...making excellence a habit.™

ISO/IEC 27017

Estendere ISO/IEC 27001 all'interno del Cloud

Whitepaper

La prima preoccupazione per chi utilizza sevizi cloud è la sicurezza – questa risulta essere il principale motivo per il quale le organizzazioni hanno esitazioni nell'adottare una soluzione cloud, nonostante la scalabilità e flessibilità che questa possa offrire. La capacità dei Cloud Service Provider (CSP) di trattare con sufficiente attenzione i dati relativi ai clienti rappresenta una delle tematiche più importanti.

Gli elementi principali sono rappresentati dalla paura che i dati potrebbero finire nelle mani sbagliate e dalla necessità di sapere quali sono le misure adottate per prevenire eventuali mancanze da parte degli operatori. Altre questioni quali l'identità del cliente, la separazione delle attività su server virtuali e ciò che accade ai beni in caso un CSP si ritiri dal mercato sono altrettanto importanti per i potenziali utenti cloud.

La serie ISO/IEC 27001 affronta alcuni di questi problemi ma il nuovo standard, ISO/IEC 27017 "Tecnologia delle Informazioni - Tecniche di sicurezza", va maggiormente in dettaglio e offre più tranquillità ai potenziali clienti di servizi cloud. Tipicamente gli standard relativi al cloud e quelli tecnici si occupano dei controlli e delle Linee guida rivolgendosi solo ai cloud provider.

L'unicità e la grande utilità dello standard ISO/IEC 27017 risiede nel fornire linee guida e consulenza sia ai CSP sia ai clienti.

Oltre a garantire che i servizi siano sicuri, ISO/IEC 27017 ha anche lo scopo di educare i clienti su cosa devono volere dal loro host nel cloud.

Lo standard fornisce una guida relativa alla siucrezza del cloud computing che si fonda su 37 dei controlli dalla norma ISO/IEC 27002, ma dispone anche di sette nuovi controlli.

- **CLD.6.3.1:** L'accordo sulla assegnazione delle responsabilità (condivisione o suddivisione) in carico a cliente e fornitore, riguardo ai diversi ruoli di sicurezza di informazione associati ai servizi cloud, deve essere definito, registrato e comunicato in modo chiaro.
- **CLD.8.1.5:** Indica le modalità attraverso le quali gli assets devono essere riconsegnati o rimossi dal cloud quando termina il contratto/accordo tra cliente e provider.
- **CLD.9.5.1:** Il fornitore deve proteggere e separare l'ambiente virtuale del cliente da quello di altri clienti e soggetti esterni.
- **CLD.9.5.2:** Il cliente e il provider devono garantire che le macchine virtuali siano configurate e rinforzate per rispondere alle esigenze dell'organizzazione.
- **CLD.12.1.5:** Responsabilità del cliente nel documentare e monitorare le operazioni amministrative e le procedure connesse con l'ambiente cloud. Requisiti dei CSP per condividere le informazioni su operazioni e procedure critiche quando richiesto dai clienti.
- **CLD.12.4.5:** Come le funzionalità del provider consentono al cliente di monitorare l'attività all'interno di un ambiente cloud computing.
- **CLD.13.1.4:** Devono essere attuate configurazioni coerenti per allineare l'ambiente di rete virtuale con le policy di sicurezza delle informazioni presenti nella rete fisica.

Ruoli e responsabilità

L'ambiguità dei ruoli e nella definizione e attribuzione delle responsabilità relative a questioni quali la proprietà dei dati, il controllo degli accessi e la manutenzione delle infrastrutture può dar luogo a controversie commerciali e legali, soprattutto quando si tratta con soggetti terzi. Citando quanto evidenziato nello standard:

> "Le informazioni e i file presenti nell'ambiente fornito dal cloud provider, creati o modificati durante l'utilizzo del servizio, possono essere fondamentali per la sicurezza delle operazioni, le attività di recovery e la continuità del servizio. La proprietà di tutti i beni e l'assegnazione delle responsabilità per le operazioni legate a tali attività, come quelle di backup e ripristino, dovrebbero essere definite e documentate. In caso contrario, c'è il rischio che il fornitore di servizi di cloud presupponga che il cliente esegua queste operazioni vitali (o viceversa), e può verificarsi una perdita di dati."

In sostanza, la norma richiede che, fin dall'inizio, venga chiaramente delineata quale parte è responsabile delle diverse attività.

Controlli di sicurezza

Lo standard ISO / IEC 27017, non solo aiuta a definire la divisione delle responsabilità, ma esamina anche in modo molto più dettagliato il tipo di controlli di sicurezza che i fornitori di servizi dovrebbero implementare, contribuendo a ridurre le barriere all'adozione del cloud.

