SICUREZZA INFORMATICA

CLOUD COMPUTING

Uso consapevole del *Cloud*

Ver.1.0, 10 luglio 2015

Pagina lasciata intenzionalmente bianca

1. IL *CLOUD COMPUTING*

Il continuo aumento delle richieste di servizi informatici, necessari per soddisfare le esigenze degli utenti e delle imprese, ha portato ad un incremento del numero di server utilizzati nei data center (*Service Provider*) e ad un maggiore uso della virtualizzazione come tecnica di memorizzazione. Il risultato di questa recente evoluzione ha contribuito all'introduzione di un nuovo tipo di tecnologia: il *Cloud Computing* ("nuvola informatica").

La definizione di *Cloud Computing* data dal NIST (*National Institute of Standards and Technology*) nel Settembre 2011, è la seguente:

> *"Il Cloud Computing è un modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi."*

In sostanza il *Cloud Computing* è una delocalizzazione delle risorse di elaborazione, di memorizzazione e di contenuti, distribuiti e raggiungibili attraverso la rete. Questo porta ad un aumento della capacità di memoria fisica e di elaborazione, spostando la gestione dei dati dai singoli computer, distribuiti e/o indipendenti, a strutture centralizzate, e ad un conseguente vantaggio economico dovuto ad una riduzione dei costi per *hardware*, *software* e per i servizi in generale.

I vantaggi che la tecnologia *Cloud* offre agli utilizzatori, possono essere raggruppati nelle seguenti categorie:

- **maggiore flessibilità e mobilità** consentendo l'accesso ai propri dati sia da un qualsiasi dispositivo mobile (come uno *smartphone* o un *tablet*), sia da uno fisso (come un *PC* o un *server*);
- **maggiore capacità d'immagazzinamento** dei dati e riduzione dei costi rispetto a soluzioni tradizionali distribuite.

La figura che segue schematizza ciò che il *Cloud* oggi rappresenta e quali sono i dispositivi e gli utenti finali dei servizi che sfruttano tale modello.Sono proprio questi vantaggi e la possibilità/convenienza di averli in *outsourcing* che continuano a guidare il crescente utilizzo del *Cloud Computing*. Tuttavia, man mano che le organizzazioni che si rivolgono al *Cloud Computing* aumentano, divengono sempre più evidenti i rischi associati al suo utilizzo, primo fra tutti la sicurezza dei dati.

La sicurezza dei dati è un elemento essenziale per privati e aziende. Le politiche di sicurezza, oltre a garantire la conformità dell'organizzazione a leggi e regolamenti vigenti, sono sviluppate per proteggere le informazioni dei clienti. Quando utilizzano il *Cloud* per archiviare e processare i propri dati a distanza, le organizzazioni assoggettano le informazioni sensibili alle pratiche di sicurezza del *Service Provider* che ha il compito di assicurarsi che sia posta in atto un'adeguata protezione.

2. RISCHI E MINACCE

I rischi associati al *Cloud Computing* dipendono naturalmente da diversi fattori come il tipo di attività, la quantità e la tipologia dei dati e il fornitore del servizio selezionato. In particolare le principali criticità riguardano questioni come la posizione, l'accesso e il recupero dei dati nel *Cloud*.

Un primo aspetto implica che chi utilizza il *Cloud* non sia generalmente a conoscenza della posizione fisica dei dati affidati al fornitore del servizio. Nel corso del normale svolgimento dell'attività, l'ubicazione fisica dei dati può apparire irrilevante. Tuttavia, il luogo dove si trovano i dati determina il tipo di normativa applicabile per la loro protezione e sorveglianza. Un secondo aspetto implica che i clienti del *Cloud* devono informarsi su chi gestirà i dati archiviati in remoto. Le organizzazioni mantengono il controllo sull'accesso degli utenti ma anche alcuni membri del team del fornitore del servizio acquisiranno l'accesso alle informazioni. Infine, i clienti del *Cloud* devono interessarsi alle pratiche e alle procedure adottate dal fornitore di servizio in materia di recupero dei dati in caso di violazione della sicurezza o perdita dei dati.

La continua crescita del mercato del *Cloud Computing* ha portato alla nascita di un gruppo di lavoro che sollecita pratiche di sicurezza standardizzate nel settore: il *Cloud Security Alliance* (CSA). È un'organizzazione senza fini di lucro composta da importanti esperti in materia che ha lo scopo di promuovere, tra gli utenti e i fornitori, l'uso di *best practice* per fornire garanzie di sicurezza nel *Cloud Computing*, e offrire formazione specifica con le relative certificazioni. Il CSA e altre organizzazioni analoghe hanno individuato la necessità di ridurre i rischi di sicurezza associati al *Cloud Computing* ma le norme sono ancora da emanare ufficialmente. In assenza di norme di sicurezza obbligatorie nel settore, i fornitori di servizi sono liberi di implementare protocolli che possono non aderire alle esigenze delle singole imprese. I singoli *Provider* hanno comunque sviluppato procedure per la protezione dei dati contro i rischi alla sicurezza. I clienti del *Cloud* devono informarsi sulle politiche e le procedure di sicurezza dei fornitori di servizio e attivarsi per negoziare e inserire nei contratti eventuali ulteriori misure di sicurezza ritenute necessarie, magari evidenziate da specifiche analisi dei rischi.

Per identificare le principali minacce alla sicurezza del *Cloud Computing*, il CSA ha condotto un sondaggio tra gli esperti del settore per analizzare le vulnerabilità specifiche di quest'ambito. La metodologia d'indagine usata ha condotto alla redazione di una lista che riflette le principali preoccupazioni del settore. In una più recente edizione di questo rapporto, gli esperti hanno individuato le seguenti minacce alla sicurezza del *Cloud* (classificate in ordine di gravità):

1. **Violazioni dei dati** - Dati sensibili delle aziende possono cadere nelle mani dei loro concorrenti. Un pirata informatico potrebbe aver accesso a un database del servizio di *Cloud* non correttamente configurato. Una falla nella sicurezza del *Cloud* potrebbe consentire ad un utente malintenzionato di accedere non solo ai dati del singolo cliente, ma a quelli di tutti i clienti. Utilizzare la crittografia per la protezione dei dati è una possibile soluzione.

2. **Perdita dei dati** - La prospettiva di perdere i propri dati è inaccettabile sia per i consumatori, sia per le imprese, in quanto potrebbe provocare danni sia economici, sia di immagine. Qualunque cancellazione accidentale causata dal fornitore di servizi di *Cloud*, o peggio, una catastrofe fisica come un incendio o un terremoto, potrebbe portare alla perdita permanente dei dati dei clienti a meno che il *Provider* prenda adeguate misure per il *backup* dei dati. Inoltre, l'onere di garantire la possibilità di recuperare i dati potrebbe non ricadere solo sulle spalle del *Provider*: se un cliente cifra i suoi dati prima di caricarli sul *Cloud* e perde la chiave crittografica, i dati saranno comunque persi.

3. **Compromissione *account*** – In caso di "account *hijacking*" un servizio viene utilizzato in maniera fraudolenta da un attaccante che impersona l'utente legittimo. Molto comuni sono metodi di attacco come il *phishing* e lo sfruttamento di *software* malevolo per ottenere informazioni. Le credenziali e le *password* sono spesso riutilizzate per accedere in maniera fraudolenta a informazioni personali. Le soluzioni *Cloud* aggiungono una nuova minaccia: se un *hacker* carpisce le credenziali, può intercettare le attività e le transazioni dell'utente, manipolare i dati, restituire informazioni falsificate o reindirizzare la clientela verso siti illegittimi.

4. **Interfacce e API non sicure** - I gestori di *Cloud Computing* forniscono una serie d'interfacce *software* o API (*Application Programming Interface*) che i clienti utilizzano per gestire e interagire con i servizi. La sicurezza e la disponibilità dei servizi generali di *Cloud* dipendono dalla sicurezza di queste API di base, utilizzate ad esempio per l'autenticazione ed il controllo di accesso, per la crittografia e il monitoraggio delle attività. Queste interfacce devono essere progettate per resistere a tentativi di accesso non autorizzato sia accidentali, sia fraudolenti. Inoltre, i fornitori e i gestori di terze parti spesso ampliano tali interfacce per offrire servizi a valore aggiunto ai propri clienti. Questo aumenta la complessità delle API ma anche i rischi in termini di sicurezza.

5. **Negazione del servizio** - Gli attacchi "*denial-of-service*" sono rivolti a impedire agli utenti di un servizio *Cloud* di accedere ai propri dati o applicazioni forzando il servizio a utilizzare una quantità eccessiva di risorse di sistema come la potenza del processore, la memoria, lo spazio su disco o la larghezza di banda della rete, causando un rallentamento del sistema.

6. **Addetti ai lavori malintenzionati** - Il rischio di impiegati disonesti (*"insider*") è un argomento molto discusso nel settore della sicurezza. Una minaccia dall'interno per un'organizzazione può essere un dipendente o ex dipendente, un amministratore di sistema o altro partner che ha o aveva l'autorizzazione per l'accesso alla rete. Un *insider* all'interno di una struttura *Cloud* impropriamente progettata potrebbe avere accesso a informazioni potenzialmente sensibili.

7. **Abuso di servizi *Cloud*** - Uno dei maggiori vantaggi del *Cloud Computing* consiste nel fatto che permette anche a piccole organizzazioni di accedere a grandi quantità di potenza di calcolo e spazio di memoria. Mentre risulta impensabile per la maggior parte delle organizzazioni acquistare e mantenere migliaia di server, la possibilità di affittare tali server da un fornitore di *Cloud Computing* risulta molto più conveniente.

L'avere a disposizione questo potere può però portare ad usi non sempre corretti. Si potrebbe ad esempio pensare ad un *hacker* che, con i propri limitati mezzi *hardware*, impiegherebbe anni per scoprire una chiave crittografica, mentre utilizzando un *array* di server *Cloud* potrebbe essere in grado di farlo in pochi minuti. Oppure potrebbe utilizzare quello stesso *array* di server *cloud* per organizzare un attacco informatico o per distribuire *malware* o *software* pirata.

8. **Insufficiente scrupolosità** – I principali vantaggi del *Cloud Computing* sono rappresentati dalla riduzione dei costi e dall'incremento di efficienza operativa. Mentre questi possono essere considerati obiettivi realistici per le organizzazioni che hanno le risorse per adottare tecnologie *Cloud* correttamente, troppe aziende si spacciano per *Provider* di servizi *Cloud* senza capire la piena portata dell'impegno. Senza una comprensione completa dell'ambiente, delle applicazioni o dei servizi proposti dal *Cloud* e le responsabilità operative nella risposta agli incidenti, nell'uso della crittografia, e nel monitoraggio della sicurezza, i *Provider* si assumono livelli elevatissimi di rischio.

9. **Questioni tecnologiche** - I fornitori di servizi *Cloud* offrono i loro servizi in modo scalabile condividendo infrastrutture, piattaforme e applicazioni. Una singola vulnerabilità nei vari servizi o un errore di configurazione può portare a compromettere un intero *Provider Cloud*.

I rischi connessi all'utilizzo di questa tecnologia, sicuramente da tenere presenti, affrontare e risolvere, non devono far passare in secondo piano gli innumerevoli vantaggi legati al suo utilizzo, in termini di risparmio di tempo e di denaro, di maggiore flessibilità, efficienza ed efficacia, oltre che di condivisione e collaborazione.

È evidente, quindi, che una maggiore diffusione del *Cloud* porta a doversi sempre più confrontare con le minacce ed i rischi sopra descritti, soprattutto per quanto riguarda i grandi *repository* di informazioni.

Molta attenzione è richiesta ai semplici utilizzatori di *smartphone* e *tablet* con riferimento a ciò che viene conservato nel *Cloud* (immagini, foto, documenti, anche afferenti alla propria sfera riservata).

Ad esempio è di qualche tempo fa la notizia secondo la quale alcuni *hacker* sarebbero riusciti ad entrare in *iCloud* sfruttando la funzionalità "Trova il mio *iPhone*". La vulnerabilità di questa specifica funzionalità consisteva nel non prevedere protocolli di sicurezza per proteggersi da attacchi "*brute force*", implementati invece nel restante ambito dell'*account*. Moltissime immagini private di star di Hollywood hanno iniziato a diffondersi in rete facendo entrare nel panico l'intero *show business* americano. Tutto quello che i malintenzionati dovevano fare era trovare l'indirizzo email collegato all'account di quei VIP e poi far partire l'attacco. In sostanza, gli *hacker* hanno utilizzato un semplice programma (*script*) in grado di inserire migliaia di *password*, ripetutamente e velocemente, per provare a trovare quella giusta. Solo in seguito a tale attacco il sistema fu opportunamente modificato per risultare più robusto a questo genere di attacco.

3. PROTEGGERE I PROPRI DATI

Cosa fare, dunque, per proteggere i propri dati e quelli della propria azienda dalle minacce in agguato nel *Cloud*? Molti degli aspetti di sicurezza sono legati alla specifica realizzazione dell'infrastruttura della rete *Cloud* quindi non esistono delle regole che valgano per tutte le implementazioni esistenti.

Si riportano dii seguito alcuni suggerimenti utili per ridurre i rischi associati all'utilizzo del *Cloud* e poterne sfruttare gli intrinseci vantaggi.

1. **Utilizzare l'autenticazione a due fattori** - Molti fornitori di *Cloud Computing* offrono un sistema di accesso in "due fasi", aggiungendo un livello di protezione e richiedendo l'inserimento di un codice di autenticazione in aggiunta alla normale *password* (di solito inviato direttamente tramite SMS). Questo impedisce a ospiti indesiderati di accedere al proprio account da un dispositivo sconosciuto.

2. **Scegliere solo *password* complesse ed univoche** - Avere una *password* sicura ed univoca è uno dei modi più semplici per contrastare le minacce online.

