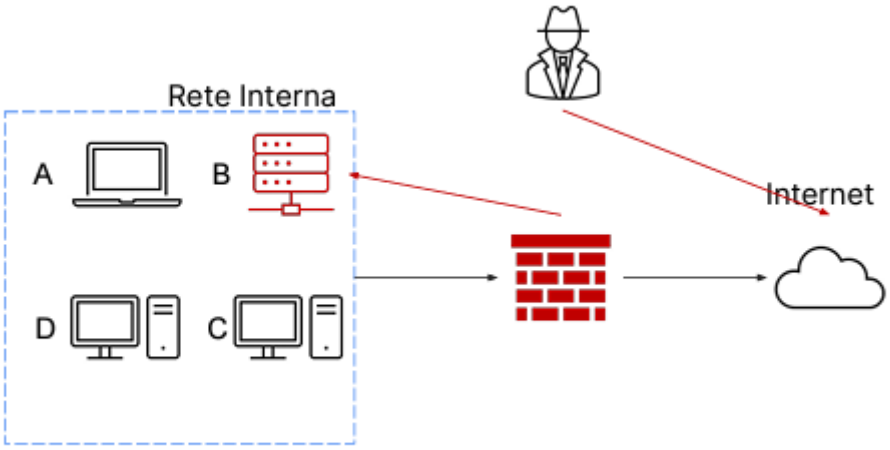
CONSEGNA SETTIMANA 9 LEZIONE 4

Incident response

---

*Supponiamo di essere parte del team **CSIRT**. Un database è stato compromesso da un attaccante, il quale è riuscito ad accedere al sistema tramite la rete internet. L'attacco è attualmente in corso, come affrontiamo le seguenti task?*

- Isolamento
- Rimozione del sistema B infetto



Prima di procedere alla rimozione del sistema infetto (nel nostro caso il database B), è necessario isolarlo dall'intera rete interna. Per fare ciò possiamo creare una **rete di quarantena**, segmentando la rete. In questo modo il sistema compromesso risulta separato e rende difficile all'eventuale attacante di poter infettare il resto della rete.

Nonostante questa sia una possibile prima linea di difesa, non sempre garantisce la protezione necessaria. Per questo, uno step successivo è il totale **isolamento** del sistema infetto, disconnettendolo completamente dalla rete locale, mantenendo l'accesso alla rete internet (se malauguratamente l'isolamento dalla rete interna non fosse sufficiente, è possibile isolare il sistema infetto anche dalla rete internet).

Possiamo infine passare alla fase di rimozione dell'incidente, ovvero, quando il team CSIRT elimina tutte le possibili attività e processi collegati all'attacco (un esempio può essere la rimozione di una shell o di una backdoor inserite malevolmente).

Quali sono le differenze tra Purge e Destroy?

Purge e destroy sono due modalità per gestire i dati contenuti in dischi di memoria.

Purge si approccia sia logicamente (come il **clear** che sfrutta le funzioni di factory reset o la capacità di read/write) sia fisicamente, tramite l'utilizzo di macchinari magnetici chiamati degausser, in grado di rendere inaccessibili i dati contenuti.

Destroy, invece è un metodo che introduce, oltre ad un approccio logico e fisico, un sistema ad alte temperature per la completa disintegrazione dei dati. Nonostante sia sicuramente il più efficace comporta anche un dispendio economico maggiore rispetto agli altri 2 metodi.