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.

INTERVISTE

- CISO
- Amministratore di sistema
- Responsabile sicurezza informatica
- Resonsabile Risorse umane
- Responsabile Finanziario
- Responsabile Marketing
- Responsabile sicurezza fisica

Argomenti

- CISO
  - Politiche di sicurezza informatica e standard adottati
  - Processi di gestione degli accessi
  - Strategie di risposta agli incidenti di sicurezza
  - Piani di formazione e consapevolezza sulla sicurezza

- Amministratore di sistema
  - Configurazione e gestione dei sistemi IT
  - Procedure di controllo degli accessi a livello di sistema e rete
  - Pratiche di gestione delle password e autenticazione multifattoriale (MFA)
  - Monitoraggio e registrazione delle attività degli utenti
  - Procedure di aggiornamento e patching dei sistemi

- Responsabile sicurezza informatica
  - Implementazione dei controlli di sicurezza tecnici
  - Monitoraggio delle minacce e gestione delle vulnerabilità
  - Incident response e gestione delle crisi
  - Piani di continuità operativa e disaster recovery

- Responsabile Risorse umane
  - Processi di onboarding e offboarding dei dipendenti
  - Controlli di background check e verifica delle credenziali
  - Accessi temporanei e gestione dei contratti di consulenza
  - Procedure di segnalazione e risoluzione delle violazioni di sicurezza

- Responsabile Finanziario
  - Budget per la sicurezza informatica
  - Controlli di accesso ai sistemi finanziari
  - Gestione dei rischi finanziari legati alla sicurezza informatica
  - Conformità alle normative finanziarie

- Responsabile Marketing
  - Accesso ai dati sensibili dei clienti
  - Controlli di accesso alle piattaforme di marketing e CRM
  - Protezione dei dati personali nei processi di marketing
  - Consapevolezza e formazione sulla sicurezza informatica per il personale di marketing

- Responsabile sicurezza fisica
  - Controlli di accesso fisico agli edifici e ai data center
  - Integrazione della sicurezza fisica con la sicurezza informatica
  - Monitoraggio e registrazione degli accessi fisici
  - Procedure di emergenza e risposta agli incidenti fisici

Documentazione da Rivedere

- Politiche e Procedure
  - Politiche di sicurezza informatica
  - Procedure di gestione degli accessi
  - Politiche di gestione delle password
- Diagrammi di Rete e Configurazioni
  - Diagrammi di rete aggiornati
  - Configurazioni dei firewall e delle VPN
  - Configurazioni dei server e delle workstation
- Registri di Accesso e Log
  - Log di accesso degli utenti
  - Registri di modifiche alle autorizzazioni
  - Log di eventi di sicurezza
- Report di Audit e Valutazioni Precedenti
  - Risultati degli audit interni ed esterni
  - Report di valutazioni di sicurezza precedenti
  - Piani di miglioramento e azioni correttive

- Documentazione di Conformità
  - Documentazione relativa al rispetto delle normative (GDPR, ISO 27001)
  - Certificazioni di conformità
  - Report di valutazione del rischio

Test

- Vulnerability Assessment e Penetration Testing:
  - **Obiettivo**: Identificare e valutare le vulnerabilità nei sistemi e nella rete
  - **Dettagli**: Utilizzare strumenti di scansione delle vulnerabilità per identificare punti deboli e condurre test di penetrazione per valutare l'efficacia delle difese

- Analisi del traffico di rete:
  - **Obiettivo**: Identificare traffico di rete anomalo
  - **Dettagli**: Utilizzare strumenti di monitoraggio della rete per identificare potenziali minacce

- Revisionare codice sorgente:
  - **Obiettivo**: Identificare bug nel codice
  - **Dettagli**: Utilizzare strumenti di testing del codice per identificare in maniera efficace eventuali problemi nella logica dell’intero sistema