3. **Utilizzare *password* diverse per diversi *account*** - Assicurarsi che tutti i membri dell'azienda utilizzino *password* diverse per i diversi tipi di *account*, in particolare quelli che utilizzano informazioni sensibili, come estratti conto bancari o informazioni sulle carte di credito. Avere una *password* diversa per ogni account impedirà agli sconosciuti di accedere a tutti gli *account* se anche solo una *password* è compromessa.

4. **Modificare regolarmente la *password*** - Alcuni attacchi alla sicurezza di un *account* richiedono molto tempo e non è possibile sapere in che momento stanno accadendo. Gli *hacker* possono rintracciare una *password*, ma non curiosare nell'*account* compromesso anche per mesi. Per queste ragioni, è consigliabile rimanere al passo e cambiare regolarmente le *password*.

5. **Non collegare gli *account*** – Evitare di collegare gli *account* tutti insieme (problema noto anche come *daisy-chaining*), ad esempio usando la stessa *password* per diversi siti o collegando lo stesso indirizzo *email* a metodi di pagamento per diversi servizi online, esponendosi così al rischio di perdere i dati e compromettere la sicurezza di tutti gli *account* in una volta sola.

6. **Condividere le informazioni in modo intelligente** - Anche se ci si fida della sicurezza del proprio *account*, non è possibile essere certi che questo valga anche per le altre persone. Nel caso che qualcuno riesca ad accedere al proprio *account* evitare di condividere le informazioni delle carte di credito, dei dati sensibili o di altre informazioni private tramite *email* o via *chat*.

7. **Diffidare di tutte le truffe e di tutte le potenziali minacce di *hacking*** - Tutti gli utenti devono essere al corrente che applicazioni, collegamenti, *email* e siti *web* possono essere falsificati al fine di rubare informazioni personali. Particolare attenzione

dovrebbe essere fatta alla formazione relativa alla conoscenza delle tecniche di *phishing*, a proposito delle quali alcune cose importanti da ricordare sono:

- se si riceve una *mail* da un indirizzo sospetto, chiamare l'azienda per verificare che la comunicazione sia legittima;
- non aprire o rispondere a messaggi di posta elettronica provenienti da fonti sconosciute (tenendo anche in considerazione che è estremamente semplice falsificare il nome del mittente in una *email*);
- **mai cliccare su un *link* o un allegato contenuto in una *email* sconosciuta** o della quale non si abbia assoluta certezza della legittimità della provenienza.

8. **Installare e aggiornare il *software* antivirus** - Utilizzare un buon *software antivirus* per bloccare e rimuovere le minacce informatiche (*virus*, *spyware*, *malware*, *spam* e *adware*) che possono minare la sicurezza del proprio computer.

9. **Verificare l'uso di tecnologia sicura e crittografia** - Assicurarsi che le credenziali di accesso dei tuoi servizi *online* siano abbastanza robuste e assicurarsi che gli utenti navighino in modo sicuro. Ecco una lista utile per il controllo sulla sicurezza della navigazione dei siti e dei fornitori di servizi:

    - i servizi *Cloud* devono crittografare i dati sia quando vengono archiviati, sia in *upload* che in *download*;
    - eseguire l'analisi dei *log*, controlli dell'integrità dei file, il monitoraggio delle politiche, utilizzando applicazioni in grado di fornire questi strumenti;
    - controllare che il servizio *Cloud* offra sempre connessioni sicure per la trasmissione dei dati via Internet, verificando la presenza del protocollo *https* prima dell'indirizzo del sito (URL) e di un piccolo lucchetto nella barra degli indirizzi o nella parte più bassa della finestra del *browser*;
    - assicurarsi che il proprio *browser* ed il *Provider* utilizzino i protocolli di sicurezza più aggiornati (per esempio è ormai fortemente sconsigliato l'utilizzo di protocolli SSL – i principali *browser* non ne supportano più l'uso –, ma dovrebbero essere utilizzati i protocolli TLS, possibilmente TLS 1.2).

10. **Eseguire il *backup*** - Il *backup* è una procedura sicura, utile nel caso in cui siano compromessi i dati aziendali. Gli esperti di protezione dei dati raccomandano di eseguire il *backup* per quelle aziende che gestiscono i propri dati online. Il *backup* è una procedura periodica che crea una copia di tutte le informazioni, così i dati non vengono persi nel caso in cui dovesse succedere qualcosa alla versione originale. Una soluzione di *backup* e di ripristino completo può proteggere anche dall'errore umano che è, di fatto, una delle principali cause di perdita dei dati. Senza *backup* e ripristino, se un utente elimina accidentalmente una *email* importante o un file, questi sono cancellati definitivamente. Con l'aiuto del software di *backup*, non si perdono informazioni e si riescono a ripristinare rapidamente tutti i dati cancellati o compromessi.