S3/L3 BCC Iccrea-
Sara Spaccialbelli

Reporting e comunicazione del rischio

Traccia:

Un’azienda ha richiesto la raccolta di informazione per la conduzione di un risk assessment. Lo scenario da valutare è la gestione dei controlli di accesso.

- **Prepara un elenco di persone chiave da intervistare nell'azienda e i potenziali argomenti di discussione per ciascuna di esse:**

1)Responsabile della sicurezza informatica: Discutere dei protocolli attualmente in atto per il controllo degli accessi, delle politiche di sicurezza esistenti e dei rischi identificati.

2)Amministratore di sistema: Esaminare le procedure di gestione degli account utente, i processi di autenticazione e autorizzazione, nonché le eventuali vulnerabilità rilevate nei sistemi informatici.

3)Responsabile del reparto HR: Rivedere le politiche di assunzione e licenziamento per garantire che gli accessi siano revocati in modo tempestivo quando necessario.

4)Responsabile del reparto legale o della conformità normativa: Esaminare le leggi e i regolamenti pertinenti relativi alla gestione degli accessi e garantire la conformità.

5)Utenti chiave dei sistemi informatici: Ottenere feedback sull'esperienza pratica con i controlli di accesso attuali e identificare eventuali lacune o problemi.

- **Identifica i tipi di documentazione che dovresti rivedere per raccogliere informazioni su processi, sistemi e controlli di sicurezza.**

1)Politiche di sicurezza aziendale.

2)Procedure di gestione degli account utente e dei privilegi.

3) Documentazione sui sistemi informatici e reti.

4) Report di audit precedenti e risultati delle valutazioni della sicurezza.

5) Registro degli accessi e delle modifiche ai privilegi degli utenti.

- **Descrivi i test che potresti eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti.**

1) Scansione della vulnerabilità: Utilizzare strumenti di scansione per identificare potenziali punti deboli nei sistemi e nelle reti

.

2) Analisi dei log di accesso: Esaminare i log di accesso per individuare attività sospette o anomalie nei tentativi di accesso.

3) Test di penetrazione: Condurre test di penetrazione etici per identificare vulnerabilità e valutare l'efficacia dei controlli di sicurezza.

4) Analisi delle configurazioni dei dispositivi di rete e dei server: Verificare che le configurazioni siano in linea con le best practice di sicurezza e identificare eventuali errori di configurazione che potrebbero compromettere la sicurezza.

Grazie