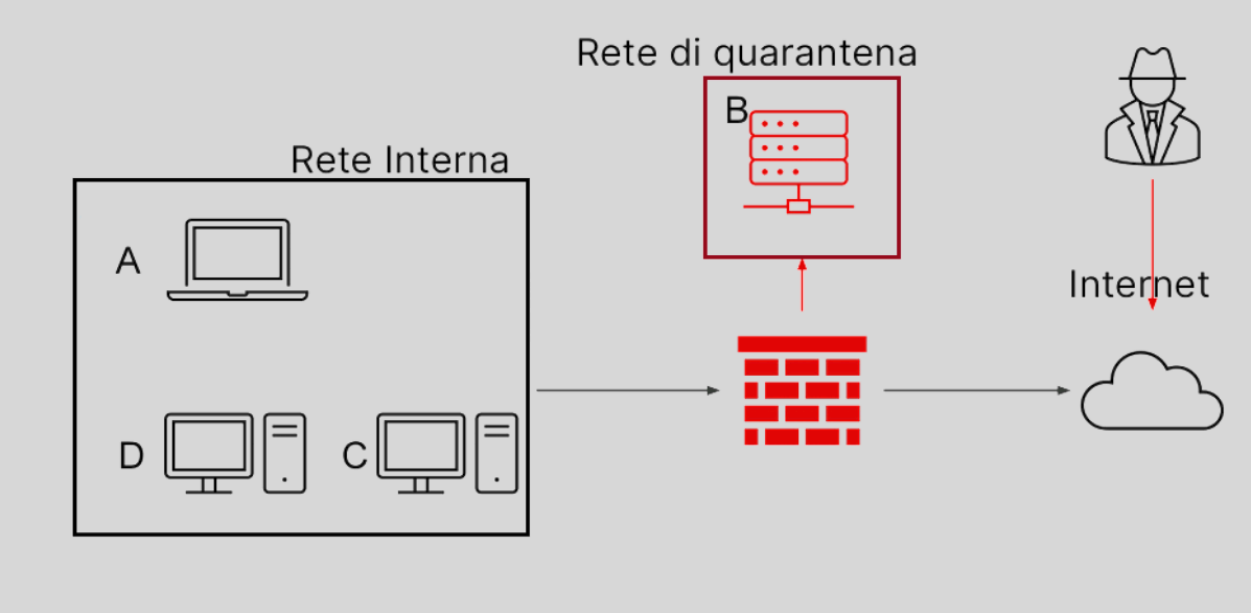
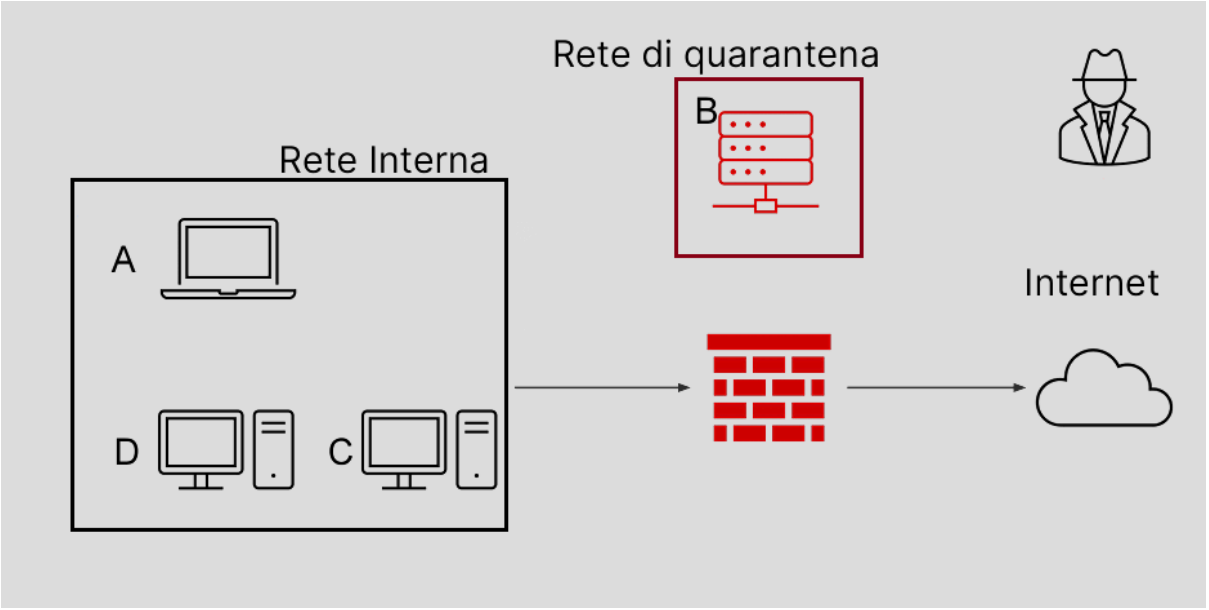
Lezione S9/L4

Rosario Giaimo

ISOLAMENTO
La tecnica di isolamento permette di limitare l'accesso dell'attaccante alla rete interna, isolando il sistema infetto. Questo può essere fatto creando una rete separata, segmentando la rete, utilizzando firewall o virtualizzazione. Per rimuovere il sistema infetto, è necessario utilizzare strumenti antivirus e antimalware per individuare e rimuovere il malware. In alcuni casi, potrebbe essere necessario ripristinare il sistema a uno stato precedente o reinstallare completamente il sistema operativo.



RIMOZIONE
La tecnica di rimozione del sistema infetto comporta l'eliminazione completa del sistema dalla rete, rendendolo inaccessibile sia dalla rete interna che da Internet. Ciò riduce l'accesso dell'attaccante al sistema infetto e minimizza il rischio di ulteriori danni o accessi non autorizzati. Questo processo coinvolge la formattazione del disco rigido e la reinstallazione completa del sistema operativo, seguita dall'installazione di misure di sicurezza aggiuntive.



La differenza tra Purge (pulizia) e Destroy (distruzione) nell'eliminazione delle informazioni sensibili prima dello smaltimento dei dischi compromessi è la seguente:

Purge: L'approccio di purge implica l'utilizzo di misure logiche e fisiche per l'eliminazione permanente dei dati su un disco o dispositivo di storage. Le tecniche logiche coinvolgono l'uso di software specializzati per sovrascrivere i dati in modo sicuro, rendendo difficile o impossibile il recupero delle informazioni originali. Questo processo può essere eseguito utilizzando algoritmi di cancellazione sicuri che sovrascrivono i dati più volte.

Destroy: D'altra parte, l'approccio di destroy comporta la distruzione fisica del disco o del dispositivo di storage. Questo può essere fatto utilizzando metodi come la perforazione, la triturazione o la fusione del dispositivo per renderlo completamente inutilizzabile e impedire il recupero dei dati. La distruzione fisica è un metodo molto sicuro per garantire che i dati sensibili non siano più accessibili, ma può comportare la perdita permanente dell'hardware stesso.