Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

Spiegazioni sul cloud computing

Introduzione

Sempre più imprese e autorità/istituzioni affidano i propri dati elettronici, finora di solito gestiti internamente, a imprese esterne («outsourcing») secondo un sistema cosiddetto di cloud computing. Questo concetto della tecnologia dell'informazione, traducibile in italiano con «calcolare tra le nuvole», significa in parole semplici **noleggiare** programmi, unità di memoria o capacità di calcolo in rete, per esempio Internet o una rete privata virtuale (virtual private network, VPN), secondo i propri bisogni specifici. L'utente o l'autorità non possiede più il panorama informatico (p.es. centro di calcolo, unità di memoria, programmi collaborativi o di posta elettronica, ambienti di sviluppo o programmi speciali come il customer relationship management, CRM) e nemmeno lo gestisce, bensì lo **noleggia come prestazione** a pagamento da uno o più fornitori di servizi di cloud computing. Le applicazioni (e i dati) non si trovano più nella propria rete ma in un cloud. L'accesso ai dati, ai servizi e all'infrastruttura a disposizione nel cloud avviene mediante accesso remoto (remote access).

I diversi cloud computing si differenziano per la forma di organizzazione e il modello di servizio.

Forme di organizzazione

Si distingue tra **private** cloud**, public** cloud**, hybrid** cloud e **community** cloud.

In un public cloud l'infrastruttura è allestita e gestita totalmente dal fornitore di servizi di cloud computing. L'utente non ha voce in capitolo e, per esempio, non può esercitare alcuna influenza riguardo all'ubicazione dei server. Il private cloud è invece gestito dall'impresa stessa, o tramite un terzo esterno, ed è dunque strutturato in tutto e per tutto in base alle esigenze dell'impresa relativa. Una simile soluzione è molto più sicura, ma anche più costosa. Quando si utilizzano in parallelo public e private cloud, si parla di hybrid cloud. La community cloud, infine, consente a diversi enti di utilizzare in comune la medesima infrastruttura.

Modelli di servizio

Vi sono tre modelli di servizio: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS).

L'**IaaS** riguarda lo stoccaggio dei dati: il fornitore di servizi di cloud computing mette a disposizione nel cloud un server nel quale gli utilizzatori possono memorizzare i loro dati o applicazioni. Responsabile del funzionamento della rete, del suo accesso, dell'hardware ecc. è esclusivamente il fornitore di servizi di cloud computing. Il **PaaS** concerne il trattamento dei dati: il fornitore di servizi di cloud computing sviluppa un'applicazione e la mette a disposizione dell'utente nel cloud. A gestire i dati mediante questa applicazione è tuttavia l'utente stesso. Nel caso dell'**SaaS** l'utente è soltanto un consumatore nel cloud: non gestisce nulla direttamente, né le applicazioni, né i dati. Ha soltanto a disposizione una funzionalità che gli consente di trattare i dati memorizzati nel cloud.

I **vantaggi principali** del cloud computing sono: il contenimento dei costi dell'infrastruttura e dei programmi, gli aggiornamenti del software su richiesta, le maggiori capacità di calcolo, l'unità di memoria dinamica (l'unità di memoria noleggiata nel cloud aumenta o diminuisce a dipendenza della quantità di dati conservati), la mobilità, la disponibilità rapida e semplice, la scalabilità e in alcuni casi una migliore e più elevata sicurezza.

Feldeggweg 1, 3003 Berna
Tel. 031 323 74 84, fax 031 325 99 96
www.edoeb.admin.ch

Rischi del cloud computing

La **delocalizzazione** di dati comporta sempre alcuni rischi. I rischi principali del cloud computing sono i seguenti:

