PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3710 di mercoledì 03 febbraio 2016

Entrare nel cloud: 11 rischi ed 11 opportunità

Una guida illustra i rischi e le opportunità legati all'utilizzo del cloud e i quesiti che l'azienda deve porre per scegliere il fornitore. Di Adalberto Biasiotti.

Troppo spesso si mettono in evidenza i problemi che crea un'Europa unita, soprattutto per una burocrazia talvolta pesante, mentre non sempre si dà adeguato peso alle meritevoli iniziative, che la Europa unita mette a punto.
Tra le recenti iniziative, che desidero portare all'attenzione dei lettori, vi è la pubblicazione di un documento di una cinquantina di pagine che illustra i rischi e opportunità che sono legati all'utilizzo del cloud.
È ben noto che ormai questa tecnologia di archiviazione dei dati sta occupando uno spazio sempre maggiore, perché i vantaggi che presenta sono significativi. Purtroppo, come sempre, chi offre questo servizio tende a sottolinearne i pregi, non dando adeguato spazio ai rischi, che inevitabilmente sono connessi all'utilizzo di nuove tecnologie: questa nuova tecnologia non fa eccezione. Non per nulla, la unione europea ha già elaborato alcuni documenti che tendono a stabilire delle regole uniformi per tutti i fornitori di servizi nel cloud, in modo da garantire agli utenti una serie di garanzie di base.
Ad esempio, vengono già messi a disposizione dei contratti tipo, che rappresentano un equo compromesso fra diritti e doveri delle parti coinvolte.

Cominciamo a presentare la agenzia dell'unione europea che ha messo al punto questo documento.
Stiamo parlando della European Union Agency for Network and Information Security (ENISA), il cui compito è proprio quello di sviluppare consigli e raccomandazioni afferenti soprattutto alla sicurezza delle informazioni digitali.
Essa funge anche da consulente per la commissione europea e per il Parlamento, nel mettere a punto provvedimenti legislativi in merito.

Una breve illustrazione della guida
La guida, che i lettori troveranno integralmente riportata in allegato, seppure solo in lingua inglese, intende aiutare le piccole e medie imprese, che spesso non hanno una competenza informatica elevata, circa i rischi e le opportunità legati all'utilizzo di servizi nel cloud.
In particolare, con un approccio molto analitico e pragmatico, il documento elenca **11 rischi ed 11 opportunità**, e mette a disposizione un certo numero di quesiti che l'azienda, che vorrebbe migrare nel cloud, dovrebbe porre al suo fornitore.
Cominciamo ad esaminare, per partire con il bicchiere mezzo pieno, le 11 opportunità, legate alla sicurezza della rete delle informazioni che su di essa viaggiano.

01: la distribuzione geografica e l'accessibilità delle informazioni
02: la elasticità è flessibilità del servizio
03: l'utilizzo di interfacce e formati standardizzati
04: La sicurezza fisica dei dati, che non sono fisicamente accessibile, perché non sono residenti presso l'azienda
05: la disponibilità di servizi di pronto intervento, in caso di emergenza, nell'arco delle ventiquattrore
06: efficienti ed efficaci le risorse destinate a sviluppare migliorare il software di gestione
07: tempestivi interventi di correzione di possibili anomalie del software
08: un efficiente servizio di backup
09: un'archiviazione dei dati adeguatamente protetta

010: la fornitura di servizi di sicurezza complementare ed integrativi
011: garanzia di certificazione e conformità dei servizi resi

Subito dopo, come è evidente, andiamo ad esaminare il bicchiere mezzo vuoto, vale a dire quali sono i rischi afferenti alla sicurezza dei dati custoditi nella nuvola.

R1: vulnerabilità della sicurezza del software
R2: attacchi mirati alla rete
R3: attacchi di Social engineering
R4: modalità di gestione delle informazioni da parte del fornitore del servizio
R5: il furto o perdita di apparati collegabili al cloud
R6: rischi fisici afferenti alle obbligazioni dove i dati sono custoditi
R7: sovraccarico di traffico di archiviazione di dati
R8: costi supplementari non programmabili in precedenza
R9: legame a doppio filo con il fornitore del servizio
R10: lacune amministrative o problemi legali
R11: problemi legati a giurisdizioni applicabili in campo internazionale

Seguono infine i quesiti che sarebbe opportuno che un potenziale acquirente di questi servizi ponesse al proprio fornitore.
A questo proposito, segnalo che tra le meritorie iniziative di ENISA vi è anche la messa a punto di schemi di certificazione, che indubbiamente sollevano l'acquirente dall'impegno e dalla responsabilità di effettuare una selezione critica dei fornitori. Quando un fornitore gode di una certificazione per la resa di questo servizio, con ogni probabilità è un fornitore di buon livello e la negoziazione può concentrarsi sul prezzo.

Enisa - Cloud Security Guide for SMEs

Adalberto Biasiotti
