Nella casistica in esempio della rete interna compromessa da un hakcer introdottosi nel database,quindi al di sopra delle leggi del FIREWALL e dunque capace di infettare le altre macchine della rete,risolvero' la criticita' delle problematiche procedendo by steps.
Per prima cosa isoleremo il database dalla rete e dalle altre macchine in quest'ultima segmentando le reti dunque cambiando la subnet/subnetmask della macchinna infetta ed eliminando legami relativi al software,hardware e server non gestiti dal FIREWALL,in questo modo si ottengono due reti non comunicanti tra loro ma difese dallo stesso FIREWALL,ma' se' l'entita' del malware/software risultasse ancor piu' critica in modo immediato si dovrebbe optare per la rimozione completa della vittima(da reti interne,FIREWALL ed internet),che in questo caso e' un database di piu'dischi che ritengo opportuno rimuovere ed analizzare nella loro totalita'.
Ora nel caso si parli di una macchina non compromessa da un ransomware,come per esempio un "eternal blue",casi di reverse shell o compromissione dei privilegi nel sistema,ma si tratti di in malware/rasomware di minore entita' si procedera' con il "CLEAR",con un approccio di tipo "READ AND WRITE" sulla macchina non necessariamente il reset/formattazione totale il piu' delle volte,ma dopo un analisi approfondita delle vulnerabilita' presenti e degli exploit usati,avendo risolto sovrascrivendo i dati danneggiati,si riportera la macchina allo stato in cui era prima dell'attacco.
Nel caso il danno fosse irreversibile in quanto dati sensibili potrebbero essere esposti,si proccedera con il "PURGE" ovvero la riomozione fisica con l'utilizzo di forti magneti per rendere le informazioni inaccessibli da altri dispositivi smagnetizzando elementi hardware.
Nell'ultimo e peggiore dei casi si procede con l'aproccio "DESTROY" che prevede la polverizazzione dell'elemento infetto.