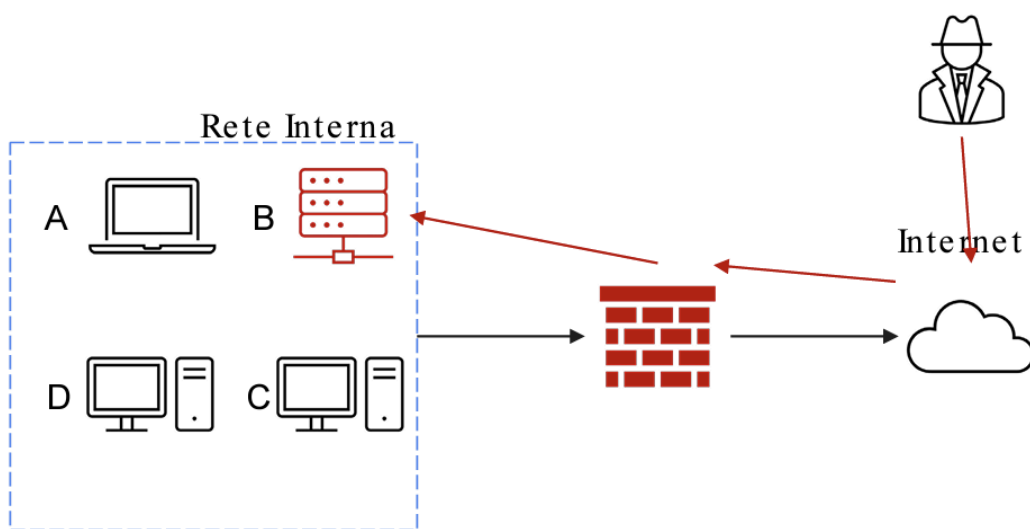


S9/L4

Stefano Di Prospero

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.



Per prima cosa ISOLIAMO il sistema B creando una zona di quarantena così da restringere l'attacco alla sola macchina vittima.

Successivamente procediamo alla RIMOZIONE rendendo la macchina inaccessibile dalla rete , eliminando così l'accesso da parte dell'attaccante.

La tecnica PURGE è un approccio sia a livello software, quali eliminazione dati ad esempio, sia a livello fisico, che però non prevede la distruzione dell'hardware.

La tecnica DESTROY implica un approccio che punta a rendere completamente inaccessibili i dati. Ciò prevede la distruzione fisica dell'hardware.