ISO/IEC 27017 offre ai fornitori di servizi cloud un mezzo per indicare il livello di controlli che vengono attuati. La certificazione da parte di soggetti indipendenti significa dimostrare la presenza di policy adeguate e, soprattutto, dare indicazione su quali controlli sono stati introdotti.

Queste informazioni dovrebbero essere condivise con il cliente prima di qualsiasi firma del contratto per diminuire la possibilità di problemi in futuro.

Nel caso in cui gli audit indipendenti non fossero funzionali o potessero comportare un rischio maggiore per le informazioni, lo standard prevede la possibilità per il CSP di effettuare un self-assessment. In questo caso il CSP è tenuto ad avvisare il cliente di avere effettuato un self-assessment.

Crittografia

È presente anche una linea guida relativa alla crittografia utilizzata, valida sia per il cliente sia per il fornitore, poiché entrambi sono responsabili di questo aspetto. Il provider dovrebbe comunicare al cliente come sta utilizzando la crittografia e aiutarlo nell'applicare la propria protezione. Inoltre vanno anche considerati i casi specifici, quali le informazioni sanitarie, che richiedono ulteriori normative.

Ai clienti dovrebbe essere comunicato in anticipo quale tipo di crittografia si utilizza e questi dovrebbero utilizzarla se, da un analisi del rischio, emergesse che il suo utilizzo sia necessario. In realtà, questo è proprio il tipo di controversia o incomprensione che ha generato la necessità di avere uno standard. Non solo le due parti devono assicurare reciprocamente che la rete sia protetta ma dovrebbero anche essere in grado di assicurare l'un l'altro che c'è compatibilità tra i due sistemi. Soprattutto, dovrebbe essere stabilito se questi controlli si applichino solo ai dati all'interno dei sistemi, solo a quelli in transito o ad entrambi (tematica che causa incomprensioni)..

Rapporti col cliente

La norma non si occupa solo di aspetti tecnologici ma delinea le linee guida anche per la formazione. Molti clienti sono soddisfatti delle infrastrutture fornite dal cloud provider ma sono prudenti circa il livello di supporto che possono avere.

Vi sono diverse evidenze che indicano come siano spesso i dipendenti il punto debole all'interno del sistema di sicurezza di un'organizzazione. I clienti devono essere consapevoli non sono solo della presenza di dispositivi di sicurezza difettosi, ma piuttosto se il personale stia seguendo tutte le misure appropriate. Il nuovo standard non solo prevede che i fornitori debbano fornire la consapevolezza e la formazione ai dipendenti e collaboratori, ma stabilisce anche che la formazione debba essere incentrata sui requisiti normativi, l'accesso dei clienti e richieste specifiche..

Proprietà degli Asset

Un punto che genera confusione è la determinazione di chi è il proprietario di tutto quello che risiede all'interno del cloud. Lo standard suggerisce che ci sia un inventario dei beni memorizzati nel cloud e fa riferimento alle line guida sulla proprietà, sull'uso corretto e sulla restituzione degli asset presenti nella ISO/IEC 27002. Il nuovo standard definisce anche i parametri per l'eliminazione sicura degli asset dei clienti in modo che i dati sensibili non vengano semplicemente gettati in cestini virtuali.

Chi ne trae beneficio?

La risposta è semplice: tutti. Chiunque si avvicini ai servizi cloud.

La strada verso il cloud può essere piena di incomprensioni e apprensione. Qualsiasi organizzazione che affidi a terzi dati sensibili dei clienti è a conoscenza che esistono "zone grigie" in cui i diritti e le responsabilità non sono stati chiaramente definiti. Capita spesso che ci basi esclusivamente sulla fiducia, non necessariamente la migliore ricetta per il successo.

Grazie al supporto dello standard, CIO e IT manager saranno incoraggiati ad un cambiamento nei loro rapporti con i CSP introducendo la garanzia di un livello minimo di sicurezza del cloud computing.

Una formazione adeguata per comprendere e implementare la ISO/IEC 27017 può rivelarsi molto utile per prendere decisioni circa l'adozione di soluzioni cloud e sulla scelta dei partner più adatti alle proprie esigenze.

I CSP che scelgono di implementare ISO/IEC 27017 ne beneficeranno avendo la consapevolezza che stanno offrendo una soluzione sicura e che genera fiducia nei loro clienti, requisito fondamentale nella costruzione di un rapporto di lungo corso. E, naturalmente, lavorando con i propri clienti attraverso il loro processo di adozione ISO/IEC 27017 si proteggeranno da accuse pericolose o azioni legali che possono interrompere la loro attività e danneggiare il loro marchio.

bsi.

bsigroup.it
marketing.italy@bsigroup.com
+39 02 6679091