- **perdita di controllo sui dati:** a causa della ramificazione internazionale delle reti e della virtualità, il luogo di conservazione dei dati spesso non è riconoscibile. Questo vale in particolare per i public cloud. L'utente del cloud, che è il titolare dei dati, non sa con esattezza dove, all'interno del cloud, questi siano memorizzati e trattati. Spesso non sa nemmeno se sono coinvolte ditte in subappalto e se queste provvedono a garantire un livello di sicurezza adeguato. L'utente del cloud non è (più) in grado di valutare se adempie gli obblighi legali in materia di protezione dei dati concernenti la sicurezza dei dati, il diritto a essere informati sul loro utilizzo o la rettifica e cancellazione degli stessi;
- **dati non isolati o sufficientemente separati:** rientra nell'idea stessa di cloud computing che diversi utenti senza alcun legame tra loro trattino i rispettivi dati nel medesimo sistema presente nel cloud (le cosiddette architetture Multi-Tenant). Questo aumenta il rischio di essere coinvolto quando uno degli utenti subisce un attacco. Per via di un attacco proveniente da hacker o mossi simultaneamente da numerosi sistemi diversi (Distributed Denial of Services, DDoS) i propri dati potrebbero dunque non essere più disponibili o diventare essi stessi oggetto di pirateria elettronica. È pertanto estremamente importante che i dati dei diversi utenti del cloud siano mantenuti rigorosamente separati e non mischiati;
- **rischi di compliance:** è possibile che nel cloud parti di un record si trovino in centri di calcolo diversi sparpagliati nel mondo. Questo può essere problematico non soltanto per la protezione e la sicurezza dei dati, ma pure per l'adempimento di altri obblighi legali (obbligo di conservare o di provare, obblighi di serbare il segreto ecc.). Imprese e autorità che fanno capo a servizi di cloud computing sono spesso poco consapevoli del fatto che l'obbligo primario di rispettare le disposizioni in materia di protezione dei dati incombe in primo luogo a loro e non al fornitore di servizi di cloud computing che memorizza i dati su un server di cloud o che li tratta nel cloud;
- **accesso ai dati da parte di autorità straniere:** in molti casi per essere trattati nel cloud i dati sono diffusi all'estero. Spesso si memorizzano e si trattano dati anche in Paesi che non dispongono di (sufficienti) norme sulla protezione dei dati. I fornitori di servizi di cloud computing sono però tenuti, se del caso, a consentire ad autorità o tribunali stranieri l'accesso ai dati nel cloud, e anche se i dati non sono trattati o memorizzati nel Paese in cui ha sede l'autorità interessata;
- **effetti di lock in:** un altro rischio è costituito dalla dipendenza dai fornitori di servizi di cloud computing e dalla mancanza di portabilità e interoperabilità. Questo significa che, in mancanza di tecnologie e interfacce standardizzate, i dati non possono (più) - se non a costi ingenti e/o con un grande onere tecnico - essere ripresi nel proprio sistema informatico o migrati presso un altro fornitore di servizi di cloud computing.

Indipendentemente dal fatto che i dati siano trattati in un cloud, occorre sempre mettere in conto in seguenti rischi:

- **perdita dei dati:** a seguito di furti, cancellazioni, sbagli nella sovrascrittura o altre operazioni di modifica è sempre possibile perdere i dati, a meno che non vi siano sistemi per la realizzazione di copie di sicurezza (back up). La perdita di dati comporta rischi legali enormi, addirittura può mettere a repentaglio l'esistenza stessa dell'impresa. Basti pensare al caso in cui vadano persi un determinato know-how tecnico, altri segreti commerciali (per esempio elenchi dei clienti o basi di calcolo) oppure la contabilità finanziaria. Per evitare la perdita di dati dei sistemi di sicurezza relativi vanno implementati; tali dati dovrebbero essere delocalizzati con ritegno. Questi dati devono dunque essere conservati nel cloud soltanto se sono stati predisposti i relativi sistemi di sicurezza per impedire la perdita di dati;
- **guasti al sistema e alla rete e indisponibilità delle risorse e dei servizi noleggiati** possono avere come conseguenza la perdita di dati oppure l'accesso ai dati da parte di persone non

autorizzate: la confidenzialità, la sicurezza e l'integrità dei dati non sono pertanto più garantite. Inoltre questi guasti possono seriamente pregiudicare l'attività di un'impresa o di un'autorità con conseguenze finanziarie e gravi danni d'immagine;

- **uso abusivo dei dati da parte di insider o collaboratori malintenzionati**: Quando si effettua una delocalizzazione il fornitore di servizi non rivela in certe circostanze come sono disciplinati i diritti d'accesso (in modo fisico e virtuale) dei suoi collaboratori e come questi sono sorvegliati. Spesso gli utenti del cloud non possono nemmeno visionare le dichiarazioni di confidenzialità. Nell'ambito del cloud computing occorre prestare particolare attenzione a questo problema se si opera in un public cloud.

