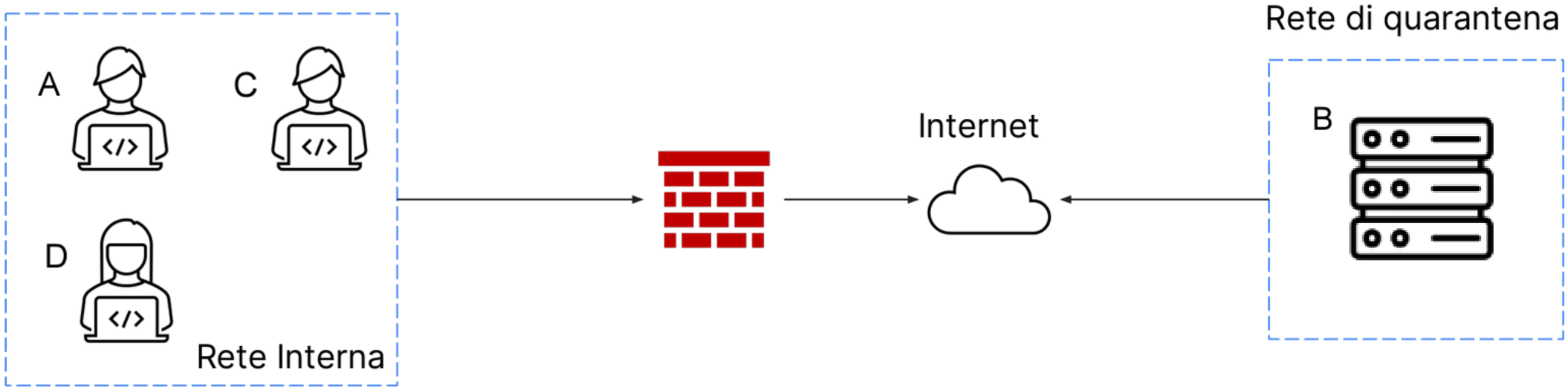
S9L4

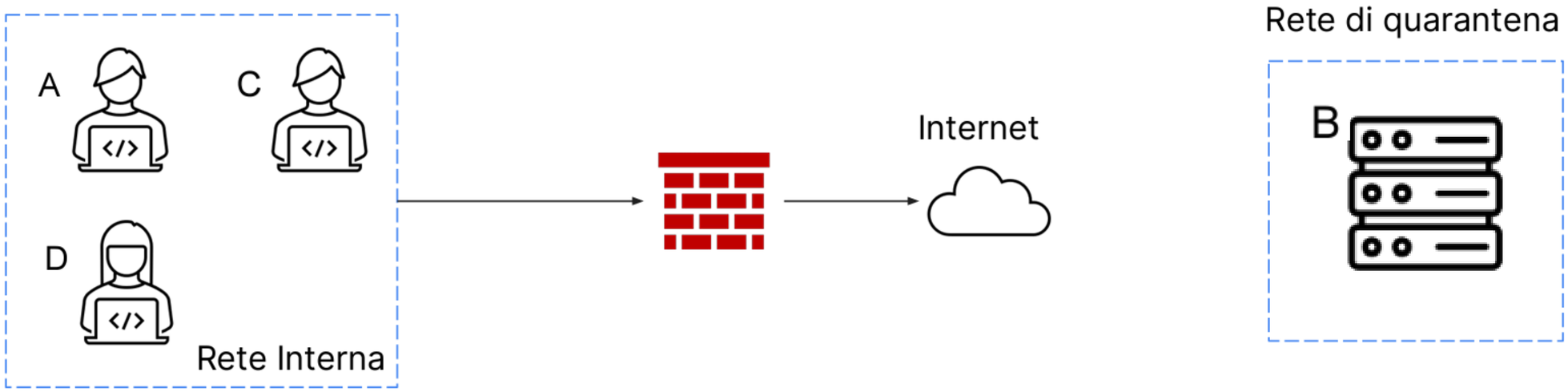
Incident response

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 ci approcciamo alla fase di contenimento, rimozione e recupero.
Il primo step della terza fase di un piano di risposta agli incidenti è il contenimento del danno causato dall'incidente di sicurezza.
Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo tale che non possa creare ulteriori danni a reti / sistemi.

L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l’accesso alla rete interna da parte dell’attaccante. Notate che in questo scenario l’attaccante ha ancora accesso al sistema B tramite internet.



Ci sono casi in cui l’isolamento non è ancora abbastanza. In questi casi 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 tantomeno al server infettato.



Durante la fase di recupero, ci si trova spesso a dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso. In questo caso bisogna accertarsi in prima istanza che le informazioni presenti sul disco/componente siano completamente inaccessibili prima di smaltire / utilizzare nuovamente il disco.

Abbiamo a nostra disposizione diverse opzioni tra cui :

- 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. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.