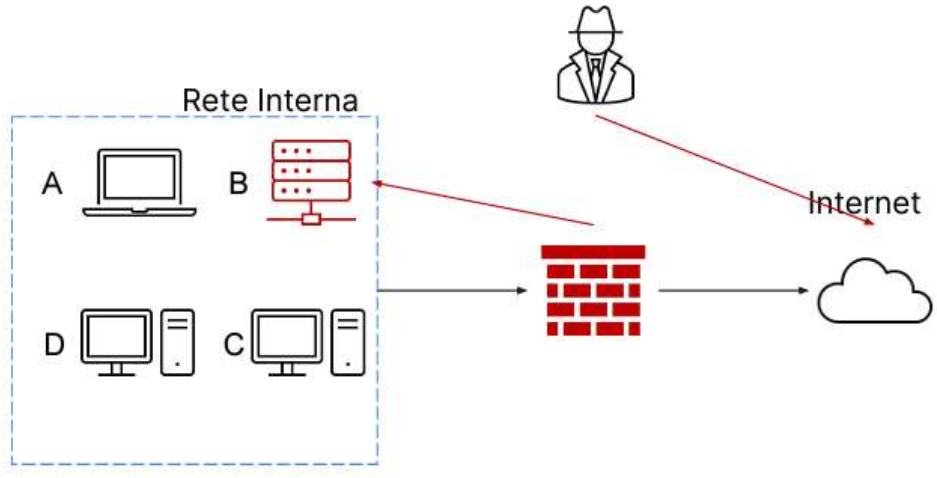
Esercizio Incident Response

Traccia



Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti:

- Mostrate le tecniche di:

    1. Isolamento
    2. Rimozione del sistema B infetto

- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear

Svolgimento

Nello scenario proposto, ci troviamo nella fase di Contenimento, Eliminazione e Recupero di un Incident Response, questa fase viene avviata dopo lo studio ed analisi di una minaccia rilevata e nel nostro caso appunto siamo riusciti a risalire ai sistemi compromessi e il vettore di attacco. La fase di Contenimento, Eliminazione e Recupero ha lo scopo principale di:

- Ridurre gli impatti causati dall'incidente
- Eliminazione dell'incidente dalla rete e dai sistemi
- Recupero dei servizi e delle operatività

Riduzione impatti causati dall'incidente

La fase di riduzione degli impatti consiste in un contenimento del danno cercando di isolare l'incidente in modo che non crei ulteriori danni alla rete o ai sistemi. Esistono svariate tecniche preventive e strategiche per la gestione degli incidenti di sicurezza tra cui:

- Isolamento
- Rimozione

Isolamento

Consiste ad isolare il sistema infetto, attraverso una completa disconnessione dalla rete, tutelandoci dai movimenti laterali, ma fornendo ancora l'accesso ad internet in modo da poter continuare le analisi sul sistema infetto, cercando di condurre un'analisi comportamentale, grazie alla quale potremmo identificare altre vulnerabilità o vettori d'attacco.

Rimozione

Consiste in un isolamento stringente con una totale rimozione del sistema infetto dalla rete interna e da Internet, eliminando ogni possibilità di accesso da parte dell'attaccante.

Clear Purge Destroy

Clear, Purge e Destroy sono tecniche di smaltimento o riutilizzo di un disco o di un sistema di storage utilizzate in fase di recupero.

- **Clear:** Il dispositivo viene completamente ripulito dal suo contenuto con tecniche "logiche". Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di "factory reset" per riportare il dispositivo nello stato iniziale.

- **Purge:** Si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi

- **Destroy:** È l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.