ESERCIZIO 1 M5 D7

INCIDENT RESPONSE

1

- ## ISOLAMENTO

Si parla di **isolamento** di un sistema infetto, come nel nostro caso ovvero un database compromesso, quando viene sfruttata una delle potenzialità della segmentazione della rete. L'isolamento consiste nella completa disconnessione del database (nel nostro caso) dalla rete intranet per fare in modo che l'attaccante non abbia la possibilità di accedere alla rete interna pur essendo sempre in grado di comunicare con il sistema attaccato essendo connesso ad internet.

- ## RIMOZIONE

Se nel nostro caso invece riteniamo che l'**isolamento** non è abbastanza performante per annullare la minaccia in corso possiamo attuare una versione più restrittiva ovvero la **rimozione**. Significa rimuovere il sistema infettato sia dalla rete interna che da internet, quindi "disconnesso" in maniera completa. In questo caso l'attaccante no sarà più in grado di comunicare con il dispositivo e quindi non potrà avanzare all'interno della nostra rete.

2

- ## PURGE VS DESTROY

Si parla di purge e destroy in ambito di recupero del sistema infettato, una volta gestito il momento dell'attacco. Quindi la decisioni da prendere sono in base al danno ricevuto ma soprattutto ci dovremmo accertare che le informazioni sui dischi siano completamente inaccessibili prima di smaltire o utilizzare nuovamente l'hardware.
Le due possibilità più "invasive" sono il purge ed il destroy: per **purge** si intende un approccio intermedio tra logico e fisico quindi utilizzo di tecniche di *read&write* per sovrascrive il disco almeno 5/7 volte e fare in modo che il contenuto che esisteva prima sia completamente cancellato (tecnica **clear**) più l'utilizzo "fisico" di magneti per rendere qualsiasi informazioni indisponibile. Per destroy si intende l'approccio più "distruttivo" infatti oltre alle tecniche precedenti si utilizzano anche procedimenti da laboratori quali disintegrazione, polverizzazione dei media ad alte temperature o la trapanazione. Ovviamente quest'ultimo metodo si utilizza per avere la certezza di aver "pulito" il sistema dall'attacco però perdendone completamente un futuro utilizzo quindi accettando il danno economico in maniera completa.