Esercitazione 5 Modulo5 - Alessio Russo,

Obiettivo: Verificare la comprensione dei concetti di confidenzialità, integrità e disponibilità dei dati. Scenario: Sei un consulente di sicurezza informatica e un'azienda ti ha assunto per valutare la sicurezza dei suoi sistemi informatici. Durante la tua analisi, ti accorgi che l'azienda ha problemi con la triade CIA. Il tuo compito è identificare e risolvere tali problemi. Fornisci un breve rapporto in cui indichi le aree di miglioramento e le misure suggerite per aumentare la sicurezza dei dati.

Durante l'analisi dei sistemi informatici dell'azienda, sono emersi alcuni problemi relativi alla triade CIA (Confidenzialità, Integrità e Disponibilità) dei dati. Questi problemi potrebbero compromettere la sicurezza complessiva dei dati aziendali e richiedono azioni correttive immediate.

Problemi Identificati:

1. Confidenzialità:
Durante l'ispezione dei sistemi, è stato riscontrato che l'accesso ai dati sensibili non è adeguatamente protetto. Sono state individuate diverse vulnerabilità nel controllo degli accessi e nell'autenticazione degli utenti. Inoltre, alcuni dipendenti hanno mostrato comportamenti non conformi alle politiche di sicurezza, come lasciare le postazioni di lavoro sbloccate quando non sono presenti.

2. Integrità:
Non è stato implementato un meccanismo di controllo dell'integrità dei dati. Ciò significa che non ci sono controlli per garantire che i dati non siano stati modificati in modo non autorizzato.
- Inoltre, non sono stati stabiliti protocolli di backup regolari, mettendo a rischio la perdita di dati critici in caso di incidente.

3. Disponibilità:
Non sono stati implementati meccanismi di ridondanza o di failover per gestire eventuali guasti hardware o software. Non è stata definita una procedura di risposta agli incidenti, il che potrebbe portare a tempi di inattività prolungati in caso di problemi di sicurezza o di emergenze informatiche.

**Misure Suggerite:**

Confidenzialità:
Implementare un sistema robusto di controllo degli accessi basato su ruoli e privilegi, garantendo che solo gli utenti autorizzati possano accedere ai dati sensibili.
Sensibilizzare il personale attraverso la formazione sulla sicurezza informatica per promuovere comportamenti responsabili, come il blocco delle postazioni di lavoro quando non sono in uso.

Integrità:
Introdurre meccanismi di controllo dell'integrità dei dati, come firme digitali o hash crittografici, per garantire che i dati non siano stati alterati in modo non autorizzato.
Stabilire un piano di backup regolare e testato per assicurare la disponibilità dei dati in caso di perdita o danneggiamento.

Disponibilità:
Implementare soluzioni di ridondanza e failover per assicurare la disponibilità continua dei servizi anche in caso di guasti hardware o software. Creare una procedura di risposta agli incidenti dettagliata e testarla regolarmente per garantire tempi di risposta rapidi ed efficaci in caso di emergenze.

Conclusioni:
L'implementazione delle misure suggerite contribuirà significativamente a rafforzare la sicurezza dei dati dell'azienda, migliorando la protezione della confidenzialità, integrità e disponibilità delle informazioni critiche. È fondamentale che queste azioni vengano intraprese senza indugi per mitigare i rischi e proteggere gli interessi dell'azienda.