RISK MANAGEMENT

REPORTING E COMUNICAZIONE DEL RISCHIO

MARIA HUAPAYA

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.
• 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 ARGOMENTI DI DISCUSSIONE

Chief Information Officer (CIO)

- Argomenti di discussione:
  - Strategia aziendale e obiettivi IT relativi alla gestione degli accessi.
  - Tecnologie e piattaforme utilizzate per gestire gli accessi.
  - Investimenti pianificati per migliorare i controlli di accesso.

Chief Information Security Officer (CISO)

- Argomenti di discussione:
  - Politiche e procedure di gestione degli accessi.
  - Tecnologie di sicurezza impiegate per controllare gli accessi.
  - Incidenti di sicurezza passati relativi agli accessi e le relative risposte.

Chief Technology Officer (CTO)

- Argomenti di discussione:
  - Architettura IT e infrastruttura utilizzate per gestire gli accessi.
  - Implementazione di tecnologie emergenti per migliorare i controlli di accesso.
  - Integrazione dei controlli di accesso con altre tecnologie aziendali.

Head IT Operations

- Argomenti di discussione:
  - Procedure operative relative alla gestione degli accessi.
  - Monitoraggio e registrazione degli accessi utente.
  - Gestione degli account utente e delle credenziali.

Information Security Manager

- Argomenti di discussione:
  - Implementazione di controlli di accesso basati su ruoli.
  - Rilevamento e risposta agli eventi di sicurezza legati agli accessi.
  - Revisione e aggiornamento delle politiche di accesso.

Business Process Owner

- Argomenti di discussione:
  - Requisiti di accesso associati a processi aziendali specifici.
  - Impatto dei controlli di accesso sui flussi di lavoro aziendali.
  - Protocolli di accesso per i dati e le risorse utilizzati nei processi aziendali.

Privacy Officer

- Argomenti di discussione:
  - Politiche di accesso in conformità con le leggi sulla privacy.
  - Accesso ai dati personali e sensibili.
  - Gestione delle richieste di accesso ai dati personali da parte degli interessati.

Legal Counsel

- Argomenti di discussione:
  - Rischi legali associati alla gestione degli accessi.
  - Conformità alle leggi e ai regolamenti in materia di sicurezza informatica e privacy.
  - Contratti e accordi relativi alla gestione degli accessi con terze parti.

Compliance Officer

- Argomenti di discussione:
  - Conformità alle normative settoriali e agli standard di sicurezza.
  - Monitoraggio della conformità ai requisiti di accesso.
  - Risultati degli audit di conformità relativi agli accessi.

Internal Auditor

- Argomenti di discussione:
  - Esame dell'efficacia dei controlli di accesso esistenti.
  - Identificazione di potenziali lacune nei controlli di accesso.
  - Raccomandazioni per migliorare la sicurezza degli accessi in base alle migliori pratiche e agli standard di settore.

DOCUMENTAZIONE DA RIVEDERE

Politiche e Procedure di Sicurezza:

- Politica sui controlli di accesso.
- Gestione delle identità e degli accessi (IAM).
- Password e autenticazione.
- Autorizzazioni e privilegi.
- Monitoraggio e registrazione degli accessi.

Documentazione Tecnica:

- Diagrammi di architettura IT.
- Configurazioni dei sistemi di controllo degli accessi.
- Manuali utente e guide di amministrazione.
- Procedure di patching e aggiornamento del software.

Registri e Report di Sicurezza:

- Log degli accessi ai sistemi.
- Report sugli incidenti di sicurezza.
- Valutazioni del rischio e audit di sicurezza.

TEST DA ESEGUIRE

Scansioni di Vulnerabilità:

- Identificare potenziali vulnerabilità nei sistemi IT e nelle configurazioni di rete.

Pentesting:

- Simulare attacchi informatici per valutare l'efficacia dei controlli di accesso.

Analisi dei Log:

- Esaminare i log degli accessi per identificare attività sospette o anomale.

Interviste e Sondaggi agli Utenti:

- Raccogliere feedback e informazioni sulle esperienze degli utenti con i controlli di accesso.

Test di Conformità:

- Verificare se il sistema informatico è conforme a determinati standard o normative di sicurezza.

Test di Consapevolezza sulla Sicurezza Informatica:

- Valutare il livello di conoscenza degli utenti in materia di sicurezza informatica e le loro capacità di riconoscere e contrastare le minacce online.

RISORSE UTILIZZATE

NIST SP 800-53: Raccomandazioni per la gestione dei controlli di accesso.

ISO/IEC 27002: Codice di buone pratiche per la sicurezza delle informazioni.

ENISA: Guida alle migliori pratiche per la gestione dei controlli di accesso.

GRAZIE

MARIA HUAPAYA