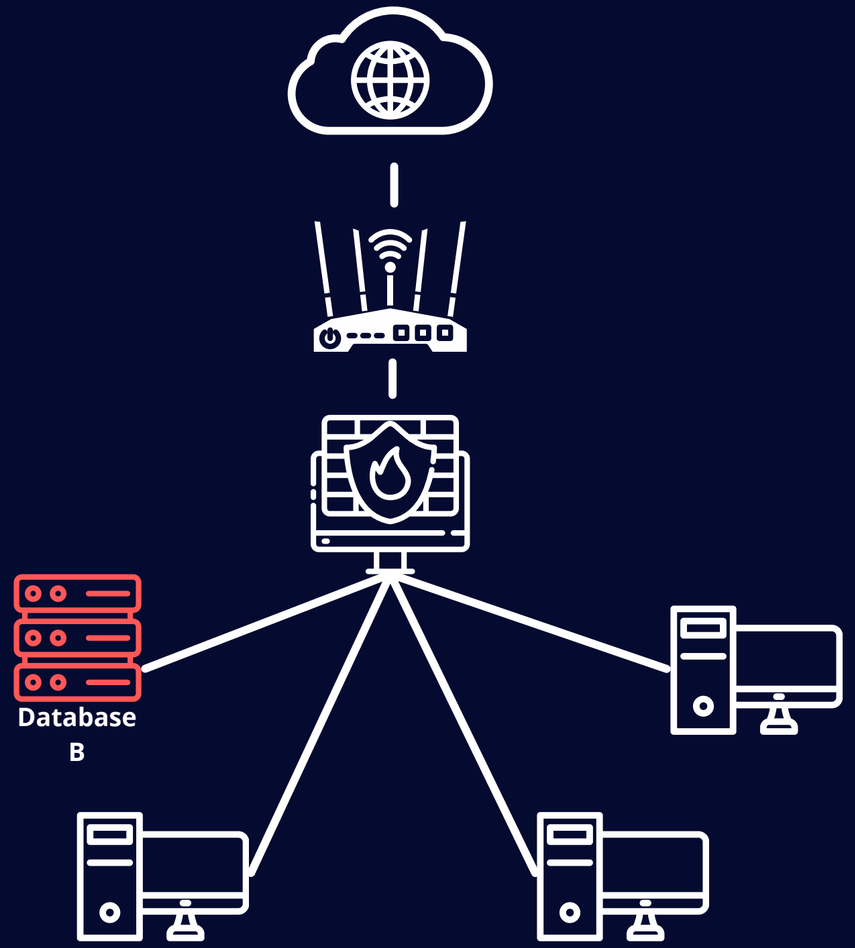
INCIDENT RESPONSE

S9 - L4

DEBRIEFING SULL'INCIDENTE

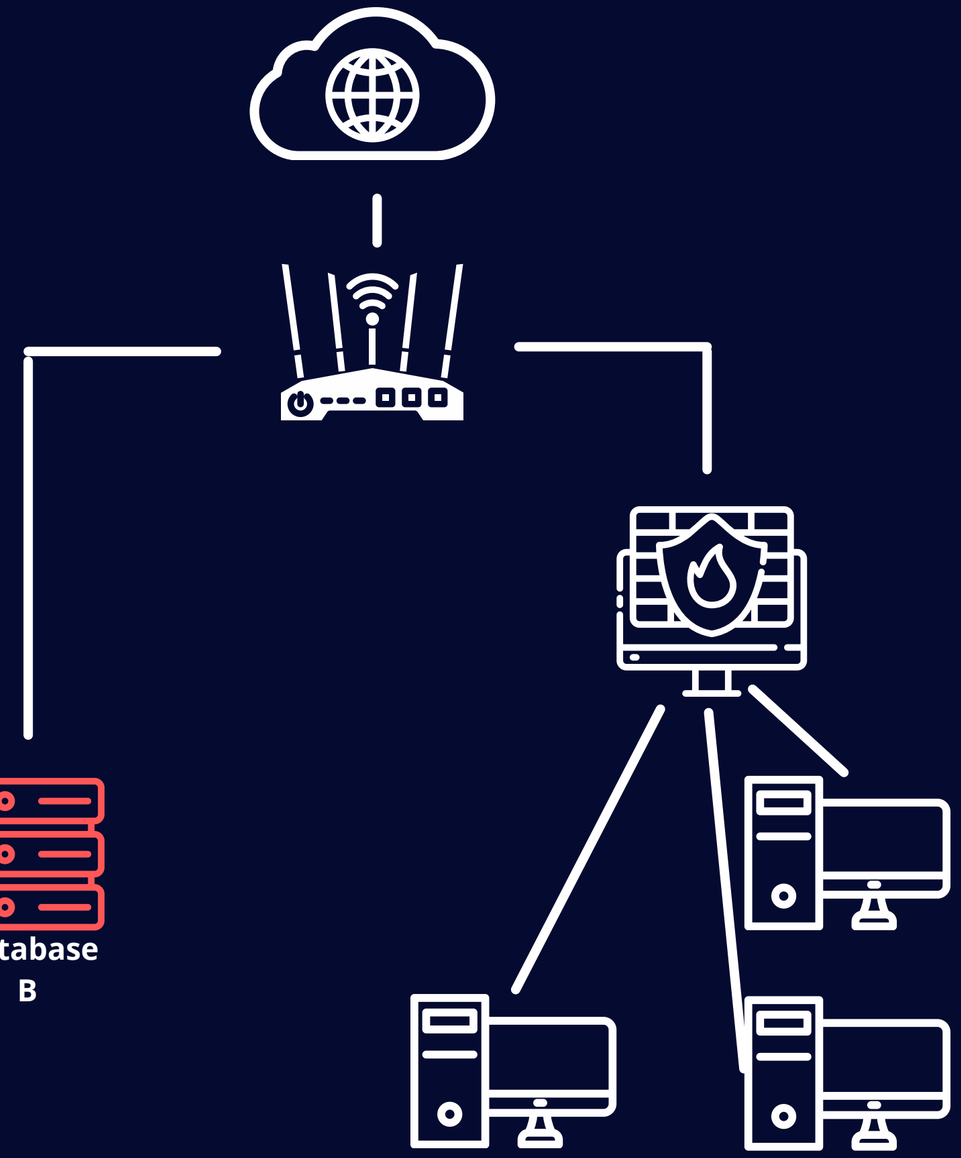


Il database B è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

Le azioni rimediative verranno esplorate nelle diapositive seguenti.

