Allegato “D”

CHECKLIST VERIFICA SERVIZIO SISTEMI DI BACKUP

Il presente documento ha l’obiettivo di verificare le modalità con cui sono strutturati ed eseguiti i processi di backup dell’organizzazione, sia per gli ambienti di virtualizzazione che per dump di database e per copie di files. Oltre al backup, vengono anche verificate le condizioni al contorno, come i backup offline, le copie remote e le operazioni pianificate di ripristino.

DOMANDA	RISPOSTA	NOTE DI COMPILAZIONE
Sono definite delle procedure per l’integrazione nel processo di backup di nuovi archivi di dati o per la revisione periodica degli archivi sottoposti a backup, con eventuale dismissione di quelli non più necessari?		Specificare se esiste una procedura che preveda la presa in carico di nuovi archivi di dati da sottoporre a backup, oltre che la verifica periodica della necessità di sottoporre a backup gli archivi in essere, eventualmente dismettendo quelli non più attivi/necessari. Tale procedura deve prevedere la verifica e la documentazione della stessa, riportando gli esiti del controllo.
Sono definite delle procedure documentate di backup, con indicazione delle operazioni effettuate e delle tempistiche, dei salvataggi effettuati, dei ruoli e delle responsabilità correlate?		Specificare se esiste un prospetto documentato in cui siano elencati: - Gli archivi sottoposti a backup - Le modalità di salvataggio (es, snapshot delle macchine virtuali, copia del dump di DB su NAS o tape, sincronizzazione di cartelle, ecc) - La frequenza e tipologia (backup full / incrementale / differenziale…) - L’orario delle singole operazioni e la durata - La destinazione logica in cui vengono salvate la copie e la localizzazione fisica dei supporti di backup - Eventuali note /criticità della copia - L’ultima versione revisionata del presente documento
In caso di archivi “storici” non più sottoposti ad aggiornamento ma di cui è necessaria la conservazione (es. backup di vecchie applicazioni legacy o archivi di dati sottoposti a consultazione periodica), è presente adeguata documentazione in cui sono illustrate le modalità per la consultazione e/o ripristino nonché la localizzazione delle copie?		Indicare se presente una mappatura documentata degli archivi “storici” soggetti a conservazione con indicata la descrizione dell’archivio, la localizzazione, la presenza di copie, le modalità di ripristino/consultazione ed eventuali dotazioni necessarie (es. spazio su disco, particolare sistema operativo o ambiente di virtualizzazione necessario per la consultazione, la posizione in cui reperire eventuali password di decrittazione, ecc). Deve essere presente almeno una copia degli archivi offline, pertanto va indicata l’esistenza e la localizzazione di detta copia.
Le attività di backup sono effettuate da un utente dedicato, diverso da administrator (o root, admin), con password complessa di almeno 14 caratteri?		Al fine di impedire l’accesso non autorizzato alle risorse dedicate al backup dei dati, è necessario proteggerle con password sicure (una password con meno di 14 caratteri non può, allo stato attuale della tecnologia, considerarsi sicura) e utenti dedicati (non appartenenti al dominio dell’infrastruttura di rete in cui si trovano i server di produzione).
Gli ambienti di backup sono accessibili da utenze separate dalla rete di produzione, con credenziali robuste e/o strumenti di sicurezza avanzati per la gestione delle credenziali?		Sarebbe auspicabile che le utenze dei sistemi di backup (e in particolare quelle di accesso ai repository) fossero separate dagli altri sistemi di autenticazione, con soluzioni avanzate di sicurezza come Multi Factor Authentication.

Allegato “D”

DOMANDA	RISPOSTA	NOTE DI COMPILAZIONE
Su quanti supporti differenti viene effettuato il backup dei dati (di quante copie di salvataggio si dispone)?		Indicare di quante copie su supporti diversi si dispone dei dati, la localizzazione e la modalità di ripristino.
Ambienti di virtualizzazione: la console di virtualizzazione e di backup delle macchine virtuali si trova sulla stessa LAN in cui operano le macchine virtuali oppure ha una rete dedicata?		Se dei cyber criminali riuscissero ad accedere alla rete LAN di produzione e ad acquisire diritti di amministrazione della stessa, nel caso in cui i sistemi di backup fossero raggiungibili attraverso strumenti di accesso remoto allora la probabilità di sabotaggio degli stessi sarebbe altissima. Pertanto, è indispensabile e inderogabile disporre di sistemi e supporti di backup inaccessibili dalla rete di produzione. Tale segregazione dal resto della rete deve essere garantita per: - La console di virtualizzazione - La console di backup delle macchine virtuali - L’ambiente operativo in cui sono localizzate le risorse dedicate ai processi di virtualizzazione - Il repository delle copie delle macchine virtuali
Ambienti di virtualizzazione: la console di virtualizzazione e gli ambienti in cui sono effettuate le copie delle macchine virtuali sono comunque raggiungibili tramite Remote Desktop, VNC, TeamViewer e/o altri strumenti di accesso da remoto?		
Ambienti di virtualizzazione: il server di virtualizzazione e gli ambienti in cui sono effettuate le copie delle macchine virtuali sono hanno cartelle condivise con altri dispositivi sulla rete?		
Ambienti di virtualizzazione: il server di virtualizzazione e gli ambienti in cui sono effettuate le copie vengono utilizzate anche per funzioni diverse dal backup delle macchine virtuali?		
Ambienti di virtualizzazione: è stabilita una strategia di backup che preveda almeno un full backup settimanale e altri backup incrementali delle macchine virtuali?		Indicare le modalità di copia delle macchine virtuali, specificando se vengono effettuate copie full e/o incrementali e con che periodicità.
Backup dei dati: è stabilita una strategia di backup che preveda almeno un full backup settimanale e altri backup incrementali o differenziali?		Il backup dei dati consiste nella copia dei files su altri supporti o cartelle di rete. Indicare la strategia di backup, specificando se vengono effettuate copie full/differenziali/incrementali e con che periodicità.
Backup dei dati: viene verificato l’esito e la consistenza dei backup effettuati (ad esempio, introducendo procedure per il conteggio dei files sottoposti a backup con raffronto con i dati di backup di periodi analoghi)?		Il backup effettuato tramite copia dei files non prevede la verifica automatica della consistenza degli archivi, pertanto deve essere verificato puntualmente l’esito delle operazioni e tale riscontro deve essere documentato (es. riportando informazioni tipo il conteggio dei file sottoposti a backup o altri dati di contesto).

