

COVERSTORY

L'IT CLOUD COM

6

Alla prima edizione di SecureCloud si sono confrontati operatori, esperti ed esponenti di organismi internazionali sulle problematiche legate alla sicurezza

Al SecureCloud 2010 di Barcellona le principali organizzazioni che operano a livello europeo nel settore della sicurezza si sono date appuntamento per discutere degli aspetti della sicurezza legati al cloud computing. ENISA, Cloud Security Alliance, ISACA e IEEE hanno di fatto offerto la prima importante opportunità di confronto su questo tema a livello internazionale. Non sono mancati poi i principali fornitori di servizi cloud: Amazon, Microsoft e Google. Il messaggio emerso alla due giorni spagnola è chiaro: il cloud computing rappresenta un cambio sostanziale di paradigma nel quadro della fornitura dei servizi IT.

Una delle tavole rotonde più interessanti delle due giornate è stata quella che ha coinvolto i rappresentanti dei governi coreano, spagnolo e giapponese, oltre a un rappresentante statunitense del NIST (National Institute of Standards and Technology). Tutti hanno condiviso le stesse ambizioni di riduzione dei costi, di raggiungimento dei benefici di scala, così come le

DI DANIELE VITALI*



sulla strada del PUTING⁷



© o'ly - Fotolia.com

www.it

COVERSTORY

stesse preoccupazioni legate alla protezione dei dati, ai problemi di giurisdizione internazionale, alle differenze tra le diverse normative e approcci alla gestione della privacy.

Ma l'elemento veramente interessante dell'intera manifestazione è stata la conclusione alla quale sono giunti tutti i partecipanti: sin da subito è necessario affiancare al tema del cloud computing quello della sicurezza.

La conferenza ha di fatto rappresentato l'intenzione di mettere a fattor comune gli sforzi delle community internazionali al fine di portare velocemente a un livello di maturità adeguato i modelli di gestione dei rischi, che dovrebbero contemplare questo nuovo paradigma di erogazione dei servizi, per renderli applicabili dalle aziende di ogni dimensione e consentire la valutazione dei servizi cloud.

8

QUELL'ALONE DI MISTERO

Udo Helmbrecht, da poco eletto executive director di ENISA, nel suo intervento ha illustrato i risultati dell'analisi effettuata dall'agenzia europea su benefici, rischi e raccomandazioni per la sicurezza delle informazioni su cloud (liberamente scaricabile dal sito dell'ENISA). L'analisi è stata coordinata da Daniele Catteddu e Giles Hogben di ENISA.

In particolare, Helmbrecht ha evidenziato diversi benefici di sicurezza legati soprattutto alla possibilità di applicare economia di scala

PROBLEMA 1: RISCHI DI COMPLIANCE E CRITICITÀ NORMATIVE

Come si possono superare i rischi di compliance e le criticità normative?

Risponde Feliciano Intini, chief security advisor di Microsoft Italia



Bisogna operare su due fronti. In primo luogo, stimolare l'azione dei legislatori nello sforzo di sviluppare una normativa consistente a livello internazionale che riconosca i requisiti degli scambi di dati transnazionali con forti garanzie su protezione dati e privacy. In seconda battuta, supportare tali sforzi fornendo la competenza necessaria per comprendere le architetture multi-geografiche e le dinamiche operative di trasferimento dei dati tipiche del cloud computing.

alle soluzioni tecniche e ha messo in evidenza alcuni rischi peculiari del cloud, quali per esempio rischi di compliance, di proprietà intellettuale, lock-in del fornitore e molti altri legati alle informazioni in transito e residenti su cloud.

Ha inoltre evidenziato un punto cruciale: l'alone di mistero che i fornitori di servizi di cloud computing pubblici stanno tenendo sulle loro pratiche di gestione dei sistemi non permette di avere tutti gli elementi per compiere un'analisi del rischio completa. È dunque necessaria una maggiore trasparenza da parte dei fornitori di servizi di cloud computing al fine di permettere a ogni azienda di comparare realmente il rischio di un servizio su cloud pubblico con il rischio di un servizio gestito in autonomia.

