PREMESSA

L'affidamento dei dati in cloud ai sensi della ISO 27017: 2015 prevede la verifica sia per il cliente che per il fornitore di determinati requisiti.

Boxxapps in completa trasparenza per la gestione dei servizi offerti vi fornisce in seguito un riepilogo dei vostri adempimenti anche riferiti a quelli che Boxxapps adotta come fornitore in ottemperanza alla ISO 27017: 2015.

Qualora riscontriate delle difformità rispetto a quanto sotto riportato e gli eventuali servizi offerti, vi invitiamo a segnalarcelo tramite i nostri consueti canali di comunicazione

PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

- I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte del fornitore pertanto deve adottare l'applicazione di metodi e processi che siano certificati da terzi in ambito ISO 27001, ISO 27018 e ISO 27017;

- Devono essere ben definiti gli utenti del servizio cloud.
  Il contesto in cui gli utenti utilizzano il servizio cloud;
  Gli utenti del Cliente con profilo amministratori del servizio cloud che hanno accesso privilegiato;
  Le posizioni geografiche dell'organizzazione del fornitore di servizi cloud;
  I paesi in cui il fornitore può memorizzare i dati dei Clienti (anche temporaneamente).

- Il cliente del servizio deve concordare con il fornitore un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e confermare che può adempiere ai propri ruoli e responsabilità assegnati. I ruoli di sicurezza delle informazioni e le responsabilità di entrambe le parti dovrebbero essere indicati in un accordo.

- Il cliente del servizio dovrebbe identificare le autorità rilevanti per l'operazione tra cliente e fornitore quali ad esempio il Garante per la protezione dei dati personali Italiano, l'Agid, la Polizia postale e delle comunicazioni.

- Il cliente del servizio deve aggiungere i seguenti elementi ai programmi interni di sensibilizzazione, istruzione e formazione per:
  - I responsabili,
  - Gli amministratori,
  - Gli integratori di servizi cloud
  - Gli utenti del servizio cloud, inclusi i dipendenti e gli appaltatori interessati.

  La consapevolezza della sicurezza delle informazioni, i programmi di istruzione e formazione sui servizi cloud dovrebbero essere forniti alla direzione e ai responsabili della supervisione, compresi quelli delle unità operative.
  Questi sforzi supportano un efficace coordinamento delle attività di sicurezza delle informazioni in ambiti quali:
  - Standard e procedure per l'utilizzo dei servizi cloud;

- Rischi per la sicurezza delle informazioni relativi ai servizi cloud e come tali rischi sono gestiti;
- Rischi per l'ambiente di rete e di sistema con l'uso di servizi cloud;
- considerazioni legali e normative applicabili.

- L'inventario delle risorse deve tenere conto delle informazioni e delle risorse associate e archiviate nell'ambiente di cloud computing. I registri dell'inventario dovrebbero indicare dove vengono mantenute le risorse, ad esempio l'identificazione geografica del servizio.

- Ogni informazione dislocata in cloud dovrebbe essere identificata ed etichettata. Ove applicabile, è possibile adottare la funzionalità fornita dal provider di servizi cloud che supporta l'etichettatura.

- La politica di controllo dell'accesso al servizio in cloud deve prevedere la compartimentazione per ciascun servizio cloud, nel caso dovessero essere molteplici.

- Il cliente del servizio deve utilizzare tecniche di autenticazione sufficienti (ad esempio, autenticazione a più fattori) per autenticare i suoi utenti con profilo amministratore in base ai rischi identificati.

- Il cliente del servizio deve verificare che la procedura di gestione del fornitore per l'allocazione delle informazioni di autenticazione segreta, come le password, soddisfi i propri requisiti.

- Il cliente del servizio dovrebbe garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate.
  Ciò include:
  - La limitazione dell'accesso ai servizi cloud;
  - Alle funzioni del servizio cloud;
  - Ai dati dei clienti gestiti dal servizio cloud.

- Laddove l'utilizzo di programmi di utilità è consentito, il cliente deve identificare i programmi di utilità da utilizzare nel proprio ambiente e assicurarsi che non interferiscano con i controlli del servizio cloud.

