PRATICA S3/L4

MISURAZIONE DELL'EFFICACIA DEI CONTROLLI

BONATO LISA

FIORILLO ALEX

MINOTTI MARIA FLAVIA

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	Deviazioni dai processi standard di gestione delle modifiche	Monitoria il numero di deviazioni dai processi standard di gestione delle modifiche per le configurazioni di sicurezza	Numero di deviazioni dai processi standard	Lead
KRI-3	Mancanza di approvazioni per le modifiche alle configurazioni di sicurezza	Monitora il numero di modifiche alle configurazioni di sicurezza effettuate senza le necessarie approvazioni	Numero di modifiche senza approvazioni	Lag
KRI-4	Tentativi di accesso non autorizzato	Monitora il numero di tentativi di accesso non autorizzato a tutti i sistemi del”organizzazione	Rilevati tentativi di accesso non autorizzato	Lead

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

ID	Nome	Descrizione	Metrica	Tipo
KRI-5	Diffusione di malware tramite abuso di privilegi	Monitora utilizzo di privilegi per installare software dannoso	Rilevata diffusione di malware	Lead
KRI-6	Attività di trasferimento dati anomala	Monitorare i trasferimenti di dati per individuare flussi di dati anomali o volumi di dati insolitamente elevati	Tentativo di manipolazione anomala dei dati rilevata	Lead

Gli indicatori di rischio chiave **(KRI)** sono metriche utilizzate per determinare se e quando l'organizzazione ha un'alta probabilità di incorrere in rischi che superano la soglia di rischio definita.

I KRI riguardano quanto la metrica prevede i rischi attuali e futuri. KRI è utile per identificare punti deboli o aree di potenziale fallimento dei controlli.

I KRI sono connessi a rischi specifici e forniscono un preavviso che un rischio sta emergendo, permettendo alla leadership di essere proattiva e affrontarlo tempestivamente.

I KRI vengono monitorati regolarmente e i loro valori vengono analizzati per identificare eventuali trend o anomalie. Se un KRI supera una certa soglia predefinita, questo è un segnale che il rischio associato sta crescendo e che è necessario intervenire.

I KRI dovrebbero essere SMART e basarsi sull’analisi della causa principale (RCA) per la determinazione del vero fattore/causa di rischio, non solo sui sintomi evidenti.

Lag risk indicator: metrica retrospettiva che indica che il rischio si concretizza dopo che si è verificato un evento.
Lead risk indicator: metrica previsionale che fornisce un'indicazione del rischio che potrebbe concretizzarsi prima che si verifichi un evento.