LA GESTIONE DEL RISCHIO NEL CLOUD COMPUTING: QUALI APPROCCI E STRUMENTI APPROPRIATI

Alberto Manfredi
Presidente CSA Italy

Francesca Capuano
ICT Security Consultant in Network Integration and Solutions Srl: consulente per IT Governance e Information Security

Matteo Mangini
Project Manager e Solution Architect di Network Integration and Solutions Srl: responsabile del servizio di analisi del rischio denominato RiS (Risk Integrated Service), basato sui principali standard internazionali (ISO27001, ISO2000, ISO22301, CCM...)

Negli ultimi anni abbiamo assistito a profondi cambiamenti del mercato ICT testimoniati dalla crescente adozione di paradigmi e tecnologie innovative quali il Cloud, l'Internet of Things, la stampa 3D, i Big Data Analytics, le infrastrutture *software-defined* fino al nuovo trend del *Web-scale IT*[1]. In questo nuovo e mutevole contesto tecnologico, la pianificazione strategica aziendale non può ormai non tener conto di investire in modelli di business sempre più innovativi e dinamici in grado di far fronte alla crescente competizione e *time to market*.

L'ultimo rapporto Assinform[2] sottolinea come in Italia l'apprezzamento del Cloud stia aumentando e nel 2015 il mercato complessivo è cresciuto del 28,7% rispetto all'anno precedente, in particolare nell' adozione di servizi SaaS (in crescita su applicazioni "core") e IaaS infrastrutturale.

Anche nella ricerca di Coleman Parkes Research[3] si stima che, nel corso del 2016, il 75% dei servizi IT aziendali saranno su Cloud, sottolineando come l'impatto di tale tecnologia nelle imprese sia di fatto "disruptive".

Il mercato della "nuvola" pare, quindi, non viva crisi di crescita, anzi sembrano lontani i tempi in cui le aziende erano restie ad approcciare questo nuovo paradigma IT.

Se la difficoltà iniziale a dotarsi o meno di un servizio, una piattaforma o un'infrastruttura Cloud[4] sembra superata, manca ancora una visione chiara e strategica di come il "governo" dei dati possa e debba essere definito in termini di responsabilità e confini. La sicurezza risulta essere comunque un "must-have" ormai non derogabile, come testimonia ancora la ricerca Coleman Parkes, in cui il 72% la pone al primo posto tra i fattori di maggiore criticità nell'adozione di servizi in Cloud.

Le criticità di sicurezza introdotte dal Cloud Computing sono ormai note:

- la dislocazione sempre più internazionale dei sistemi di calcolo e memorizzazione rende il luogo di trattamento e conservazione dei dati spesso non identificabile, dando la sensazione di perderne il controllo, in particolare sulla tracciabilità;
- la non omogeneità di leggi e norme tra stati in cui sono presenti i Datacenter dei fornitori Cloud, in particolare extra UE, possono causare problemi di non conformità e/o sanzioni (anche se mitigati dall'entrata in vigore del nuovo regolamento europeo sulla data protection[5]);
- la *multi-tenancy*, per cui è possibile creare più ambienti virtuali logicamente distinti presenti sullo stesso componente fisico consentendo di fatto a più clienti (*tenant*) di lavorare indipendentemente, aumenta il rischio di attacchi che possono compromettere tale separazione e quindi la riservatezza del dato;
- infine, le modalità con cui vengono fruiti i servizi Cloud e l'immaturità e scarsa adozione di strumenti, standard e formati di dati interoperabili rendono spesso difficile un'eventuale migrazione da un provider ad un altro, così come il semplice recupero dei propri dati.

LA SICUREZZA RISULTA ESSERE UN "MUST-HAVE" ORMAI NON DEROGABILE, MA MANCA ANCORA UNA VISIONE CHIARA E STRATEGICA DI COME IL "GOVERNO" DEI DATI POSSA E DEBBA ESSERE DEFINITO IN TERMINI DI RESPONSABILITÀ E CONFINI

Alberto Manfredi è Presidente di CSA Italy dal 2011. Dottore in Scienze dell'Informazione e Dottore Magistrale in Informatica con pieni voti assoluti e lode, lavora da piu` di 20 anni nel settore ICT e Cyber Security. Attualmente lavora in Finmeccanica Spa come Business Development Manager nel Settore Elettronica e Sistemi di Difesa e Sicurezza. Detiene le certificazioni professionali CISA, CRISC, CISSP, GCFA, CCSK, Lead Auditor 27001, Certified CSA STAR Auditor. Cofondatore e Managing Director dell'associazione Club R2GS Europe nata per favorire lo scambio di esperienze e conoscenza nel campo Security Information and Event Management e Security Operation Centres.

