S3L4 MISURAZIONE DELL‘ EFFICACIA DEI CONTROLLI

Scenario di rischio: Risk Management Esercizio 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

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

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	Numero di modifiche di configurazione riuscite	Monitora il numero di modifiche di configurazione che sono state effettivamente eseguite, autorizzate e non	Numero di modifiche eseguite	Lag
KRI-3	Incidenti di sicurezza causati da insider	Monitora il numero di incidenti di sicurezza attribuiti ad azioni	Numero di incidenti di sicurezza causati da insider	Lag

KRI-4	Tempo medio di rilevamento delle modifiche non autorizzate	Monitora il tempo medio impiegato per rilevare modifiche non autorizzate alle configurazioni	Tempo medio (in ore)	Lead
KRI-5	Numero di alert di sicurezza generati da IDS/IPS	Monitora il numero di alert di sicurezza generati da sistemi IDS/IPS relativi a tentativi di modifica non autorizzata	Numero di alert generati	Lead
KRI-6	Accessi sospetti ai sistemi di configurazione	Monitora il numero di accessi sospetti ai sistemi che gestiscono le configurazioni di sicurezza	Numero di accessi sospetti rilevati	Lead

KRI-7	Percentuale di configurazioni ripristinate dai backup	Monitora la percentuale di configurazioni di sicurezza che sono state ripristinate dai backup a seguito di modifiche non autorizzate	Percentuale di configurazioni ripristinate	Lag
KRI-8	Compliance alle procedure di gestione delle modifiche	Monitora il grado di aderenza alle procedure standard di gestione delle modifiche	Percentuale di aderenza	Lead
KRI-9	Tempo di risposta agli incidenti di sicurezza	Monitora il tempo medio impiegato per rispondere e mitigare gli incidenti di sicurezza	Tempo medio di risposta (in ore)	Lag
KRI-10	Livello di formazione e consapevolezza del personale	Monitora il livello di formazione e consapevolezza del personale	Percentuale di completamento delle sessioni di formazione	Lead

- KRI-1 (Lead): Monitorando il numero di tentativi di modifica non autorizzata, si può identificare proattivamente attività sospette prima che causino danni significativi.
- KRI-2 (Lag): Questo KRI aiuta a misurare l'efficacia delle misure di sicurezza e la frequenza delle modifiche non autorizzate.
- KRI-3 (Lag): Rilevando il numero di incidenti causati da insider, si può valutare la gravità del rischio interno.
- KRI-4 (Lead): Un tempo di rilevamento rapido è essenziale per limitare il danno potenziale delle modifiche non autorizzate.
- KRI-5 (Lead): Gli alert di IDS/IPS forniscono un primo livello di difesa contro tentativi di modifica non autorizzata.
- KRI-6 (Lead): Monitorare gli accessi sospetti ai sistemi di configurazione aiuta a identificare possibili insider malevoli.
- KRI-7 (Lag): La capacità di ripristinare configurazioni dai backup è cruciale per il recupero rapido da modifiche non autorizzate.
- KRI-8 (Lead): La compliance alle procedure di gestione delle modifiche garantisce che tutte le modifiche siano tracciate e autorizzate.
- KRI-9 (Lag): Il tempo di risposta agli incidenti indica l'efficacia del team di sicurezza nel mitigare i rischi.
- KRI-10 (Lead): Un personale ben formato e consapevole delle politiche di sicurezza riduce il rischio di modifiche non autorizzate.