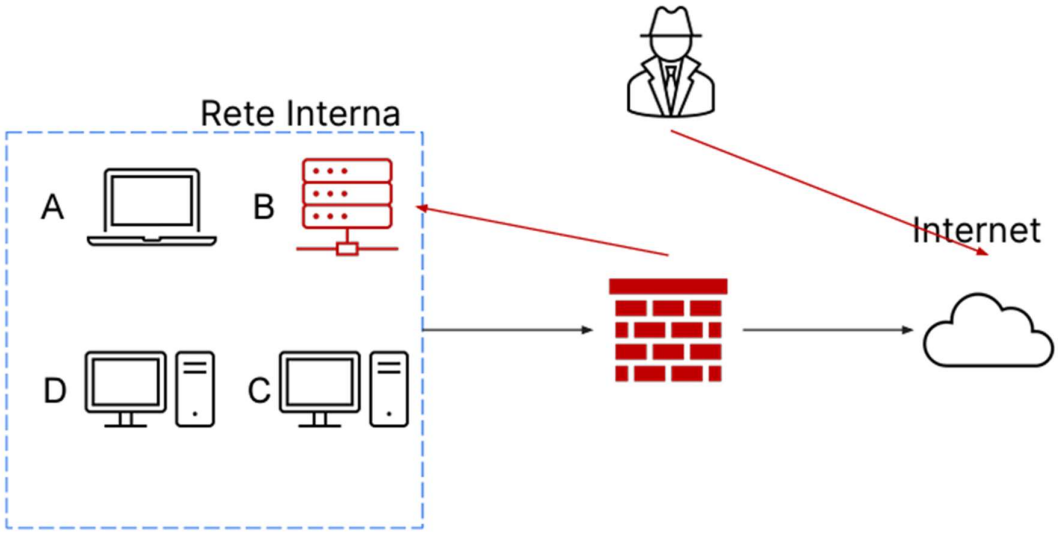
ESERCIZIO S9-L4

Nell'esercizio di oggi andremo a simulare un componente del team CSIRT. Con riferimento alla figura sotto dobbiamo rispondere ai seguenti quesiti:

- Mostrare le tecniche di isolamento e rimozione del sistema B infetto.
- Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



Il team CSIRT si occupa di monitorare e rispondere agli incidenti. E' simile al SOC livello 2, però quest'ultimo è un'organizzazione privata a differenza del team CSIRT che è molto più importante in quanto nel suo team ci sono figure a livello governativo.

Per contenere il danno causato dall'incidente di sicurezza per quanto riguarda la figura sopra, la prima cosa da fare è quello di isolare l'incidente in modo che non causi danni ad altri sistemi. Per isolare il sistema B si deve sconnettere completamente dalla rete per diminuire maggiormente l'accesso alla rete interna da parte dell'attaccante. Questa tecnica però a volte non è sufficiente e quindi si ricorre alla completa rimozione del sistema dalla rete sia interna sia internet, in questo modo l'attaccante non avrà accesso né al sistema infettato né alla rete interna.

Per la fase di recupero, prima di procedere allo smaltimento dei dischi compromessi si individuano delle opzioni per la gestione delle informazioni. Due di queste opzioni sono Purge e Destroy.

- Per la prima tecnica si utilizza una rimozione fisica come l'utilizzo di magneti per rendere le informazioni inaccessibili sui dispositivi.
- La seconda tecnica invece riguarda proprio la disintegrazione dei media ad alte temperature.

Durante questa fase di recupero si deve ristabilire la normale attività delle applicazioni.