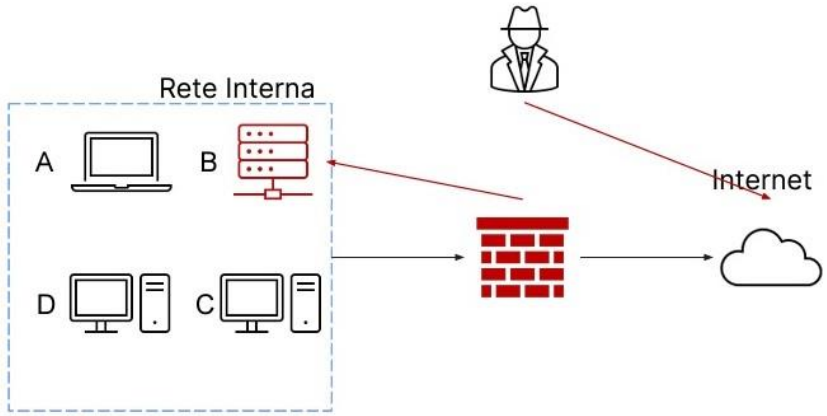
S9/L4 Esercizio 23/11/2023

Nell'esercizio odierno ci viene richiesto di mostrare le tecniche di isolamento e rimozione di un sistema infetto durante un attacco e spiegare la differenza tra Purge e Destroy

Situazione di attacco

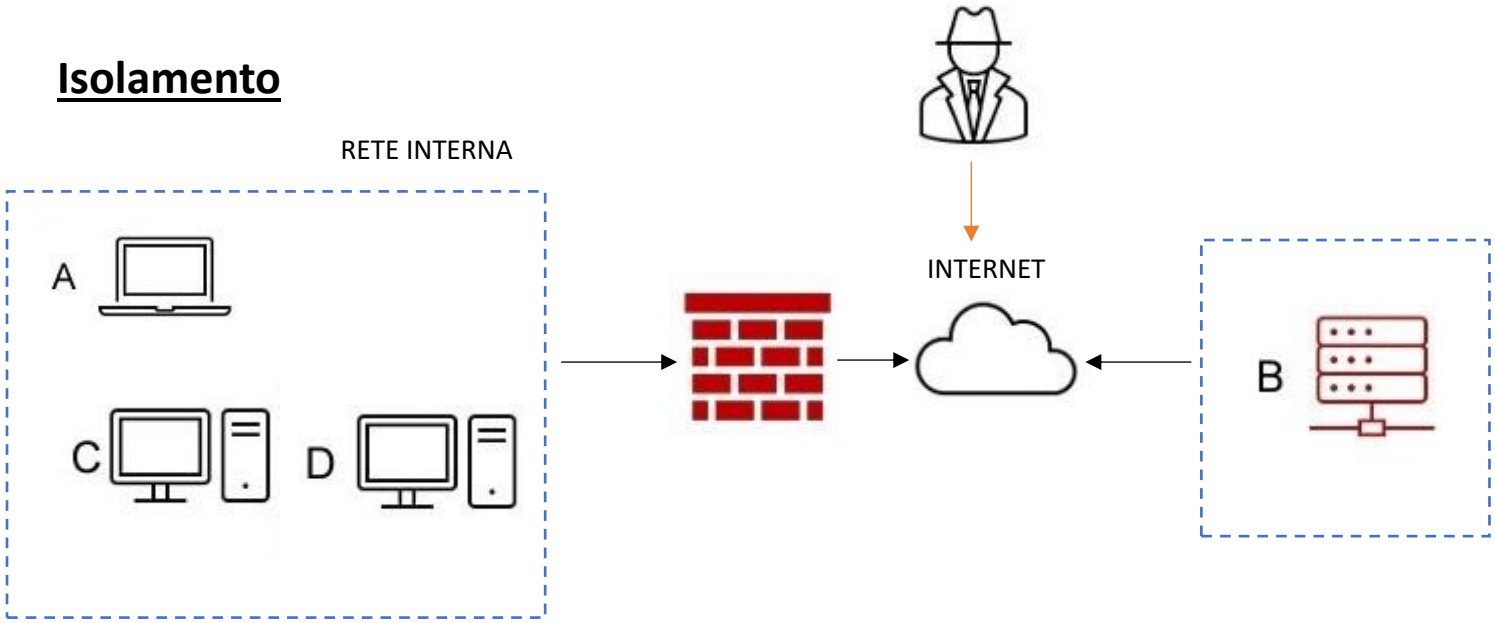


Nell'immagine possiamo notare che è stato compromesso il database con diversi dischi per lo storage.

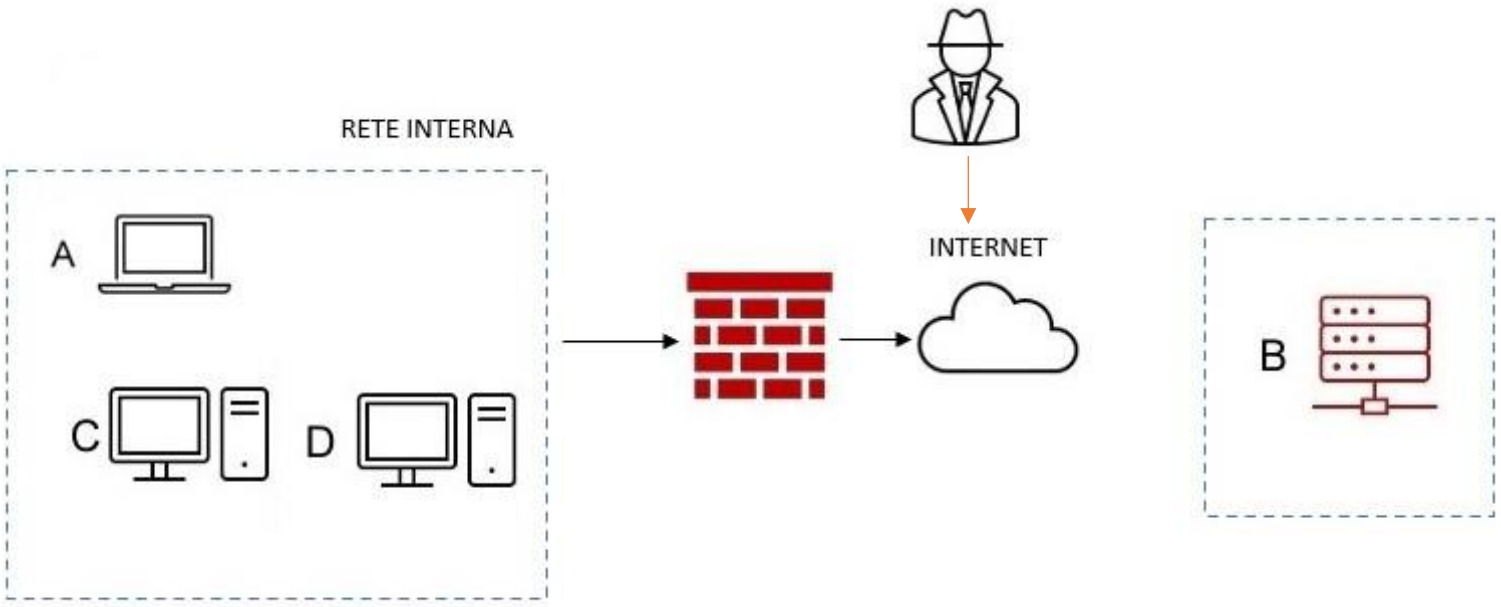
Abbiamo, a questo punto, due soluzioni per il contenimento:

- Isolamento del sistema infetto, che consiste nella completa disconnessione del sistema dagli altri dispositivi. In poche parole c'è ancora l'accesso ad internet ma la rete segmentata mi permette di isolarlo dagli altri dispositivi
- Rimozione del sistema infetto che consiste nello staccare i cavi, il dispositivo sarà isolato totalmente, sia dagli altri dispositivi che dalla rete internet. Questa avviene in situazioni particolarmente problematiche, è utilizzata soprattutto quando si tratta di proteggere dati sensibili o critici viene chiamata air gap, cioè una misura di sicurezza che implica la separazione fisica tra due sistemi informatici o reti

Isolamento



Rimozione



Una volta decisa la strategia si passa alla fase di recupero. In questa fase si deve tenere conto della gestione dei media contenenti dati sensibili o critici e gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso e ho 3 opzioni per farlo:

- **Clear**
  Il dispositivo viene formattato
- **Purge**
  si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi
- **Destroy**
  è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Si tratta di "disintegrare", "poverizzare" i media a livello fisico

La differenza tra le due opzioni è, dunque, che nella prima il dispositivo non viene distrutto, nella seconda si.