- Il cliente del servizio, se giustificato dall'analisi del rischio, dovrebbe implementare i controlli crittografici per l'utilizzo dei servizi cloud.
  I controlli dovrebbero essere di forza sufficiente per mitigare i rischi identificati, indipendentemente dal fatto che tali controlli siano forniti dal cliente o dal fornitore di servizi cloud.
  Quando il fornitore offre la crittografia, il Cliente del servizio deve esaminare tutte le informazioni fornite dal fornitore per confermare se le funzionalità di crittografia:
  - soddisfano i suoi requisiti di politica ……;
  - sono compatibili con qualsiasi altra protezione crittografica già utilizzata;
  - sono applicate ai dati a riposo e in transito e all'interno del servizio.

- Il cliente deve identificare le chiavi crittografiche per ciascun servizio cloud e implementare le procedure per la loro gestione.

  Laddove il servizio cloud fornisce funzionalità di gestione delle chiavi crittografiche, il Cliente dovrebbe richiedere le seguenti informazioni sulle procedure utilizzate per la loro gestire:
  - tipo di chiavi;
  - specifiche del sistema di gestione delle chiavi, comprese le procedure per ciascuna fase del ciclo di vita chiave, ossia la generazione, la modifica o l'aggiornamento, la memorizzazione, il ritiro, il recupero, il mantenimento e la distruzione;
  - procedure di gestione delle chiavi consigliate per l'utilizzo da parte del cliente. Il cliente del servizio non dovrebbe consentire al fornitore di archiviare e gestire le chiavi di crittografia per operazioni crittografiche quando il cliente impiega la propria gestione delle chiavi o un servizio di gestione delle chiavi separato e distinto.

- Il cliente del servizio deve richiedere la conferma che il fornitore ha le politiche e le procedure per lo smaltimento sicuro o il riutilizzo delle risorse.

- Il processo di gestione del cliente del servizio cloud dovrebbe tenere conto del profilo di servizi cloud fornito dal fornitore.

- Il cliente del servizio deve assicurarsi che la capacità concordata con il fornitore venga soddisfatta. Il cliente deve monitorare l'utilizzo dei servizi e prevedere le proprie esigenze di capacità, al fine di garantire le prestazioni dei servizi cloud nel tempo.

- Laddove il fornitore fornisca funzionalità di backup come parte del servizio cloud, il cliente dovrebbe:
  - richiedere le specifiche della capacità di backup dal fornitore.
  - verificare che soddisfi i requisiti di backup.
  - essere responsabile dell'implementazione delle funzionalità di backup quando il provider del servizio cloud non le fornisce.

- Devono essere definiti i requisiti per la registrazione degli eventi e verificare che il servizio cloud soddisfi tali requisiti.

- Se le operazioni di amministrazione informatica sono delegate al cliente del servizio cloud, è necessario registrare l'operazione e le prestazioni di tali operazioni. Il cliente del servizio cloud deve determinare se le funzionalità di registrazione fornite dal provider di servizi cloud sono appropriate.

- Il cliente del servizio cloud dovrebbe richiedere informazioni sulla sincronizzazione dell'orologio utilizzata per i sistemi del fornitore di servizi cloud.

- Il cliente del servizio dovrebbe richiedere informazioni al fornitore sulla gestione delle vulnerabilità tecniche che possono influenzare i servizi forniti.

Il cliente del servizio dovrebbe identificare le vulnerabilità tecniche di cui sarà responsabile e dovrà definire chiaramente un processo per gestirle.

- Il cliente del servizio deve definire i requisiti per la separazione delle reti per ottenere l'isolamento nell'ambiente condiviso di un servizio cloud e verificare che il provider di servizi cloud soddisfi tali requisiti.

- Il cliente del servizio deve determinare i requisiti di sicurezza delle informazioni e quindi valutare se i servizi offerti dal fornitore possono soddisfare tali requisiti. Per questa valutazione, il cliente del servizio dovrebbe richiedere informazioni sulle funzionalità di sicurezza delle informazioni al fornitore.

- Il cliente del servizio dovrebbe richiedere informazioni al fornitore in merito all'utilizzo di procedure di sviluppo sicure.

- Il cliente del servizio dovrebbe includere il fornitore nella sua politica di sicurezza delle informazioni, per le relazioni con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati dei clienti del servizio da parte del fornitore.