L'APPLICAZIONE DELLA LEGGE

Alexander Seger, responsabile dell'Economic Crime Division del Consiglio Europeo, ha evidenziato invece come sussistono problemi significativi anche dal punto di vista di chi deve fare applicare la legge. In particolare, può succedere con facilità che non sia chiara la giurisdizione



PROBLEMA 2: SCARSA CONOSCENZA DEI SISTEMI DEI FORNITORI

Quali sono le informazioni sulla gestione dei sistemi che i fornitori di servizi cloud computing dovrebbero rendere pubbliche, e verificabili, per consentire un'analisi del rischio completa su un servizio di questo tipo?



Risponde Daniele Vitali, senior consultant di Spike Reply

Purtroppo, analisi 'generiche' condotte con modelli non appropriati tendono a far emergere rischi altrettanto 'generici' e non contestualizzati. Una azienda ha quindi bisogno di applicare una metodologia di analisi specifica per il cloud computing, che permetta di ottenere informazioni di dettaglio su come il fornitore di servizi affronta e gestisce tutti i temi legati alla sicurezza.

sui dati o che non sia chiaro quale sia la responsabilità relativamente all'adempimento di obblighi di legge; come per esempio la necessità di intercettare una comunicazione. In questa direzione va sicuramente la 'Convention on Cybercrime' ormai ratificata da molti Paesi europei, Italia compresa, che sta trovando difficoltà nella messa in pratica da parte dei governi. Sager raccomanda una maggiore standardizzazione delle normative privacy, auspicando addirittura uno standard unico per la privacy con regole chiare e condivise.

RISCHIO CONTRATTI STANDARD

Una sessione specifica è stata invece dedicata ai temi di carattere legale, quali la giurisdizione e le leggi applicabili al contesto, le normative di data protection, l'accesso ai dati da parte delle forze dell'ordine, la proprietà intellettuale e l'allocazione delle responsabilità per il trattamento dei dati.

Un tema articolato e complesso, ma che può essere cruciale, così sintetizzato: la standardizzazione dei servizi porta inevitabilmente alla standardizzazione delle clausole contrattuali e la negoziazione di un contratto di-

PROBLEMA 3: LA STANDARDIZZAZIONE DEI CONTRATTI

Come si supera il rischio della standardizzazione dei contratti?

Risponde Gabriele Provinciali, senior solutions architect di CA



La standardizzazione tecnologica non è necessariamente correlata a una standardizzazione contrattuale: in particolare, tutte le tecnologie di compatibilità nelle diverse tipologie di cloud rendono più facile la combinazione di servizi compositi, formati da elementi eterogenei come ambienti virtualizzati, storage... Il rischio di rigidità può essere minimizzato potenziando l'accesso all'offerta attraverso sistemi personalizzati e di composizione dinamica del servizio.

venta importantissima per definire le responsabilità delle parti. Purtroppo, la realtà vuole che siano poche le realtà abbastanza forti e in grado di negoziare i termini non standard con i grandi provider internazionali di servizi di cloud computing.

Un contributo particolare è stato portato da Ben Katsumi (IPA), che ha illustrato come in Giappone il governo stesso stia diventando promotore e fornitore di servizi SaaS dedicati alle piccole e medie aziende, proponendo un modello di cooperazione con il mercato dei fornitori di servizi, finalizzato a garantire una maggiore flessibilità al business nazionale.

Per concludere, la conferenza SecureCloud 2010 ha segnato un momento importante per la community internazionale della sicurezza. Le più importanti associazioni, istituzioni, aziende fornitrici di servizi di sicurezza e di cloud computing hanno preso un serio impegno di cooperazione, collaborazione e trasparenza.

L'appuntamento è tra un anno alla seconda edizione di SecureCloud, per vedere quanti di questi impegni saranno rispettati seriamente. ■

**Daniele Vitali è senior consultant di Spike Reply*