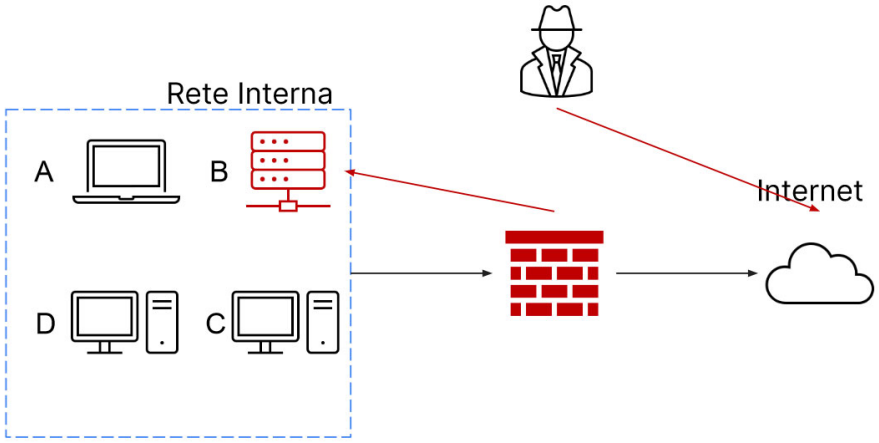
INCIDENT RESPONSE

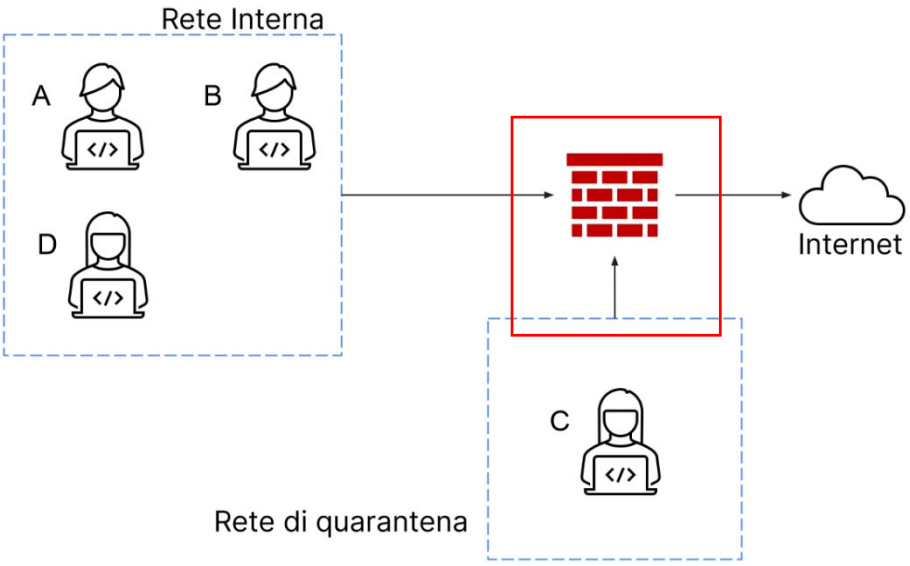
Il sistema **B** (database con dischi per storage) è stato compromesso internamene da un attaccante che è ruscito a bucare la rete ed accedere al sistema tramite internet.



FASE 1

Inizialmente si utilizza il metodo di quarantena classica. Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la "**segmentazione**", che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso.

La segmentazione permette di separare il sesitema **B** dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata generalemte "**rete di quarantena**". La rete ad hoc sarebbe una seconda rete interna collegata sempre al nostro firewall.

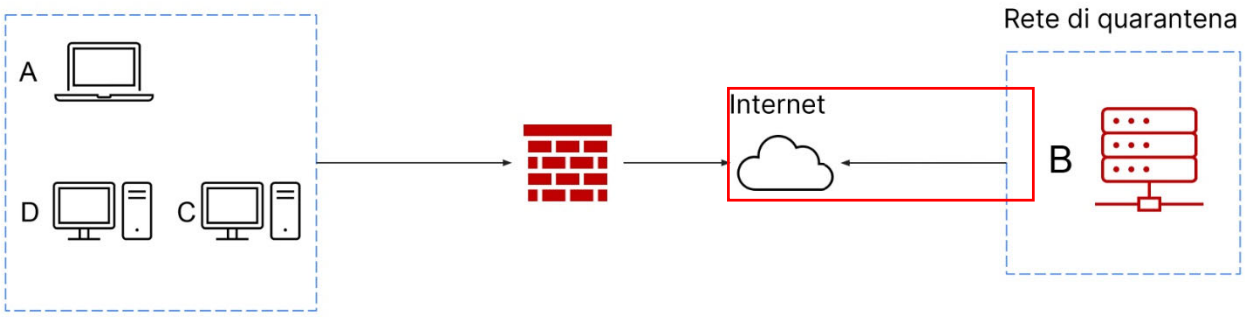


esempio di rete in quarantena

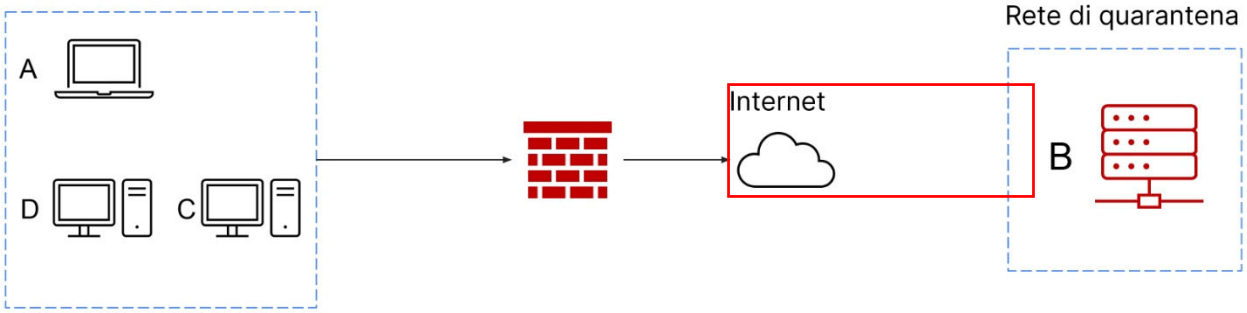
FASE 2

Nella seconda fase utilizzeremo la **tecnica dell'isolamento**.

La Tecnica dell'isolamento consiste nella completa disconessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In questo caso l'attaccante ha ancora accesso al sistema **B** tramite internet. Questo metodo viene utilizzato anche per poter analizzare il nostro attaccante per raccogliere maggiori informazioni.



In alcuni casi l'isolamento non è abbastanza e si ricorre alla "**rimozione**" del sistema **B** dalla rete (interna e internet). In questo caso l'attaccante non avrà ne accesso alla rete interna né alla macchina infettata.



FASE 3

Per quanto riguarda i sistemi che sono stati compromessi durante un attacco, vengono considerati compromessi. In questo caso i sistemi infettati vengono ripuliti a fondo prima di essere riutilizzati nuovamente. I metodi utilizzati sono **Clear**, **Purge** e **Destroy.**

CLEAR: il dispositivo viene ripulito usando tecniche logiche. Con tecniche wipe (dati sovrascritti più volte) si riporta al factory reset.

PURGE: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili 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 dei dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici s 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 quello che comporta un effort in termini economici maggiore.