**CONSEGNA 14 MAGGIO S3L3**

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.

**Elenco di Persone Chiave da Intervistare e Potenziali Argomenti di Discussione**

1. **Responsabile IT (CIO/CTO)**
   - Politiche e procedure di gestione degli accessi.
   - Struttura dei permessi e dei ruoli.
   - Tecnologie utilizzate per il controllo degli accessi.
2. **Amministratore di Sistema**
   - Configurazione attuale dei sistemi e delle reti.
   - Metodi di autenticazione e autorizzazione in uso.
   - Processi di provisioning e de-provisioning degli utenti.
3. **Responsabile della Sicurezza Informatica (CISO)**
   - Strategie di sicurezza informatica e piani di risposta agli incidenti.
   - Valutazioni del rischio precedenti e azioni correttive implementate.
   - Formazione e consapevolezza degli utenti in materia di sicurezza.
4. **Responsabile delle Risorse Umane**
   - Processi di onboarding e offboarding del personale.
   - Procedure di verifica dei background dei dipendenti.
   - Politiche di gestione delle credenziali (password policy, MFA).
5. **Responsabile della Compliance**
   - Requisiti normativi e standard di sicurezza applicabili.
   - Audit e ispezioni passate.
   - Documentazione necessaria per la conformità.

6. **Utenti Finali (es. personale di vari reparti)**

    - Esperienza con il sistema di controllo degli accessi.
    - Problemi riscontrati nell'accesso alle risorse aziendali.
    - Suggerimenti per miglioramenti.

**Tipi di Documentazione da Rivedere**

1. **Politiche e Procedure**

    - Policy di sicurezza IT.
    - Procedure di gestione degli accessi.
    - Manuali di configurazione dei sistemi.

2. **Documentazione Tecnica**

    - Diagrammi di rete e architettura dei sistemi.
    - Documentazione dei sistemi di autenticazione e autorizzazione.
    - Log e report di accesso.

3. **Audit e Report di Valutazione**

    - Report di audit interni ed esterni.
    - Valutazioni del rischio precedenti.
    - Report di incidenti di sicurezza.

4. **Documentazione di Compliance**

    - Requisiti normativi e standard di settore (es. GDPR, ISO 27001).
    - Registri di conformità.
    - Report di controllo interno.

5. **Training e Consapevolezza**

    - Materiali di formazione per gli utenti.
    - Report di partecipazione alla formazione.
    - Valutazioni delle competenze degli utenti.

**Test da Eseguire**

1. **Penetration Testing**

    - Simulare attacchi per identificare vulnerabilità nei sistemi di controllo degli accessi.
    - Testare la robustezza delle misure di autenticazione (es. password, MFA).

2. **Vulnerability Assessment**

    - Scansione dei sistemi e delle reti per individuare vulnerabilità note.
    - Verifica delle patch e degli aggiornamenti di sicurezza applicati.

3. **Review delle Configurazioni di Sistema**

    - Analisi delle configurazioni dei server, dei dispositivi di rete e dei sistemi operativi.
    - Verifica delle impostazioni di sicurezza (es. firewall, antivirus).

4. **Log Review e Monitoring**

    - Analisi dei log di accesso per identificare comportamenti anomali.
    - Verifica dell'efficacia dei sistemi di monitoraggio degli accessi.

5. **Test di Controllo degli Accessi Fisici**

    - Verifica dei controlli di accesso fisici agli edifici e ai data center.
    - Simulazione di tentativi di accesso non autorizzato.

6. **Test di Conformità**

    - Verifica della conformità ai requisiti normativi e agli standard di sicurezza.
    - Controllo della documentazione di audit e delle procedure di conformità.