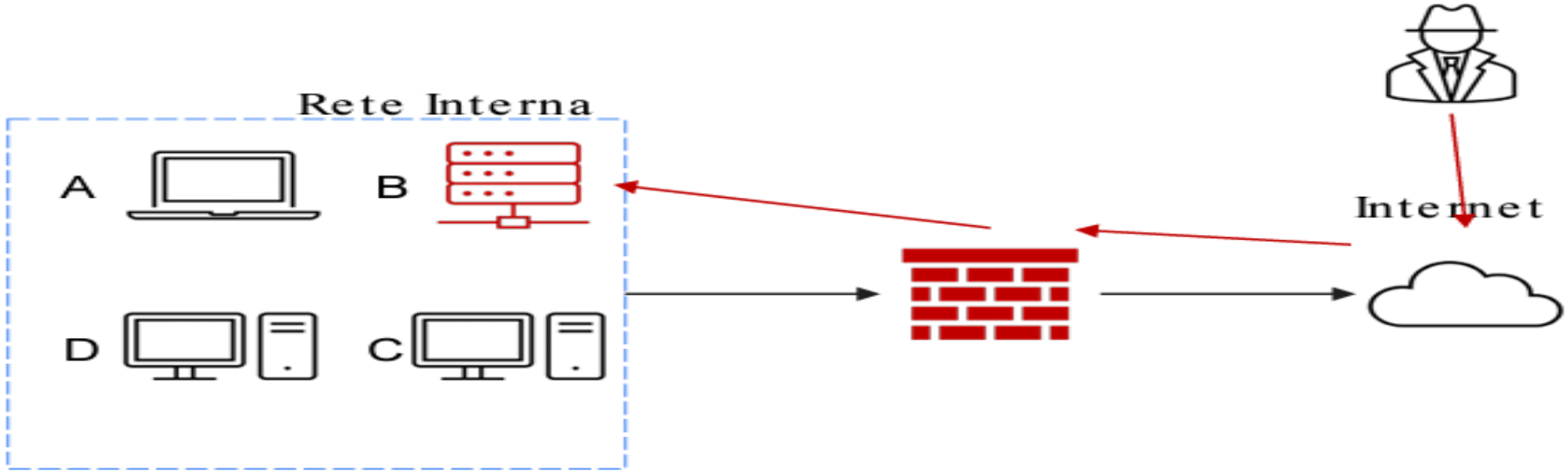
ES LEZIONE 4 SETTIMANA 9

Traccia:

Con riferimento alla figura in slide 4, 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.



- In questo specifico caso andiamo a svolgere due fasi per la salvaguardia della nostra rete. La prima sarà la fase di isolamento del sistema infetto, la seconda sarà quella della rimozione.
- Fase1 Isolamento: consiste nella completa disconnessione del sistema infetto dalla rete, per restringere l'accesso alla rete interna da parte dell'attaccante. In questo scenario l'attaccante ha ancora accesso al sistema C tramite internet, questo ci da modo di attuare azioni di information gathering verso il nostro attaccante.
- Fase2 Rimozioni: essendo sicuri che sia un hacker e che il sistema sia completamente compromesso si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet. In quest'ultimo scenario, l'attaccante non avrà né accesso alla rete interna né tanto meno alla macchina infettata.

- In fine abbiamo diverse tecniche di smaltimento che possiamo adottare, nel nostro caso la più indicata è la destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre a meccanismi logici e fisici dei metodi Purge e Clear, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.