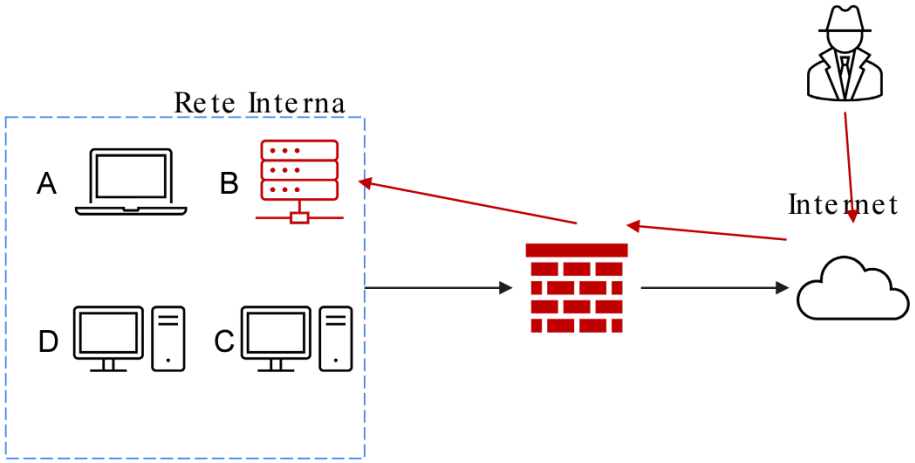
**Traccia:**

Con riferimento alla figura in slide, 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: I) Isolamento II) 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




*Isolamento:*
consiste nella completa disconnessione del database infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.

*Rimozione del sistema B infetto:*
In questo caso procediamo con la completa rimozione del sistema dalla rete sia interna sia internet.

*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 utilizzala funzione di «factoryreset» per riportare il dispositivo allo stato iniziale;

*Purge:*
Oltre un approccio logico per la rimozione dei contenuti sensibili,come visto nel caso di clear, si usano anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;

*Destroy:*
Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione, etc.