Relazione: Tecniche di Rimozione e Distruzione dei Dati in Risposta a Incidenti di Sicurezza

Introduzione: In risposta a un incidente di sicurezza informatica, è cruciale adottare misure efficaci per eliminare le minacce e proteggere i dati. Questa relazione esamina due tecniche fondamentali: la Rimozione e le strategie di Purge e Destroy.

Tecnica di Rimozione: La Rimozione è un processo che disconnette completamente un sistema infetto dalla rete. Questo metodo rende il sistema inaccessibile, sia internamente che esternamente via internet, precludendo all'attaccante l'accesso e limitando la diffusione dell'attacco.

Strategia di Purge: Il Purge combina misure logiche e fisiche per cancellare definitivamente i dati da un dispositivo di storage. Le tecniche fisiche impiegate sono non invasive e non comportano la distruzione dell'hardware, consentendo la possibile riutilizzazione del dispositivo.

Strategia di Destroy: Destroy è l'approccio più radicale, che utilizza tecniche fisiche invasive per rendere i dati irrecuperabili. Questo metodo include la distruzione fisica dell'hardware, garantendo che i dati e l'hardware stesso non possano essere recuperati o riutilizzati.

Discussione: La scelta tra queste tecniche dipende dalla gravità dell'incidente e dalla necessità di preservare o distruggere l'hardware. Mentre il Purge è meno costoso e permette la conservazione dell'hardware, Destroy è il metodo preferito per smaltire hardware non riutilizzabile, nonostante i costi più elevati.

Conclusione: La Rimozione, il Purge e il Destroy sono tecniche vitali nella gestione degli incidenti di sicurezza informatica. La loro implementazione deve essere guidata da una valutazione approfondita dell'incidente e dalla politica di sicurezza dell'organizzazione