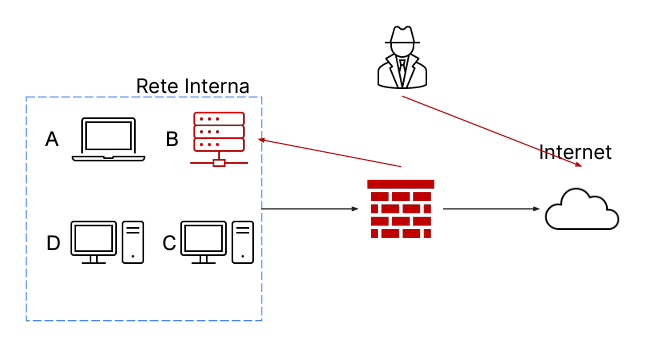
**INCIDENT RESPONSE**

**CENNI TEORICI**  
CSIRT (Computer Security Incident Response Team): Team che si occupa dell’Incident Response.  
Incident Response: è un insieme di procedure e azioni messe in atto per gestire e mitigare gli effetti di un attacco o minaccia alla sicurezza informatica.   
Questi eventi, noti come incidenti di sicurezza, possono includere attacchi informatici, violazioni dei dati, malware, perdita di informazioni sensibili e altri problemi che minacciano l'integrità, la riservatezza o la disponibilità dei dati.  
Il processo di Incident Response coinvolge 4 fasi:  
1) Preparazione: Definizione delle politiche e dei protocolli di sicurezza, formazione del personale e implementazione di strumenti di monitoraggio per rilevare e prevenire incidenti.  
2) Rilevamento e Analisi: Riconoscimento di attività anomale o sospette che potrebbero indicare un incidente di sicurezza.  
3) Contenimento, Eliminazione e Recupero:   
 a) Contenimento: Si “contiene” l'incidente per evitare ulteriori danni e limitare la sua diffusione. Una tecnica può essere la segmentazione in diverse LAN o VLAN. In casi peggiori possiamo pensare di “mettere in quarantena” (separare e monitorare il dispositivo) o “isolare” (separare completamente il dispositivo fino a nuove patch). Nel caso più estremo verrà effettuata la “rimozione” del dispositivo dalla rete.  
 b) Eliminazione: Lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell’incidente all’interno della rete o sui sistemi. Questa attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette usb compromesse.  
 c) Recupero: La fase di recupero consiste nel ristabilire la normale operatività delle applicazioni e dei servizi. Include ad esempio il recupero dei dati e delle informazioni perse, l’applicazione delle patch dove disponibili per eventuali sistemi obsoleti, la revisione delle politiche dei firewall, IPS e IDS oppure l’aggiornamento delle firme degli antivirus. Infatti, lo scopo della fase di recupero è anche quello di evitare che lo stesso attacco possa capitare nuovamente in futuro.  
   
  
 Per quanto riguarda i sistemi, server e host, se sono stati compromessi da un attaccante durante un attacco dovrebbero essere considerati non più affidabili e dovrebbero essere di conseguenza ripuliti a fondo prima di essere utilizzati nuovamente. A tale scopo, si utilizzano le tecniche di Reconstruction o Rebuilding.   
 c1.1) Reconstruction: include tutte quelle attività che mirano a recuperare quelle parti ancora affidabili di un sistema compromesso.   
 c1.2) Rebuilding: include tutte quelle attività che mirano a ricostruire interamente un sistema impattato considerato non più affidabile.  
 Per quanto riguarda l’integrità di un disco, ritroviamo invece 3 tecniche da eseguire in base alla situazione:  
 c2.1) Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.  
 c2.2) Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.  
 c2.3) Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.  
4) Analisi post-incidente: Valutazione dell'incidente per comprendere le cause, migliorare le procedure e prevenire futuri incidenti.

L'obiettivo principale della risposta agli incidenti è ridurre al minimo l'impatto di un incidente sulla sicurezza e ripristinare le operazioni normali nel minor tempo possibile.   
Un piano di risposta agli incidenti ben strutturato è essenziale per le organizzazioni al fine di proteggere gli assets e preservare la fiducia dei clienti ed il loro budget.  
  
**ESERCIZIO**

Con riferimento all’immagine sotto riportata, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.  
L’attacco è attualmente in corso e siete parte del team di CSIRT.  
Rispondere ai seguenti quesiti.  
Mostrate le tecniche di:  
I) Isolamento e rimozione del sistema B infetto.  
II) Spiegate la differenza tra Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



I) Isolamento e Rimozione:   
 1) Segmentazione in diverse LAN o VLAN.   
 2) “mettere in quarantena” (separare e monitorare il dispositivo). 3) Isolare (separare completamente il dispositivo fino a nuove patch).   
 4) Rimozione del dispositivo dalla rete (l’attaccante non avrà più accesso alla rete interna né tantomeno alla macchina infettata).  
II) Differenza tra Purge e Destroy:   
 1) Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.  
 2) Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature.