Il sistema B, un database con diversi dischi predisposti allo storage, è stato compromesso interamente da un attaccante che ha violato la rete e ha ottenuto l'accesso al sistema tramite Internet. Come parte del nostro ruolo nel CSIRT, dobbiamo adottare misure per contrastare l'attacco e mitigare i danni. Le tre opzioni principali da prendere in considerazione sono l'isolamento, la rimozione del sistema B infetto e l'eliminazione delle informazioni sensibili presenti nei dischi compromessi.

Per quanto riguarda l'isolamento, l'obiettivo è limitare la diffusione dell'attacco e proteggere i sistemi e le reti adiacenti da ulteriori danni. Questa misura prevede la disconnessione immediata del sistema B dalla rete, interrompendo la comunicazione con l'attaccante e impedendo la propagazione dell'attacco ad altri sistemi. Inoltre, può essere implementata la segmentazione di rete, creando una sottorete separata dedicata all'isolamento dell sistema compromesso per ridurre il rischio di ulteriori compromissioni. L'utilizzo di firewall e liste di controllo accessi (ACL) potrebbe aiutare a filtrare il traffico sospetto e limitare le connessioni in ingresso e in uscita verso il sistema B.

La rimozione del sistema B infetto implica l'eliminazione del malware, delle backdoor e di tutti i componenti che minano la sicurezza dal sistema. Questa azione richiede l'utilizzo di software di sicurezza aggiornati per eseguire una scansione completa del sistema e identificare le minacce. Se disponibile, potrebbe essere consigliabile ripristinare il sistema da un backup precedente alla compromissione per assicurare la rimozione completa delle minacce. In alcuni casi gravi, potrebbe invece essere necessaria la reinstallazione completa del sistema per garantire uno stato sicuro.

Infine, riguardo all'eliminazione delle informazioni sensibili presenti nei dischi compromessi, dobbiamo considerare le opzioni di purging e distruzione. Il purging prevede l'eliminazione sicura delle informazioni sensibili sovrascrivendole o cancellandole in modo da rendere praticamente impossibile il loro recupero. Questo processo preserva l'integrità del dispositivo, consentendone un eventuale riutilizzo futuro. D'altra parte, la distruzione implica una forma più drastica di eliminazione delle informazioni; in questo caso, il dispositivo o il sistema viene fisicamente distrutto, garantendo che le informazioni non siano più recuperabili o accessibili in alcun modo. Si potrebbe anche valutare l'ipotesi di effettuare una semplice operazione di clearing dei dispositivi ma, essendo a conoscenza della portata abbastanza importante dell'attacco subito, sarebbe una scelta azzardata in quanto a differenza delle precedenti, il clearing, potrebbe lasciare tracce.

In conclusione, affrontare l'attacco in corso richiede un'azione tempestiva. L'isolamento del sistema B compromesso, la sua successiva rimozione e l'eliminazione sicura delle informazioni sensibili dai supporti compromessi sono misure essenziali per mitigare l'impatto dell'attacco e ripristinare la sicurezza del sistema.