sicurezza dei nostri dati utilizzando un servizio di Cloud Storage ?

- Sicurezza dei protocolli Layer2-Layer 1 nei Data Center
  - Crittazione o meno dei dati sul server di storage / Soluzioni h/w specifiche dedicate
  - Fabric protocols : NFS/ CIFS / SATA / AoE / iSCSI / FC

- Sicurezza dei protocolli dei filesystem aggregativi
  - GlusterFS
  - Oracle Cloud Filesystem
  - HadoopFS
  - NFS
  - GPFS
  - Lustre

- Policy di Sicurezza dei Data Center
  - Firewalling
  - IDS
  - Networking/VPN isolation
  - Networking tra i data centers di uno stesso Cloud Provider

- Sicurezza al livello architetturale del Cloud Storage system e clients
  - Front End
  - Data Encryption
  - Soluzioni di Load Balancing / High Availability / DCN
  - Protocollo specifico Client-Server Cloud Storage Protocol
  - Metadati / InformationSystem (DB sql / nosql / ..)
  - Sicurezza nelle policy e meccanismi di condivisione folders / file
  - Georeplica dei dati / Ridondanza / DCN

Layers architetturali Storage Cloud