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

CLOUD E CYBER RESILIENCE

E' di fatto ormai noto che nessun dato è totalmente al sicuro, sia su sistemi tradizionali sia in Cloud[6].

Per questi e altri motivi, differenti a seconda della modalità di servizio Cloud prescelto, avere una adeguata conoscenza delle criticità di un servizio Cloud sulle quali porre maggiore attenzione permetterebbe alle imprese di poter effettuare scelte migliori per il business e adottare nello stesso tempo le contromisure più efficaci per ridurre i rischi.

Cosa fare allora se l'adozione delle nuove tecnologie, seppur le più avanzate ed efficaci come il Cloud, non assicura automaticamente una riduzione del rischio?

In questa direzione, nel panorama IT si sta affermando il concetto di *resilienza*, vista come l'abilità di un'organizzazione di anticipare, prepararsi, rispondere ed adattarsi attivamente agli eventi, siano essi cambiamenti graduali o improvvisi, in modo tale da assicurare la propria sopravvivenza (definizione dello standard BS 65000[7]).

Il concetto di resilienza nasce dalla convergenza dei concetti di *cyber security* e *business continuity*. Secondo una recente analisi di mercato[8], tra i maggiori rischi per il business aziendale continuano ad esserci quelli legati alla *Business Interruption*. Tale primato è rafforzato dal fatto che molti degli altri *top risk* (tra cui gli attacchi informatici, le catastrofi naturali, gli incendi ed i rischi politici) concorrono ad accrescere l'importanza di dover garantire la continuità del business aziendale.

In ambito Cloud, il fornitore del servizio dovrebbe essere in grado di dimostrare al-

1 https://www.digital4.biz/executive/approfondimenti/gartner-i-10-trend-tecnologici-che-i-manager-devono-conoscere_43672153720.htm
2 http://www.zerounoweb.it/approfondimenti/mercato/rapporto-assinform-2016-rivoluzione-digitale-in-corso-1.html
3 http://www.hp.com/hpinfo/newsroom/press_kits/2013/HPDiscover2013/ResearchAdvisory_Cloud.pdf
4 Saas= Software as a Service, PaaS= Platform as a Service, IaaS= Infrastructure as a Service
5 http://ec.europa.eu/justice/data-protection/reform/index_en.htm
6 "Cyber security e resilienza: come gestire il rischio", di Giuseppe Saccardi, 4 marzo 2016
7 BS 65000:2014 - "Guidance on organizational resilience" - Definition: "Resilience is the ability to anticipate, prepare for, respond and adapt to events – both sudden shocks and gradual change. That means being adaptable, competitive, agile and robust"
8 Allianz Global Corporate a Specialty - Risk Barometer 2016

NESSUN DATO È TOTALMENTE AL SICURO: DIVENTA FONDAMENTALE L'ABILITÀ DI UN'ORGANIZZAZIONE DI ANTICIPARE, PREPARARSI ED ADATTARSI ATTIVAMENTE AGLI EVENTI IN MODO TALE DA ASSICURARE LA PROPRIA SOPRAVVIVENZA

(fonte: https://resilience.enisa.europa.eu/)

l'azienda cliente di saper affrontare prontamente i potenziali attacchi informatici e soprattutto di avere un adeguato livello di *cyber resilience*, ovvero di saper resistere ad un attacco adattandosi all'evento in maniera dinamica, garantendo autenticità, riservatezza, integrità e disponibilità dei dati. Questa garanzia comporterebbe di conseguenza anche un aumento della capacità di resilienza del cliente fruitore dei servizi Cloud. L'attributo di resilienza, associato ad altri *business attributes*[9], contribuisce alla valorizzazione complessiva della criticità degli asset di una organizzazione.

STRUMENTI DI ANALISI DEL RISCHIO CLOUD

Esistono ormai metodologie consolidate per l'analisi del rischio in ambienti IT tradizionali, ma cosa accade quando l'organizzazione decide di uscire dal perimetro, almeno apparentemente protetto, della propria infrastruttura IT? Sono sufficienti gli strumenti di analisi tradizionali?

9 Per "business attributes" si intendono una serie di parametri il cui impatto determina un potenziale danno sul business dell'organizzazione. Sono i parametri su cui basare una Business Impact Analysis (BIA): ad esempio, un asset risulta critico per il business dell'organizzazione quando la sua compromissione ha un alto impatto reputazionale, finanziario, legale o operativo sull'azienda.

