Il futuro è cloud, ma come garantire la sicurezza dei dati rispettando il GDPR?

Qualsiasi passaggio al **cloud computing** dovrebbe essere basato su una approfondita analisi aziendale. Le domande standard che dovrebbero essere poste sono: È possibile calcolare un rendimento sull'investimento? Può il ritorno a lungo termine essere anticipato? La tecnologia funziona così come la piattaforma interna esistente, se non meglio? È la soluzione cloud efficiente, se non più efficiente, dell'ambiente esistente?

Il passo successivo alla suddetta analisi e forse il più critico nello studio della fattibilità, affidabilità e sicurezza di soluzioni cloud computing a lungo termine è la creazione di una richiesta di proposta (**RFP**) che sia in grado di indirizzare diversi obiettivi. Una **RFP** ben preparata consente ad una organizzazione di indicare in modo conciso tutti i requisiti necessari per una particolare iniziativa tecnologica. Una volta che i requisiti sono tutti concordati e determinati, un'organizzazione ha l'opportunità di richiedere formalmente proposte da vari offerenti e per gli offerenti di presentare tutte le loro proposte utilizzando gli stessi requisiti.

Una componente standard di qualsiasi RFP è la richiesta di informazioni sulla situazione finanziaria e sulla redditività della società venditrice. È importante raccogliere queste informazioni dai fornitori di offerte qualsiasi sia la RFP, ma è particolarmente importante con le nuove tecnologie dove i fornitori considerati sono un mix di venditori tradizionali, con una reputazione riconosciuta da lunga data, e venditori più recenti con una base di clienti più piccola, meno risorse finanziarie, credibilità e reputazione.

Le informazioni pertinenti inserite nella RFP possono richiedere: da quanto tempo l'azienda è in attività, la crescita della base clienti e delle entrate, il credito disponibile dell'azienda e riferimenti da altri clienti. In definitiva, queste informazioni aiutano il potenziale cliente a valutare e bilanciare il valore della potenziale soluzione del fornitore, che potrebbe sembrare significativa, sullo sfondo della forza finanziaria e del futuro dell'azienda, che potrebbero essere traballanti.

Una volta selezionato un fornitore per supportare un'iniziativa di cloud computing, un modo intelligente di proseguire è quello di attivare un progetto pilota: un'iniziativa limitata che aiuti l'organizzazione a muovere i primi passi nel cloud riducendo al minimo i rischi possibili perché il progetto è più piccolo e gestibile. Un progetto pilota consente inoltre all'organizzazione di apprendere e acquisire conoscenze e competenze durante il suo svolgimento: se e quando dovessero sorgere problemi, potenzialmente saranno più facili da risolvere e meno rischiosi in quanto l'impronta del progetto è relativamente piccola.

Il raggiungimento di tale traguardo può essere agevolato impiegando metodologie sviluppate e consolidate essendo state impiegate da organizzazioni differenti operanti in molteplici industrie. Una metodologia approvata e diffusa è quella indicata da **Cloud Security Alliance**. Gli strumenti resi disponibili alle organizzazioni in procinto di lanciare iniziative in ambito cloud computing sono: CSA Security Trust Assurance Registry (CSA STAR) accreditata anche in ambito **AgID** per la valutazione dei fornitori di servizi cloud SaaS, Cloud Control Matrix contente i controlli per la valutazione dei rischi per soluzioni cloud e/o impiegabile per la predisposizione di RFP.

La sicurezza è probabilmente la principale preoccupazione delle aziende quando si considera uno spostamento di dati o risorse informatiche nel cloud. Le aziende si sono abituate a salvaguardare dati e applicazioni all'interno dei data center, così qualunque asset situato al di fuori della giurisdizione aziendale tradizionale scaturisce preoccupazioni, preoccupazioni e sfide non solo per le policy sui dati e sulle applicazioni, ma anche per la cultura e i valori ben radicati di un'azienda.

Prima del cloud computing, la sicurezza informativa era interpretata come una sicurezza perimetrale in cui una soluzione firewall serviva per bloccare i traffico indesiderato, in cui un sistema di controllo serviva per stabilire restrizioni accesso alla rete aziendale, e in cui un strumento antivirus serviva per impedire la proliferazione di malware. Con molti meno cellulari e con praticamente tutti i dati interni, questa strategia aveva senso.

I tempi sono cambiati: il cloud computing sposta i dati al di fuori del tradizionale perimetro della sicurezza aziendale, hacker professionisti hanno dato prova di esplorare a loro favore ogni possibile tattica per individuare punti deboli nelle soluzioni adottate. Le aziende sono chiamate a dare devono dare un nuovo sguardo alla strategia, obiettivi e alle misure difese di sicurezza.

Altresì molte organizzazioni sono riluttanti a passare al cloud computing a causa di restrizioni normative che vietano loro di utilizzare il cloud computing per l'archiviazione di dati sensibili o a causa di dubbi sulla privacy (**GDPR**) dei dati nel cloud.

Come dovrebbero procedere le organizzazioni per sfruttare i benefici del cloud computing e contestualmente rispondere anche ai requisiti di sicurezza e più in generale agli obblighi di privacy?

Una buona pratica prevede che l’organizzazione si doti di una cornice operativa di riferimento per la gestione dei requisiti di sicurezza, che rappresenti la struttura portante sulla quale aggiungere i mattoni per la gestione dei requisiti di sicurezza nel cloud e per la gestione degli obblighi relativi alla privacy.

Uno schema adottabile prevede la realizzazione delle prescrizioni di standard **ISO/IEC 27001** (information security management system) e le estensioni ISO/IEC 27017 (code of practice for information security controls based on iso/iec 27002 for cloud services) e ISO/IEC 27018 (code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors), Attraverso la realizzazione di tale schema, un insieme importante delle direttive previste dal GDPR sono soddisfatte.

Qualsiasi business leader preoccupato per la sicurezza e l’affidabilità del cloud ad ospitare dati e applicazioni, dovrebbe ricordare che si sono fidati di salvare e di archiviare le proprie risorse finanziarie personali in un sistema bancario virtuale (nuvola) per anni.

https://www.key4biz.it/il-futuro-e-cloud-ma-come-assicurare-la-sicurezza-dei-dati-rispettando-il-gdpr/270170/