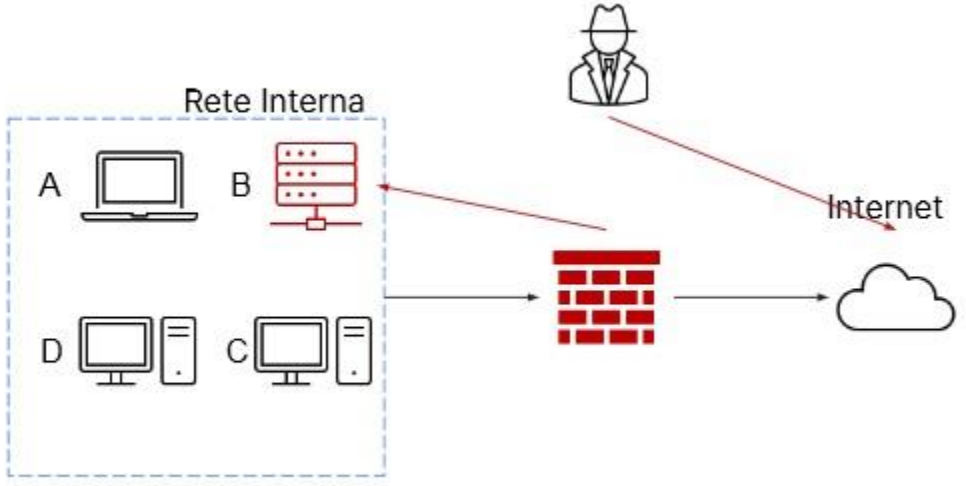
# Incident response

Il sistema B (database con diversi dischi per lo storage) è stato interamente compromesso da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

-Tecniche di: isolamento, rimozione sistema B infetto
Differenza tra: Clear, Purge, Destroy




Orlando Tangari

*Isolamento*: attività di contenimento che ha lo scopo primario di isolare l'incidente, in modo tale da non creare ulteriori danni alla rete interna. Consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante, in modo tale da poter raccogliere informazioni su di esso.

*Rimozione*: tecnica di contenimento più restringente, che ha lo scopo di rimuovere completamente il sistema infetto sia dalla rete interna che da internet, in modo tale che l'attaccante non avrà ne accesso alla rete interna, ne alla macchina infettata.

# Incident response

Tecniche di isolamento e rimozione del sistema B infetto

*Clear*: opzione per ripulire il dispositivo con tecniche logiche come read e write, sovrascrivendo il suo contenuto più volte o utilizzando la funzione di factory reset, per riportare il dispositivo allo stato iniziale.

P*urge*: opzione di rimozione fisica dei contenuti sensibili con tecniche come l'utilizzo di forti magneti, per rendere le informazioni inaccessibili su determinati dispositivi, oltre all'adozione di tecniche logiche.

*Destroy*: opzione più netta per lo smaltimento di dispositivi contenenti dati sensibili. Oltre a tecniche logiche e fisiche, si utilizzano tecniche di laboratorio come: disintegrazione, polverizzazione dei media ad alte temperature. Metodo più efficace per rendere le informazioni inaccessibili ma dai maggiori costi economici.

# Incident response

Differenza tra: *clear*, *purge*, *destroy*