QUANDO L'ORGANIZZAZIONE DECIDE DI USCIRE DAL PERIMETRO, APPARENTEMENTE PROTETTO, DELLA PROPRIA INFRASTRUTTURA IT SERVONO STRUMENTI PER VALUTARE I RISCHI IN GRADO DI CONTESTUALIZZARE E SPECIALIZZARE L'ANALISI RISPETTO AL NUOVO PARADIGMA CLOUD

A tal proposito, gli strumenti offerti dal mercato sono molteplici, ma che cosa può fare esattamente la differenza quando si affrontano contesti Cloud o Ibridi?
Includendo l'utilizzo dell'attributo di cyber resilience come parametro aggiuntivo su cui basare la propria analisi dei rischi in Cloud, lo strumento ideale dovrebbe prevedere le seguenti macro funzionalità:

- *Classificare gli asset, le minacce e le vulnerabilità specifiche del mondo Cloud:* la decisione di migrare i propri dati in ambiente Cloud amplia di fatto il perimetro aziendale tradizionale e di conseguenza gli asset, le minacce e le vulnerabilità da considerare.
- *Garantire la consistenza dei risultati*: lo strumento dovrebbe essere in grado di ripetere ad intervalli regolari, o su richiesta, la valutazione del rischio al fine di ottenere risultati misurabili, confrontabili, e ripetibili nel tempo.
- *Gestire la conformità alle best practices e norme di riferimento:* nonostante l'applicabilità della norma ISO27001 ad aziende di qualunque tipo, non dovrebbe essere considerata come l'unico riferimento normativo nei contesti Cloud. Nell'analisi del rischio devono essere considerati anche i controlli di sicurezza specifici del nuovo paradigma (ad es. la CCM[10] di CSA, le ISO27017 [11] e ISO27018[12]).
- *Valutare il grado di resilienza:* tale attributo, espresso dai valori di RPO, RTO e RCO[13], è in grado di determinare un valore di criticità più oggettivo, correlando la capacità di un'azienda di mantenere l'operatività e la sicurezza dei dati in caso di guasto/danno.

In generale, la principale caratteristica che può rendere uno strumento di analisi del rischio realmente efficace è sicuramente la sua capacità di contestualizzare e specializzare l'analisi; l'introduzione del concetto di resilienza, inoltre, lo renderebbe particolarmente adatto anche per l'analisi del rischio di Infrastrutture Critiche[14].

10 Cloud Control Matrix di CSA - Fornisce i fondamenti di sicurezza per guidare i cloud provider ed assistere i cloud consumer analizzando i rischi di sicurezza di un cloud provider
11 ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services; fornisce linee guida per l'implementazione di controlli di sicurezza delle informazioni relativi ai servizi cloud
12 ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; set di regole basato sugli standard ISO27001 e ISO27002 con riferimento alle normative privacy dettate dalla Direttiva 95/46 della Comunità Europea
13 RPO (Recovery Point Objective): rappresenta la quantità massima di dati persi a causa di un disastro che un processo può tollerare; RTO (Recovery Time Objective): rappresenta l'intervallo di tempo entro cui (a partire dal disastro) un processo di business deve essere ripristinato; RCO (Recovery Capacity Objective): identifica i requisiti minimi di risorse necessarie alla singola unità per il ripristino dell'operatività.
14 I concetti di resilienza ed interdipendenza rappresentano due elementi chiave caratterizzanti le infrastrutture critiche: con questo termine si intendono le reti energetiche e informatiche, il sistema sanitario, il mondo finanziario, l'approvvigionamento alimentare e idrico, i trasporti e le comunicazioni, la cui rilevanza ed importanza strategica è data dal fatto che l'intera società dipende dal loro corretto funzionamento.

(fonte: www.cloudsecurityalliance.org)

