Allegato 5 - Requisiti di sicurezza per l'hosting dei dati

I presenti requisiti sono applicabili all'hosting di tutte le applicazioni e tutti i dati **BT riservati (IC, "In Confidence")** o **strettamente riservati (ISC, "In Strictest Confidence")** presenti in sedi non gestite da BT né di sua proprietà. Sono inclusi, senza intento limitativo, i servizi cloud in cui a) i dati in transito sono sicuri e protetti dall'intercettazione generalmente mediante un protocollo crittografato e b) i dati BT crittografati a riposo nell'ambito del servizio cloud.

Le seguenti condizioni valgono per le applicazioni e i dati riservati gestiti in hosting al di fuori di BT:

- Il data centre deve aver ottenuto una valida certificazione ISO 27001 (o altre certificazioni che attestino controlli equivalenti) in materia di gestione della sicurezza o dovrà aderire ai requisiti di sicurezza della certificazione ISO 27001 o a politiche di sicurezza allineate alla ISO27001 e/o avere avviato la procedura di ottenimento della certificazione ISO27001 entro un lasso di tempo concordato con BT;
- I dati "in transito" devono essere altamente crittografati al fine di proteggere i dati BT tra il punto di uscita da BT e il perimetro del DC (generalmente, il dispositivo di bilanciamento del carico e decrittografia posto dietro il firewall perimetrale del DC);
- I tecnici del DC con accesso fisico ai server non devono disporre di un accesso logico all'ambiente di produzione, mentre gli amministratori con accesso logico ai sistemi non devono disporre di un accesso fisico al DC.
- L'intero accesso logico deve essere controllato tramite un sistema di sicurezza degli account per far sì che la gestione delle password sia controllata e il corretto processo di autorizzazione sia implementato in modo da garantire l'identificazione del richiedente (ad es. CyberArk).
- Per quanto riguarda l'accesso privilegiato, (incluso, senza intento limitativo, il DBA) la gestione delle password deve essere temporizzata e, laddove possibile, deve essere prevista l'implementazione di ulteriori restrizioni agli indirizzi IP di origine.
- L'accesso privilegiato, ad es. DBA, ASG ecc., ai sistemi che trattano informazioni BT deve essere conforme ai requisiti dell'allegato 1 - Classificazione delle informazioni.
- Per l'accesso remoto, dovrà essere utilizzata una rete privata virtuale in combinazione con l'autenticazione a due fattori basata sui ruoli; inoltre, l'accesso remoto privilegiato di terze parti sarà limitato ai sistemi in cui i dati BT sono in transito o a riposo nello stesso Paese del DC, oppure in un Paese o territorio in cui sia garantito un livello di protezione adeguato per i dati BT.
- Implementare processi di gestione delle chiavi crittografiche validi per l'intero ciclo di vita e commisurati alle migliori prassi di settore.
- L'accesso fisico alle aree o apparecchiature in cui sono archiviate o trattate le Informazioni BT deve essere soggetto ad un processo verificabile (ad es., richiesta di modifiche), per garantire che l'accesso venga autorizzato unicamente per la minima durata necessaria, escludendo pertanto l'accesso permanente.
- L'archiviazione fuori sede dei dati di backup deve essere crittografata ai sensi dei requisiti dell'allegato 1.
- È necessario stabilire controlli atti a contenere, individuare e prevenire l'accesso non autorizzato. I controlli devono generare una pista di controllo basata sul principio "chi, cosa, dove e quando":
- Chi era l'utente, ad es. l'ID dell'account utente;
- Per quali beni è stato effettuato l'accesso, ad es. i dati;

- Da dove è stato effettuato l'accesso, ad es. l'indirizzo IP; e
- Quando, ad es. un indicatore di data/ora.
- Ogni accesso fisico o logico deve essere registrato e la relativa documentazione dovrà essere conservata per almeno 1 anno.
- In caso di violazione con conseguente compromissione, furto o alterazione dei dati BT, deve essere prevista una procedura per far sì che BT venga informata entro tempi ragionevoli e in modo opportunamente dettagliato.

In caso di informazioni ISC trova inoltre applicazione quanto segue:

- Il data centre deve essere sottoposto ad una ispezione di sicurezza in loco;
- I database, server di applicazioni, ecc. devono essere installati presso un'apposita infrastruttura, non in regime di multi-tenancy ed essere ospitati in un rack dedicato all'interno di una gabbia di protezione. Laddove questo requisito non possa essere soddisfatto, una procedura BT di valutazione dei rischi dovrà fornire una garanzia di idoneità, dimostrando l'adeguata separazione dei dati BT dai dati degli altri clienti che condividono lo stesso ambiente e assicurando che i DBA non dispongano di accesso logico alle istanze dei clienti e non possano vedere i dati dei clienti in modo assemblato. Le tabelle e le righe dei database non devono riflettere la vista di una singola istanza cliente.
- Devono essere in atto processi atti a garantire che i dati ISC vengano eliminati in maniera sicura al termine del ciclo di vita nel cloud; tutti i dispositivi di archiviazione contenenti dati ISC devono essere cancellati/eliminati come specificato in allegato 1;