- Il cliente deve confermare i ruoli e le responsabilità in materia di sicurezza delle informazioni relative al servizio cloud, come descritto nel contratto di servizio.
  Questi possono includere i seguenti processi:
  - protezione da malware;
  - backup;
  - controlli crittografici;
  - gestione della vulnerabilità;
  - gestione degli incidenti;
  - controllo della conformità tecnica;
  - test di sicurezza;
  - auditing;
  - raccolta, manutenzione e protezione delle prove, compresi i registri e le liste di controllo;
  - protezione delle informazioni al termine del contratto di servizio;
  - autenticazione e controllo degli accessi;
  - identità e gestione degli accessi.

- Il cliente del servizio deve verificare l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni e deve assicurarsi che soddisfi i propri requisiti.

- Il cliente del servizio dovrebbe richiedere informazioni al fornitore riguardo ai meccanismi per:
  - segnalare un evento di sicurezza delle informazioni che ha rilevato al fornitore;
  - ricevere segnalazioni riguardanti un evento di sicurezza delle informazioni rilevato dal fornitore;
  - tenere traccia dello stato di un evento di sicurezza delle informazioni segnalato.

- Il cliente del servizio dovrebbe considerare il problema che leggi e regolamenti pertinenti possono essere quelli delle giurisdizioni che regolano il fornitore, oltre a quelli che regolano lui stesso
  Il cliente del servizio deve richiedere evidenza della conformità del fornitore con le normative e gli standard pertinenti richiesti per le sue attività.
  Tali prove possono essere le certificazioni prodotte dagli auditor di terze parti.

- L'installazione di software con licenza commerciale in un servizio cloud può causare una violazione dei termini della licenza per il software.
  Il cliente del servizio dovrebbe avere una procedura per identificare i requisiti di licenza specifici per il cloud prima di consentire l'installazione di qualsiasi software con licenza.
  Un'attenzione particolare dovrebbe essere rivolta ai casi in cui il servizio cloud è elastico e scalabile e il software può essere eseguito su più sistemi o core del processore rispetto a quanto concordato.

- Il cliente del servizio deve richiedere informazioni al fornitore sulla protezione dei record raccolti e archiviati dal fornitore rilevanti per l'utilizzo dei servizi.

- Il cliente del servizio deve verificare che la serie di controlli crittografici applicabili all'utilizzo di un servizio cloud sia conforme agli accordi, alle leggi e ai regolamenti pertinenti.

- Il cliente del servizio dovrebbe richiedere prove documentate che l'implementazione dei controlli di sicurezza delle informazioni e linee guida per il servizio cloud sia in linea con qualsiasi richiesta avanzata dal fornitore. Tali prove potrebbero includere certificazioni rispetto agli standard pertinenti.

- Il cliente del servizio deve definire o estendere le sue politiche e procedure esistenti in conformità con il suo uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso del servizio cloud.

- Il cliente del servizio deve richiedere una descrizione documentata del processo di cessazione del servizio che copra il reso e la rimozione delle risorse del cliente seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi del fornitore. La descrizione dovrebbe elencare tutte le risorse e documentare la pianificazione per la cessazione del servizio, che dovrebbe avvenire in modo tempestivo.

- Quando si configurano macchine virtuali, sia i clienti che i fornitori devono garantire che gli aspetti appropriati siano gestiti in hardening (ad esempio solo le porte, i protocolli ei servizi necessari) e che siano adottate le misure tecniche appropriate (ad esempio, anti-malware, logging) per ogni macchina virtuale utilizzata.

- Il cliente del servizio deve documentare le procedure per operazioni critiche in cui un errore può causare danni irreversibili alle risorse nell'ambiente di cloud computing. Esempi di operazioni critiche sono:
  - installazione, modifica e cancellazione di dispositivi virtualizzati come server, reti e storage;
  - procedure di terminazione per l'utilizzo del servizio cloud;

- backup e ripristino.

  Il documento dovrebbe specificare che un supervisore dovrebbe monitorare queste operazioni.

- Il cliente dovrebbe richiedere informazioni al fornitore delle funzionalità di monitoraggio disponibili per ciascun servizio cloud.

Mestre Venezia, 20/11/2018

BOXXAPPS S.r.l.
Amministratore unico.
Doro Luciano