LA CLOUD CONTROLS MATRIX DI CSA

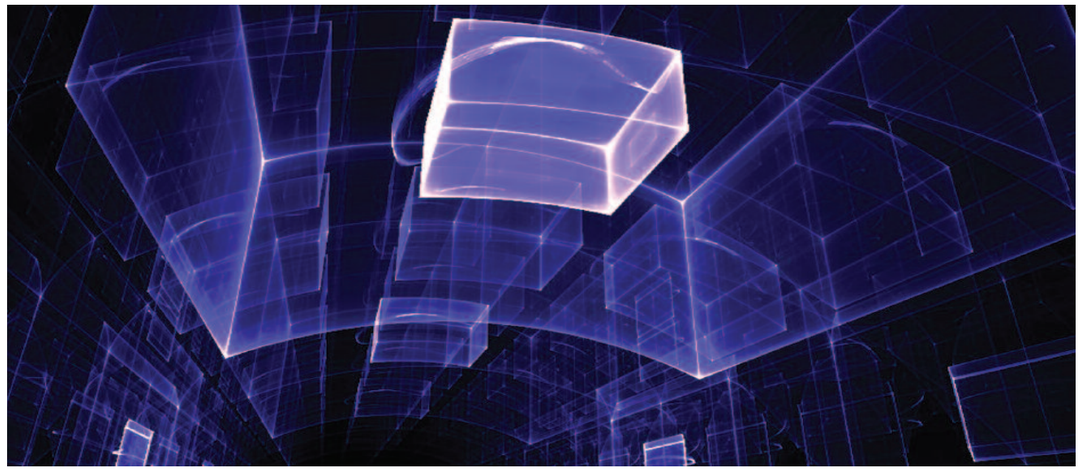
Uno degli strumenti più interessanti ed efficaci per misurare la sicurezza di un Cloud Provider è la *Cloud Control Matrix* (CCM) di CSA[15]. La CCM, sviluppata e periodicamente aggiornata da un gruppo di lavoro costituito da più di 100 esperti internazionali, è di fatto una struttura a matrice (*framework)* di 133 controlli di sicurezza specifici per servizi e infrastrutture cloud computing suddivisi in 16 *Domini*:

1. Application & Interface Security
2. Audit Assurance & Compliance
3. Business Continuity Management & Operational Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Datacenter Security
7. Encryption & Key Management
8. Governance and Risk Management
9. Human Resources
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Supply Chain Management, Transparency and Accountability
16. Threat and Vulnerability Management.

La descrizione dei controlli di sicurezza è riportata nella *Security Guidance for Critical Areas of Focus in Cloud Computing*[16], il manuale sulla sicurezza del Cloud Computing prodotto da CSA, oggi disponibile nella versione 3.0.
Per agevolare l'attività dell'auditor lo strumento consente di contestualizzare rapidamente i controlli necessari (è di fatto un documento *spreadsheet*) secondo le modalità di servizio *IaaS, PaaS,SaaS*. Nella CCM è stata predisposta anche la correlazione rispetto ad altre norme e framework di controlli noti quali le ISO 27001/27002/270017/270018, ISACA COBIT, PCI, NIST, Jericho Forum, NERC CIP che permette di gestire facilmente audit integrati in perimetri multi-compliance.
La CCM è inoltre lo strumento di riferimento per certificare, sia con un ente terzo di certificazione abilitato (ad es. BSI) sia in autovalutazione, la sicurezza dei servizi Cloud secondo la norma CSA STAR, disponibile gratuitamente dal sito internet di CSA[17].

LA CLOUD SECURITY GOVERNANCE TROVA CONSOLIDATI FONDAMENTI E LINEE GUIDE NELLA CCM E NEI SUOI133 CONTROLLI DI SICUREZZA SPECIFICI PER SERVIZI E INFRASTRUTTURE CLOUD COMPUTING

15 https://cloudsecurityalliance.org/group/cloud-controls-matrix/
16 https://cloudsecurityalliance.org/group/security-guidance/



CONCLUSIONI

La Cloud Security Governance è uno dei temi centrali delle attività di ricerca, formazione e divulgazione di CSA Italy. Entro il 2016 con il supporto del partner NIS[18] verrà avviato uno studio che avrà l'obiettivo di valutare la consapevolezza ed esperienza delle aziende italiane nella gestione del rischio nel Cloud e che vedrà come prima azione la predisposizione ed il lancio di un questionario online. I risultati della ricerca verranno successivamente presentati in un workshop dedicato al tema. ■

17 https://cloudsecurityalliance.org/star/
18 www.nispro.it

UN'ADEGUATA CONOSCENZA DELLE CRITICITÀ DI UN SERVIZIO CLOUD CONSENTE DI EFFETTUARE SCELTE MIGLIORI PER IL BUSINESS E ADOTTARE LE CONTROMISURE PIÙ EFFICACI PER RIDURRE I RISCHI: LE AZIENDE POTRANNO MISURARE LA PROPRIA CONSAPEVOLEZZA ED ESPERIENZA SULLA GESTIONE DEL RISCHIO IN CLOUD ATTRAVERSO UN QUESTIONARIO ONLINE REALIZZATO DA CSA E NIS