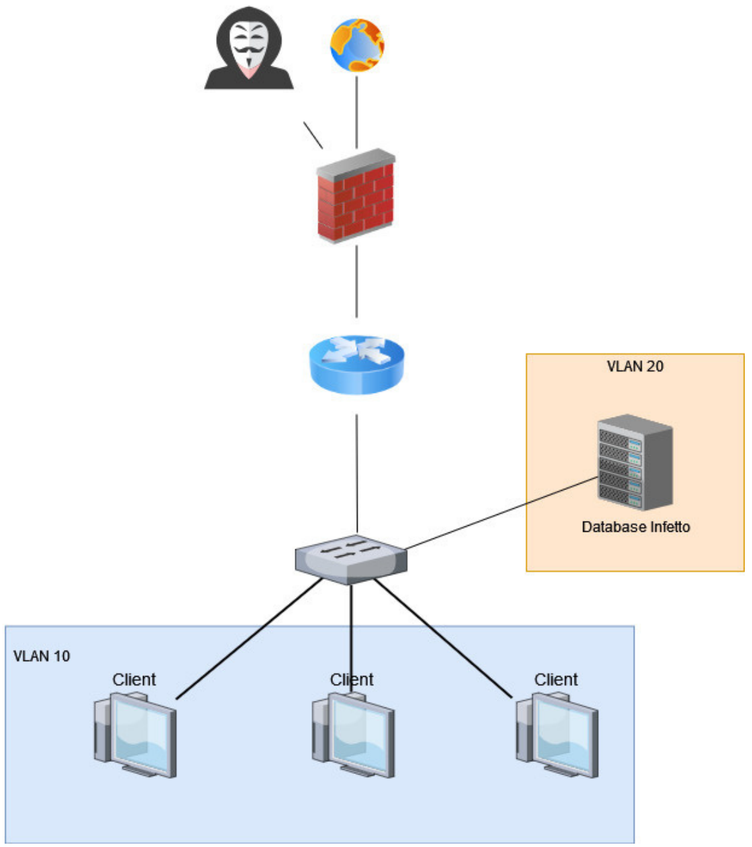
S9 L4

Incident Response

Daniele Zizzi

Per isolare un sistema infetto possiamo ricorrere al subnetting oppure creare una vlan apposita per contenere l’host infetto.
Altro modo per isolarlo sarebbe disconnettere totalmente l’host dalla rete, staccando il cavo di rete. Tentare la rimozione dei virus/malware presenti nel sistema attraverso l’uso di tool appositi(antivirus/antimalware), potrebbe essere una soluzione, ma se la minaccia ha già compromesso i file, l’azione di pulizia è inutile.



Una volta violato, un sistema non può più considerarsi affidabile, pertanto, prima di smaltirne i dischi collegati ad esso, si procedere con una delle tecniche chiamate “purge” e “destroy”.
Queste tecniche hanno lo scopo di rendere i file inaccessibili e quindi irrecuperabili, pur utilizzando tool molto potenti e macchinari dedicati a tale scopo.

Purge: consiste nell’utilizzare non solo formattazioni a basso livello, ma anche potenti magneti al fine di smagnetizzare i dischi rigidi(HDD).

Destroy: invece utilizza metodi più drastici, ma migliori al fine di rendere i dati inesistenti. Poichè comporta la distruzione completa dei dischi a livello fisico.
Il costo è più elevato rispetto al purge.