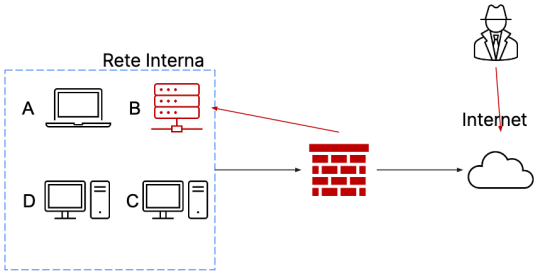
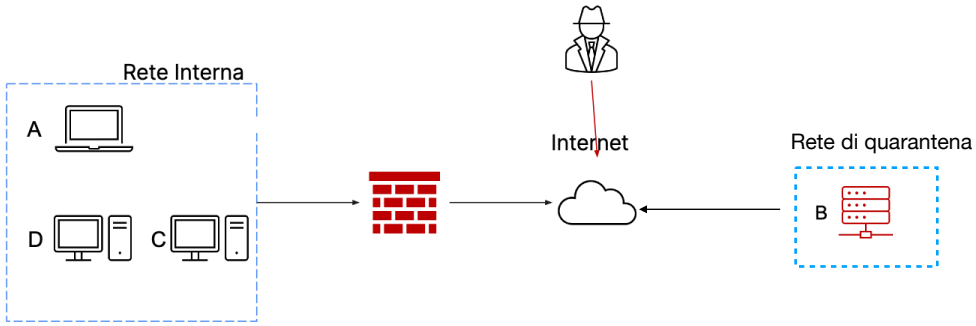
4. Le politiche e procedure di risposta agli incidenti di sicurezza

Con riferimento alla figura seguente, **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.



Mostrare le tecniche di:

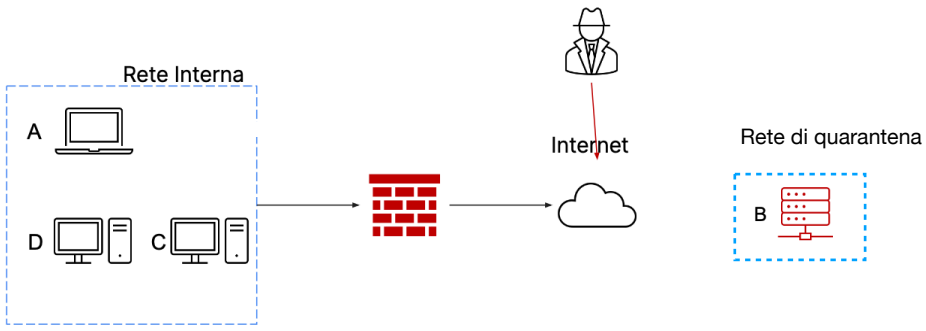
Isolamento



A differenze della semplice segmentazione creando una separazione del sistema B dagli altri computer sulla rete, **l'isolamento** è considerato un contenimento maggiore, che consiste in una completa disconnessione del sistema infetto dalla rete, in tal modo da limitare maggiormente un possibile accesso alla rete interna dell'attaccante.

Rimozione

Qualora l'isolamento non fosse sufficiente, si utilizza un attiva ancora più restrittiva, ovvero la completa rimozione del sistema sia dalla rete interna che da internet, impedendo all'attaccante l'accesso sia alla rete interna che alla macchina infetta.



Spiegazione delle differenze tra Clear, Purge e Destroy

Tre opzioni per la gestione dei media contenenti informazioni sensibili:

CLEAR
Si utilizzano tecniche logiche per ripulire completamente il dispositivo.
Un esempio può essere la sovrascrittura del contenuto svariate volte per riuscire a riportare il dispositivo allo stato iniziale.

PURGE
Oltre alla rimozione dei contenuti sensibili visti con Clear, si utilizzano anche tecniche fisiche come per esempio dei forti magneti che rendono inaccessibili le informazioni su determinati dispositivi.

DESTROY
In questa fase, l'approccio è più netto, utilizzando tecniche di laboratorio come polverizzazione ad alte temperature, disintegrazione e trapanazione dei dispositivi contenenti dati sensibili. Questo metodo richiede un costo maggiore da sostenere per l'azienda, nonostante sia anche il più efficace