Allegato “D”

DOMANDA	RISPOSTA	NOTE DI COMPILAZIONE
Backup dei dati: è disponibile un supporto di salvataggio scollegato dal resto della rete?		Il backup dei dati attraverso comandi di copia del sistema operativo prevede la connessione, almeno temporanea, dell’archivio di origine e di quello di destinazione. E’ necessario disporre di un backup offline al fine di garantire la segregazione delle copie, non bypassabile tramite accesso remoto.
Dump database: viene verificata quotidianamente la data dell’ultima esportazione, al fine di avere la certezza di disporre di un dump recente?		L’unico sistema veramente efficace di verifica dell’effettuazione del dump (della consistenza dello stesso si parlerà nel punto successivo) è verificare la data del file di dump. Pertanto, è bene documentare con una checklist, compilata ogni volta che viene fatta la verifica, la data del controllo e l’esito.
Dump database: viene verificato quotidianamente che la dimensione dei dump è di dimensioni simili al database stesso e che tende ad aumentare con il passare del tempo (e della crescita dei dati contenuti)? Viene verificato che vi sia abbastanza spazio nel supporto che custodisce il backup?		L’informazione sulla dimensione del backup è condizione necessaria (ma non sufficiente, la certezza può essere data solo da un test di ripristino) per la verifica di consistenza dello stesso. Pertanto, è necessario verificare che il dump abbia dimensioni coerenti rispetto alla dimensione del DB e documentare il controllo. NB se il DB indicizza dei files contenuti in un repository a parte, è necessario verificare anche il backup del repository.
Dump database: vengono verificati quotidianamente i log dell’esito delle operazioni di backup?		I log descrivono l’esito delle operazioni di dump ed eventuali criticità riscontrate, pertanto devono essere verificati e il controllo deve essere documentato nell’apposita checklist di riscontro del processo.
Dump database: i backup sono completati prima dell’inizio di altre procedure di salvataggio collegate (es. copia delle macchine virtuali)?		Verificare che l’orario di conclusione del dump sia precedente rispetto ad eventuali operazioni di copia delle macchine virtuali, altrimenti si rischia di fare uno snapshot contenente un dump del database non consistente, con il rischio di non riuscire a ripristinare il database.
Backup offline: viene effettuato almeno un salvataggio dei dati su un supporto separato dal resto della rete informatica dell’organizzazione?		Specificare se disponibile una copia periodica di backup scollegata dal resto della rete, che non sia raggiungibile tramite accesso remoto dalla rete LAN dell’organizzazione, onde evitare che possa venire compromessa da eventuali incursori non autorizzati.
Backup offline: vengono copiati sul supporto offline il full backup e i backup differenziali / incrementali disponibili fino al momento del salvataggio?		Verificare e documentare che il backup offline contenga l’ultimo full backup e i successivi backup differenziali / incrementali, al fine di disporre dei dati per il ripristino e minimizzare l’RPO, cioè la massima quantità di dati che si può perdere a causa di un evento imprevisto.
Ripristino dei dati: vengono effettuati test di ripristino dei dati sottoposti a backup?		Le prove di ripristino sono l’unico riscontro idoneo ad assicurare il corretto funzionamento dei processi di backup, pertanto devono essere previste, effettuate e documentate.
Copie remote: in caso di copia dei dati in ambienti remoti, è effettuata la cifratura dei dati prima del trasferimento delle copie, al fine di impedirne l’esfiltrazione in chiaro?		Le copie remote costituiscono un sistema efficace per garantire la disponibilità dei dati sottoposti a backup, ma un eventuale furto costituirebbe un grave rischio per la riservatezza dei dati. Per tale motivo, le cope remote devono essere sottoposte a cifratura, sia in fase di trasferimento (in transit) che di archiviazione (at rest).
Vengono lette e verificate le email inviate dai processi di backup?		I sistemi automatizzati di backup possono generalmente inviare email in cui è riportato l’esito del processo. E’ fondamentale verificare l’esito riportato nel testo dell’email, per avere la certezza del successo delle operazioni.