Accordo AIIC e CSA Italy per la sicurezza dei sistemi cloud computing nelle infrastrutture critiche

Accordo strategico ad alta componente tecnico-scientifica per la sicurezza dei sistemi informatici cloud computing che sovrintendono le infrastrutture critiche, ossia quelle che assicurano la regolare vita di un Paese nei settori energetici, sanitari, trasporti, comunicazioni, finanziari, ricerca ed e-Government. A siglare la convenzione sono stati Sandro Bologna, presidente dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC), e Alberto Manfredi, presidente del capitolo italiano della Cloud Security Alliance (CSA), l'organizzazione internazionale per la promozione della sicurezza nell'uso del cloud computing.

L'alleanza consentirà ai due partner di valorizzare al massimo le proprie competenze professionali attraverso una stretta sinergia per progetti, ricerche, iniziative divulgative e azioni anche nel campo della formazione, allo scopo di elevare e tenere aggiornati i livelli di sicurezza dei sistemi cloud computing nell'interesse del Sistema Paese, evitando che frangenti critici come incidenti, attentati e disastri possano compromettere la qualità della vita dei cittadini e il funzionamento degli impianti strategici.

In particolare, la partnership tra AIIC e CSA Italy si pone come obiettivo proprio quello di far convergere le competenze degli esperti delle infrastrutture critiche e di cloud security per promuovere lo scambio di esperienze e conoscenze tra i due settori, favorendo lo studio dei problemi derivanti dall'applicazione del cloud alle infrastrutture critiche".

La tecnologia cloud è ormai una realtà non solo nel mercato dei servizi consumer e si sta prepotentemente affermando nel settore business. Prodotti nati con un'ottica consumer (come Gmail o Dropbox) sono entrati a far parte degli asset ICT aziendali. La maturazione delle tecnologie e la convergenza con il mercato mobile rendono possibile l'uso del cloud anche per applicazioni critiche (health care, controllo di processi, smart cities, finance, banking, etc).

Tra i principali problemi di sicurezza del cloud computing ci sono la violazione di identità digitale; la perdita e furto dei dati; la privacy e la sicurezza dei dati quando sono gestiti in legislazioni diverse da quella del possessore dei dati; la mancanza di controllo su hardware e software da parte del fruitore del servizio; l'interoperabilità e la portabilità dei servizi tra cloud pubbliche e private.

Le opportunità del cloud computing sono tante, fanno gola, ma a quale prezzo?

Sandro Bologna (AIIC) - «Nel 2000 la neonata Comunità Europea abbatteva i confini tra gli Stati danno origine a una libera circolazione di persone, beni e servizi. Oggi il cloud computing abbatte i confini degli asset ICT aziendali dando luogo ad una potenzialmente pericolosa circolazione di dati. Se si pensa alla convergenza tra cloud e mobile, l'abbattimento dei confini ha una dimensione worldwide e potremmo ri-battezzarlo "The flat world of ICT assets". Tale nuovo panorama richiede di ripensare i modelli di sicurezza adottati che dovranno essere data-centrici. Anche la "security by design" diventa un modello imprescindibile».

Alberto Manfredi (CSA) - «Il cloud computing rende accessibili risorse e applicazioni che, dal punto di vista della scalabilità (ad esempio potenza di calcolo, spazio disco) e della complessità (CRM, Database, piattaforme di sviluppo applicativo), erano inaccessibili alla maggior parte delle aziende "consumer", in particolare PMI. La prima sfida del mercato dell'offerta, quella del prezzo di accesso, è stata vinta. Oggi la disponibilità di questa nuova tipologia di servizi/risorse pay-per-use porta il consumer a valutare la possibilità di trasferire dati importanti/sensibili sulla nuvola. Sulla base di questa nuova esigenza, CSA promuove l'adozione da parte dei provider cloud della "trasparenza" e responsabilità nella descrizione e conduzione dei servizi cloud, in particolare sugli aspetti di sicurezza e privacy per una scelta consapevole dei servizi».

Recentemente ci sono stati incidenti con ingenti danni economici a big company e con riflessi non trascurabili sugli utenti. Qual è il livello di sicurezza che i servizi cloud riescono a fornire e il livello di maturità delle soluzioni public cloud rispetto alla privacy, alla gestione delle identità digitali? Le tecnologie e le politiche di sicurezza sono mature per un'effettiva convergenza tra infrastrutture critiche e servizi cloud?

Sandro Bologna - «In questo panorama affascinante, ricco di opportunità ma pieno di insidie e incertezze, è importante stimolare e supportare la ricerca nell'ambito della sicurezza dei sistemi cloud affinché i settori critici possano trarne tutti i maggiori benefici. La partnership tra AIIC e CSA Italy si pone come obiettivo proprio quello di far convergere le competenze degli esperti di infrastrutture critiche e di cloud security per promuovere lo scambio di esperienze e conoscenze tra i due settori favorendo lo studio dei problemi derivanti dall'applicazione del cloud alle infrastrutture critiche, e per contribuire alla creazione di un cloud più sicuro e compatibile con le più stringenti linee guida di sicurezza per i sistemi critici».

Alberto Manfredi - «Le attività di ricerca di CSA hanno come obiettivo principale quello di fornire delle guide all'utilizzo ed alla progettazione sicura di infrastrutture e servizi cloud computing. Nelle gulde si fa riferimento a metodologie e standard maturi nell'information security (ad es. ISO 27001, BS25999), ma si forniscono raccomandazioni e approfondimenti sugli obiettivi di controllo e misure di sicurezza specifiche delle infrastrutture cloud (virtualization, federation, data security lifecycle, ecc.). Molto importante è la recente iniziativa dell'Open Certification Framework per Cloud Provider di CSA, basata sul precedente programma STAR (Security Trust and Assurance) che propone una metodologia di valutazione e obiettivi di controllo specifici per Cloud Provider. Le opportunità per le nostre associazioni di dare risposte concrete al tema della sicurezza delle infrastrutture critiche non mancano di certo». ■