S3L3 REPORTING E COMUNICAZIONE DEL RISCHIO

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.

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

- Descrivi i test che potresti eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti. Ricordatevi delle risorse utilizzate nell'esercizio di ieri e del materiale relativo ai controlli.

RISK ASSESSMENT

- Responsabile della sicurezza informatica: Discutere delle politiche e delle procedure di sicurezza attuali, compresi i controlli di accesso.
- Amministratori di sistema: Discutere dei processi di gestione degli account utente, dei privilegi di accesso e delle procedure di revisione.
- Responsabile IT: Discutere dell'architettura della rete e dei sistemi di sicurezza implementati.
- Utenti finali: Per comprendere le sfide pratiche nell'accesso ai sistemi e alle applicazioni.

- **Tipi di documentazione da rivedere**:

- Politiche e procedure di sicurezza: Questi documenti dovrebbero delineare le aspettative dell'organizzazione per la sicurezza delle informazioni.
- Documentazione del sistema: Questo può includere diagrammi di rete, configurazioni di sistema e documentazione di accesso.
- Registri di audit: Questi possono fornire informazioni su chi ha accesso a cosa e quando.
- **Test da eseguire**:

- Revisione dei controlli di accesso: Verificare che solo gli utenti autorizzati abbiano accesso ai sistemi e alle informazioni appropriate.
- Test di penetrazione: Questo può aiutare a identificare le vulnerabilità nella configurazione dei sistemi IT e nella sicurezza delle reti.
- Revisione dei registri di sistema: Questo può rivelare tentativi non autorizzati di accesso o anomalie nei modelli di accesso.

- **Penetration Testing (Pen Test)**

Simulazione di attacchi per identificare vulnerabilità nei controlli di accesso e nei sistemi di sicurezza.

- **Vulnerability Assessment**

Scansioni automatiche per identificare e classificare le vulnerabilità nei sistemi e nelle reti.

- **Security Configuration Review**

Verifica delle configurazioni di sicurezza su sistemi operativi, applicazioni e dispositivi di rete per garantire che seguano le best practice e le politiche aziendali.

- **Access Control Review**

Revisione degli elenchi di controllo degli accessi (ACL) e delle politiche di gestione delle identità per garantire che solo le persone autorizzate abbiano accesso ai sistemi critici.

- **Log Review and Monitoring**

Analisi dei log di accesso e degli eventi di sicurezza per identificare attività sospette o non autorizzate.

- **Network Traffic Analysis**

Monitoraggio e analisi del traffico di rete per rilevare attività anomale o non autorizzate.

- **Phishing Simulation**

Test di simulazione di phishing per valutare la consapevolezza e la reattività dei dipendenti agli attacchi di social engineering.

- **User Access Reviews**

Verifica periodica degli accessi degli utenti per garantire che gli accessi siano appropriati in base ai ruoli e alle responsabilità.