Requisiti in materia di diritto di protezione dei dati per l'utilizzazione di servizi di cloud computing

1. Il trattamento di dati personali mediante un sistema di cloud computing equivale, dal punto di vista della protezione dei dati, a un trattamento dei dati da parte di terzi secondo l'articolo 10a LPD. Questo prevede che il trattamento di dati personali può essere affidato a terzi (nella fattispecie i fornitori di servizi di cloud computing) mediante convenzione o per legge **se tale trattamento non è diverso da quello che il mandate stesso (l'utilizzatore di servizi di cloud computing) avrebbe il diritto di fare e se nessun obbligo legale o contrattuale di mantenere il segreto lo vieta. Il mandante deve in particolare assicurarsi che il terzo garantisca la sicurezza dei dati.** Il fornitore di servizi di cloud computing deve essere dunque obbligato a rispettare pienamente le disposizioni in materia di protezione dei dati vigenti in Svizzera. Questo vale anche per eventuali imprese che operano in subappalto. Nella prassi l'adempimento di questa disposizione è tuttavia problematico, dato che in genere nelle applicazioni di cloud computing le condizioni contrattuali del fornitore di servizi di cloud computing previste per l'attribuzione in subappalto non sono note all'utente del cloud.
2. L'utente di servizi di cloud computing deve inoltre accertare che il fornitore di servizi di cloud computing garantisca in quanto terzo la sicurezza dei dati ai sensi dell'articolo 7 LPD e degli articoli 8 e seguenti e 20 e seguenti OLPD. Questo significa che i dati personali devono essere **protetti contro ogni trattamento non autorizzato, mediante provvedimenti tecnici ed organizzativi appropriati**. Occorre garantire **la riservatezza, la disponibilità e l'integrità dei dati**. Il fornitore di servizi di cloud computing deve proteggere i dati contro i rischi di: distruzione accidentale o non autorizzata oppure perdita accidentale; errori tecnici; falsificazione, furto o uso illecito; modificazione, copia, accesso o altro trattamento non autorizzati. Questi provvedimenti devono essere verificati periodicamente sul posto. L'attuazione di dettaglio delle disposizioni relative alla protezione dei dati dipende dall'impresa o dall'autorità, dal tipo di dati, ma anche dall'organizzazione e dal tipo di soluzione di cloud (p.es. private o public; IaaS, PaaS o SaaS). Vale la seguente regola di base: più i dati sono confidenziali, segreti, importanti (poiché rilevanti per l'attività dell'impresa) o sensibili (poiché particolarmente degni di protezione), più è opportuno rinunciare allo stoccaggio dei dati in cloud, soprattutto se ubicati all'estero, e più i provvedimenti e i relativi controlli concernenti la protezione e la sicurezza dei dati devono essere ampi e rigorosi.
3. L'utilizzazione di servizi di cloud computing comporta in molti casi la **diffusione di dati all'estero**, poiché spesso il loro trattamento avviene in server sparsi per il mondo. Molte volte nei sistemi di cloud computing sono implicate pure imprese in subappalto. Spesso nei Paesi nei quali sono localizzati i cloud vigono disposizioni in materia di protezione dei dati più blande di quelle svizzere: vi è pertanto il rischio che i dati siano trattati in un modo che non sarebbe autorizzato in Svizzera. Per queste ragioni i dati personali non possono essere comunicati all'estero qualora la personalità della persona interessata possa subirne grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata (art. 6 cpv. 1 LPD). In tali circostanze è possibile comunicare all'estero dati personali soltanto se sussiste una delle condizioni di cui all'articolo 6 capoverso 2 LPD. In molti casi l'utente di servizi di cloud computing non potrà fare a meno di negoziare garanzie contrattuali sulla protezione dei dati con il fornitore dei servizi (coinvolgendo se del caso le imprese che operano in subappalto). In tal caso si pone un problema

