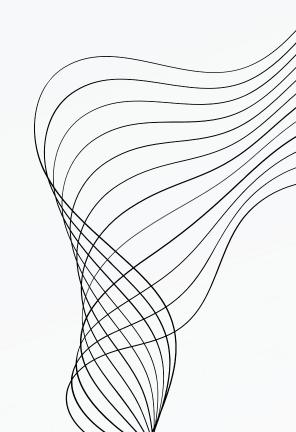


PRATICA S3-L3 REPORTING E COMUNICAZIONE DEL RISCHIO

MARIA FLAVIA MINOTTI LISA BONATO ALEX FIORILLO

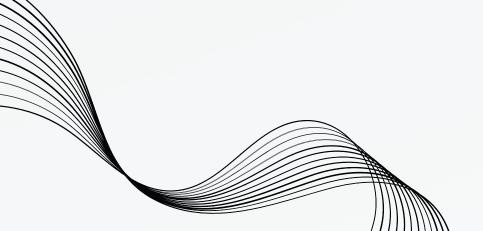


TRACCIA

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.



INTERVISTA:

Al fine della raccolta informazioni per la conduzione del risk assessment relativo alla gestione dei controlli di accesso, si procede a dettare l'elenco del personale chiave dell'azienda da intervistare. Per ciascuna delle figure individuate si elencano gli argomenti di discussione.

- Chief Information Officer (CIO): offre una visione strategica sull'infrastruttura IT dell'azienda e dettagli sulla strategia complessiva di gestione degli accessi e sulle tecnologie utilizzate per implementarla.
- Chief Information Security Officer (CISO): È responsabile della sicurezza informatica dell'azienda e può fornire informazioni dettagliate sulle politiche, i controlli e le procedure relativi alla gestione degli accessi.
- Chief Technology Officer (CTO): Può offrire una prospettiva tecnica sull'architettura IT dell'azienda e sulle tecnologie impiegate per gestire gli accessi agli asset aziendali.
- Head IT Operations: è responsabile delle operazioni quotidiane dei sistemi IT e può fornire informazioni sulle procedure operative relative alla gestione degli accessi e sul monitoraggio degli accessi utente.
- Information Security Manager: Collabora con il CISO nella gestione della sicurezza informatica e può fornire dettagli sulla implementazione dei controlli di accesso e sul monitoraggio degli eventi di sicurezza.
- Business Process Owner: Può fornire una prospettiva sui requisiti di accesso relativi ai processi aziendali e sulle politiche di controllo degli accessi implementate per garantire la sicurezza delle informazioni.
- Privacy Officer: È responsabile della protezione dei dati personali e può fornire informazioni sulle politiche e le procedure relative alla gestione degli accessi per garantire la conformità alle normative sulla privacy.
- Legal Counsel: Offre consulenza legale sulla protezione dei dati e della privacy e può fornire informazioni sulle implicazioni legali dei controlli di accesso e sulle responsabilità legali dell'azienda in caso di violazioni della sicurezza.
- Compliance: Collabora con il CISO e il Legal Counsel per garantire che gli accessi siano gestiti in conformità con le normative e gli standard di settore.
- Audit: Può esaminare l'efficacia dei controlli di accesso esistenti attraverso processi di audit e revisione e fornire raccomandazioni per migliorare la sicurezza degli accessi

INTERVISTA: ARGOMENTI PER CIASCUNA FIGURA INDIVIDUATA

Chief Information Officer (CIO):

- 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):

- 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):

- 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:

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

Information Security Manager:

- 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.

INTERVISTA: ARGOMENTI PER CIASCUNA FIGURA INDIVIDUATA

Business Process Owner:

- 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:

- 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:

- 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:

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

Audit:

- 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

Documentazione da rivedere:

• Politiche e procedure di sicurezza:

- o 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
- o Configurazioni dei sistemi di controllo degli accessi
- o Manuali utente e guide di amministrazione
- o Procedure di patching e aggiornamento del software

• Registri e report di sicurezza:

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

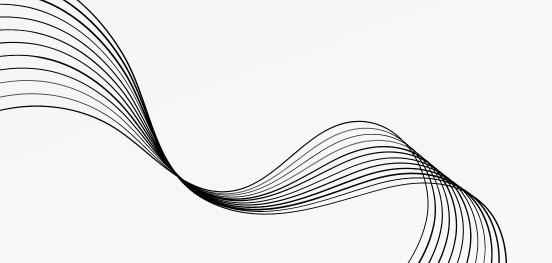
TESTING

Test per la Raccolta Dati:

- 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 UTILI

- 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 dell'attenzione!

Alex Fiorillo Maria Flavia Minotti Lisa Bonato