EPICODE

S3 - L4

Misurazione dell'efficacia dei controlli

15 maggio 2024

Team

- Davide Di Turo
- Manuel Di Gangi
- Marco Fasani

INDICE

Traccia

Scenario di rischio: Risk Management

Esercizio:

La 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 recovery 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:

Key Risk Indicator

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	Tentativi di accesso non autorizzato ai dati sensibili	Monitora il numero di tentativi di accesso non autorizzato ai dati sensibili	Numero di tentativi di accesso non autorizzato rilevati	Lead
KRI-3	Tempo medio di rilevamento e risposta agli incidenti	Misura il tempo medio necessario per rilevare e rispondere agli incidenti di sicurezza	Tempo medio (in ore)	Lag
KRI-4	Percentuale di successo degli incidenti di sicurezza	Misura la percentuale di incidenti di sicurezza causati da insider malintenzionati che hanno avuto successo	Percentuale di incidenti di sicurezza con successo rispetto al totale	Lag
KRI-5	Tentativo di esfiltrazione dei dati	Misura la quantità di dati in uscita dalla rete aziendale che l'insider interno trasmette verso l'esterno	Quantità di traffico in uscita	Lead
KRI-6	Frequenza di aggiornamento delle politiche di sicurezza	Monitora la frequenza con cui le politiche di sicurezza vengono aggiornate e revisionate	Numero di aggiornamenti delle politiche di sicurezza nell'arco di un periodo temporale	Lead
KRI-7	Capacità di recovery post-incidente	Valuta l'efficacia e la tempestività del processo di recovery dopo un incidente di sicurezza	Tempo medio necessario per ripristinare i servizi critici dopo un incidente (in ore)	Lag
KRI-8	Capacità di recovery post-incidente	Valuta l'efficacia e la tempestività del processo di recovery dopo un incidente di sicurezza	Tempo medio necessario per ripristinare i servizi critici dopo un incidente (in ore)	Lag
KRI-9	Percentuale di asset critici protetti	Monitora la percentuale di asset critici che sono adeguatamente protetti da configurazioni non autorizzate	Percentuale di asset critici con configurazioni autorizzate rispetto al totale	Lead