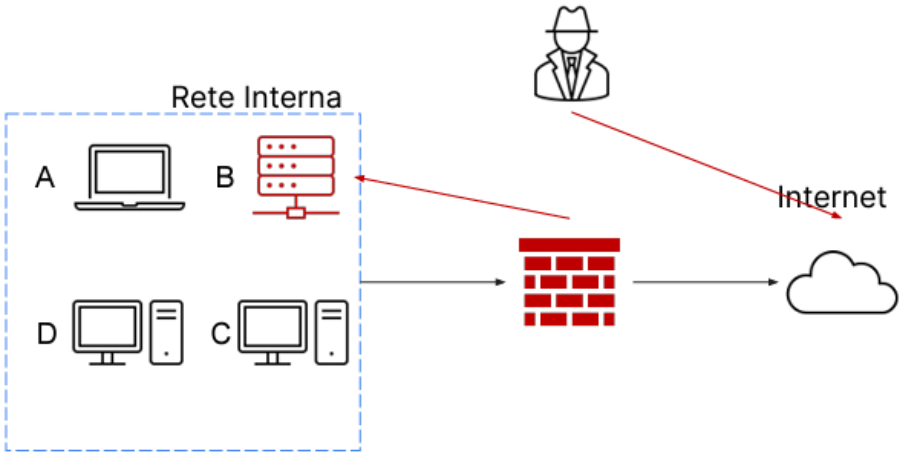

Il team CSIRT svolge le seguenti procedure:

Fase di isolamento
Si tratta di una fase dove il team cerca di, come dice lo stesso nome, di isolare l'attacco. In questa fase, si è proceduto a staccare il sistema dalla rete interna in un area separata così che possa essere analizzato .

Fase di rimozione
L'hacker come si vede in figura ha accesso a internet, quindi si è proceduto ad una disconnessione del sistema anche dalla rete. In questa fase si esegue anche un backup dei dati e si analizza il tipo di malware che ha infettato il sistema. Infine, bisogna eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi, come rimuovere eventuali backdoor, ripulire dischi e chiavette USB compromesse.

Formattazione
Purge: sovrascrizione i dati sui dischi tramite dei magneti

Clear: sovrascrizione dati tramite factory reset

Destory: si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione.