Misurazione dell'efficacia dei controlli

Traccia

Scenario di rischio:

Le configurazione dei dispositivi di sicurezza di rete (FW, IDS, IPS, …) è modificata o manipolata intenzionalmente. Utenti autorizzati con accesso alle informazioni intenzionalmente modificano la configurazione degli asset, per intaccare malevolmente la confidenzialità, l'integrità e la disponibilità dei servizi.

- **Threat actor**: Insider malintenzionati
- **Intento/motivazione**: Gli utenti autorizzati con accesso alle risorse informative compromettono intenzionalmente la riservatezza, l'integrità o la disponibilità dei sistemi, causando un incidente di sicurezza.
- **Threat event**: un incidente di sicurezza è causato dalle azioni dell'insider.
- **Asset/Risorse**: tutti i sistemi IT
- **Conseguenze**: incidenti di sicurezza, data disclosure, tampering, disservizi.
    - **Produttività**: L'indisponibilità del sistema o la mancanza di integrità dei dati possono influire sulla produttività dell'intera organizzazione.
    - **Costo della risposta**: Tempo/effort per identificare le cause ed effettuare il recover da un incidente.
    - **Vantaggio competitivo**: Se gli eventi sono sufficientemente gravi e pubblici, l'organizzazione può perdere clienti.
    - **Reputazione**: Se gli eventi sono sufficientemente gravi e di pubblico dominio, la reputazione dell'organizzazione può subire un impatto negativo a causa della mancata disponibilità e dei ritardi.
    - **Sanzioni**: Se gli eventi sono sufficientemente gravi e di pubblico dominio, è possibile che l'organizzazione si esponga a sanzioni per mancanza di conformità normative e legali.
- **Tempistiche**: La durata dell'incidente può essere molto breve o prolungata, a seconda dell'ambito lavorativo e della sovrapposizione delle mansioni. L'individuazione precoce e l'azione correttiva sono fondamentali per limitare la portata e la natura di questo scenario di rischio.
- **Estensione dello scenario**:
    - **Caso peggiore**: Gli incidenti di sicurezza e di interruzione possono causare interruzioni di massa, data breach, perdita di vantaggio competitivo, multe e sentenze. Il personale viene licenziato, il morale è basso e i costi di risanamento aumentano nel tempo.
    - **Caso tipico o più probabile**: La portata e le dimensioni degli incidenti e delle interruzioni sono limitate e vengono affrontate senza danni duraturi per l'organizzazione.
    - **Caso migliore**: Sono interessate solo funzionalità limitate dei sistemi, vengono ripristinate rapidamente e vengono immediatamente intraprese azioni correttive da parte dei dipendenti.

- **Assunzioni**:
    - I dati e i sistemi sono efficacemente sottoposti a backup e disponibili per un ripristino immediato.
    - Le procedure operative standard e il processo di gestione delle modifiche sono in atto.
    - È disponibile la documentazione relativa a politiche e procedure.
    - Esistono procedure di test e rilascio del software.
    - Il piano e la procedura di disaster recovery sono in atto e aggiornati.

Definire gli indicatori di rischio chiave (KRI) per lo scenario di rischio proposto, seguendo la tabella:

ID	Nome	Descrizione	Metrica	Tipo
KRI-1	Tentativi di modifica non autorizzata delle configurazioni	Monitora il numero di tentativi di modifica non autorizzata delle configurazioni di sicurezza	Numero di tentativi di modifica non autorizzata rilevati	Lead
KRI-2	Accessi non autorizzati ai dispositivi di sicurezza	Monitora il numero di accessi non autorizzati ai dispositivi di sicurezza	Numero di accessi non autorizzati rilevati	Lag
KRI-3	Variazioni significative nelle configurazioni di sicurezza	Monitora la frequenza e l'entità delle variazioni nelle configurazioni di sicurezza	Numero e gravità delle variazioni nelle configurazioni	Lag
KRI-4	Anomalie nell'utilizzo dei privilegi di accesso	Monitora i comportamenti anomali relativi all'uso dei privilegi di accesso	Numero e tipo di anomalie rilevate nell'uso dei privilegi	Lead
KRI-5	Aumento delle attività di accesso in orari non tipici	Monitora l'aumento delle attività di accesso ai sistemi durante orari non tipici	Numero di attività di accesso durante orari non tipici	Lag