BCC Iccrea - S3/L4
Sara Spaccialbelli

MISURAZIONE DELL'EFFICACIA DEI CONTROLLI

Traccia:

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 normativa e legale.

Traccia:

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	Lag
KRI-2	Variazioni nelle autorizzazioni degli utenti	Monitora le modifiche nelle autorizzazioni degli utenti, specialmente quelle con privilegi elevati, relative ai dispositivi	Numero di variazioni nelle autorizzazioni degli utenti rilevate	Lag
KRI-3	Accessi anomali ai dispositivi di sicurezza	Monitora gli accessi anomali ai dispositivi di sicurezza, come tentativi di accesso non autorizzati o comportamenti insoliti da parte degli utenti autorizzati.	Numero di accessi anomali ai dispositivi di sicurezza rilevati	Lag
KRI-4	Variazioni nei log di controllo	Monitora le variazioni nei log di controllo dei dispositivi di sicurezza, specialmente riguardanti operazioni di modifica delle configurazioni o accessi anomali.	Numero di variazioni nei log di controllo rilevate	Lag

ID	Nome	Descrizione	Metrica	Tipo
KRI-5	Tempo medio per identificare e rispondere a incidenti di sicurezza legati a modifiche non autorizzate	Misura il tempo medio necessario per identificare e rispondere a incidenti di sicurezza legati a modifiche non autorizzate delle configurazioni di sicurezza.	Tempo medio per identificare e rispondere a incidenti di sicurezza	Lead
KRI-6	Accesso ai dati sensibili	Monitora gli accessi ai dati sensibili da parte degli utenti, specialmente quelli che potrebbero indicare un'attività malevola da parte di insider malintenzionati.	Numero di accessi ai dati sensibili rilevati	Lag
KRI-7	Utilizzo anomalo delle credenziali degli utenti	Monitora l'utilizzo anomalo delle credenziali degli utenti, come accessi a orari insoliti o da posizioni geografiche	Numero di utilizzi anomali delle credenziali rilevati	Lag
KRI-8	Tempo medio di risposta agli incidenti di sicurezza	Misura il tempo medio necessario per rispondere agli incidenti di sicurezza legati a insider malintenzionati.	Tempo medio per rispondere agli incidenti di sicurezza	Lead

GRAZIE

Sara Spaccialbelli