

Procedura di isolamento e rimozione del sistema infetto B

Tramite la tecnica della segmentazione possiamo dividere il sistema infetto B creando una rete appropriata unica e inaccessibile che chiameremo rete di quarantena.

In questo modo il malware resterà confinato e non potrà infettare anche gli altri sistemi.

In alcuni casi, se la situazione lo richiede, si possono adottare misure di sicurezza più stringenti come la disconnessione dalla rete.

Per smaltire un sistema infetto si possono adottare due misure differenti

Purge: in questo caso si adottano sia misure logiche, utilizzo di software specifici per la rimozione dei dati che misure fisiche come l'utilizzo di forti magneti

Destroy: si impiegano ampie e nette misure fisiche come tecniche di laboratorio per la polverizzazione ad alte temperature.

Sicuramente il più efficace ma anche il più dispendioso in termini economici