pratico: tutti coloro che trattano dati personali nel calcolatore di un cloud devono essere associati al contratto. Va comunque ricordato che per principio chiunque comunica dati personali all'estero deve dimostrare di avere adottato tutte le misure necessarie per garantire un livello di protezione adeguato.

4. L'utente di servizi di cloud computing è infine anche responsabile affinché il **diritto d'accesso** secondo l'articolo 8 LPD e il **diritto alla cancellazione e alla rettifica** secondo l'articolo 5 LPD siano in qualsiasi momento garantiti e attuati conformemente alle disposizioni in materia di protezione dei dati. L'osservanza di queste condizioni può essere assai problematica, poiché, come detto, l'utilizzazione di sistemi di cloud computing comporta una perdita di controllo sui dati e l'utente non sa (più) dove sono trattati i dati. Queste difficoltà non lo esentano però dai suoi obblighi legali.

Conclusioni

La scelta oculata (inclusa la ponderazione dei rischi), l'istruzione e la sorveglianza del fornitore dei servizi sono aspetti cruciali per trattare dati mediante sistemi di cloud computing. In fin dei conti, l'utente di servizi di cloud computing resta, in qualità di committente, il responsabile verso le persone interessate per il rispetto delle disposizioni in materia di protezione dei dati e risponde di eventuali violazioni di queste disposizioni. Ed è responsabile per le violazioni delle disposizioni in materia di protezione dei dati. Di conseguenza deve valutare con attenzione quali applicazioni e dati conservare presso di sé e quali trasferire nel cloud. A questo scopo occorre che svolga preventivamente una valutazione scrupolosa sul fornitore di servizi di cloud computing e una ponderazione globale dei rischi a livello organizzativo, legale e tecnico. Per scegliere la forma di cloud computing (private cloud, public cloud proprio dell'impresa o hybrid cloud) occorre condurre tempestivamente un'analisi approfondita anche dei requisiti legali in materia di protezione dei dati. In questo modo è possibile garantire dall'inizio un allestimento del cloud conforme alle norme sulla protezione dei dati. Particolare attenzione va posta al trattamento di dati personali tenendo conto di tutte le fasi: dalla memorizzazione dei dati alla loro rielaborazione fino alla cancellazione. Se dopo la ponderazione dei rischi permangono dubbi riguardo al trattamento di dati personali nel cloud, si deve rinunciare a immettere dati nel cloud.

Per saperne di più:

- **ANSSI** Agence nationale de la sécurité des systèmes d'information, «Maîtriser les risques de l'infogérance», dicembre 2010: http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
- **BITKOM** Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., «Cloud Computing - Evolution in der Technik, Revolution im Business – BITKOM-Leitfaden», ottobre 2009: http://www.bitkom.org/de/themen/36129_61111.aspx
- **BSI** Bundesamt für die Sicherheit in der Informationstechnik, «Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestsicherheitsanforderungen in der Informationssicherheit», maggio 2011: https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html
- **CSA** Cloud Security Alliance, «Security Guidance for Critical Areas of Focus in Cloud Computing V2.1», dicembre 2009: https://cloudsecurityalliance.org/csaguide.pdf
- **ENISA** European Network and Information Security Agency, «Benefits, risks and recommendations for information security», novembre 2009: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

- **ENISA** European Network and Information Security Agency, «Security & Resilience in Governmental Clouds», gennaio 2011: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
- **Fraunhofer Institut**, «Cloud-Computing für die öffentliche Verwaltung – ISPRAT-Studie», novembre 2010: http://www.fokus.fraunhofer.de/de/elan/_docs/isprat_cloud_studie_20110106.pdf

Stato: ottobre 2011

***