Isolamento

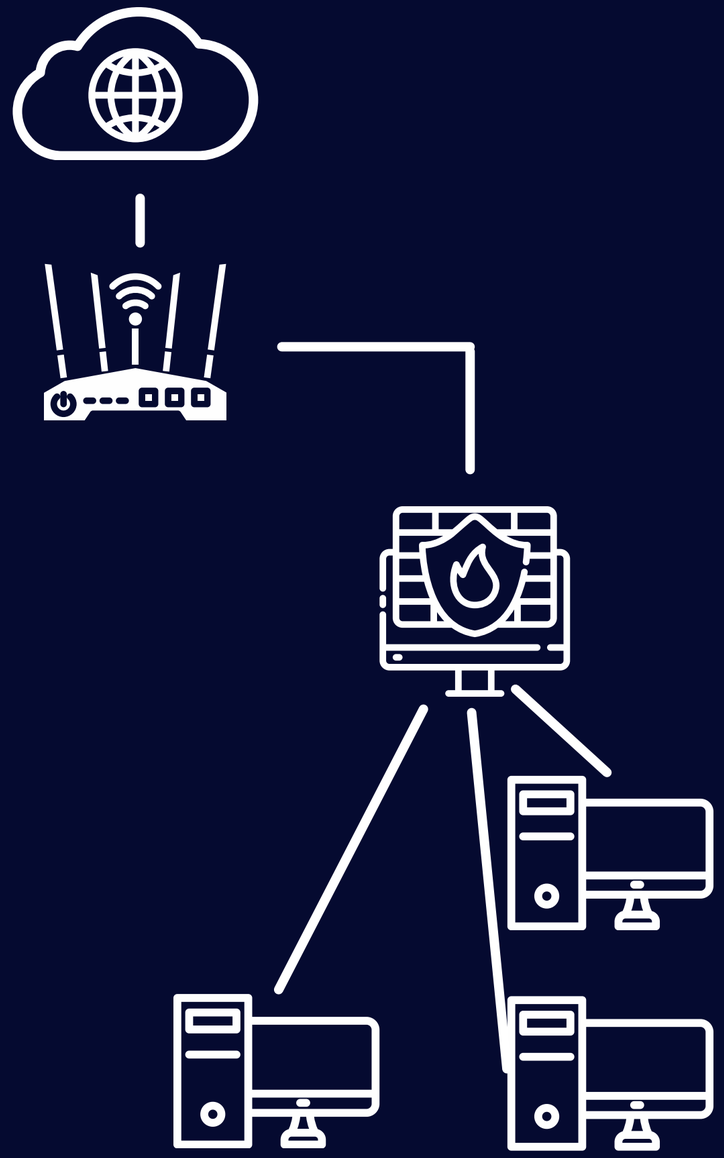
La prima azione difensiva da intraprendere sarà quella di isolare il database B attaccato, per questo lo inseriremo in una rete isolata, dove avrà comunque comunicazione con Internet, ma non con altri sistemi aziendali. In questo modo l’infezione non può diffondersi all’interno della rete aziendale interna.



Rimozione

Nel caso in cui il solo fatto che il database B sia connesso a Internet costituisca un rischio, è necessario rimuovere tutte le connessioni attive, soprattutto quelle che consentono all'aggressore di entrare in contatto con il database (Internet). Si tratta di un'opzione drastica, poiché rimuove anche tutti i servizi che il database può offrire agli utenti legittimi, ma è il modo migliore per garantire che l'aggressore non possa indagare ulteriormente il sistema da remoto.

Database B



Fase di Recupero

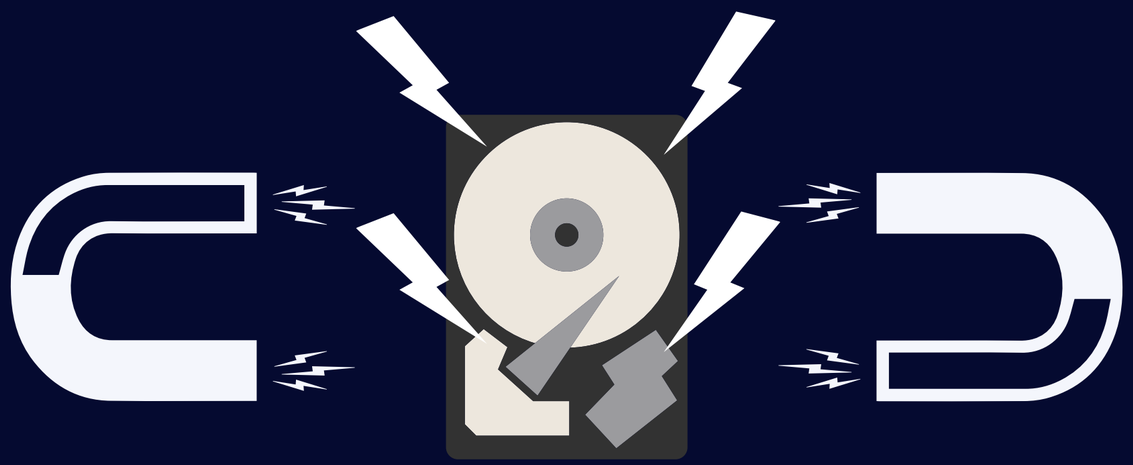
Durante la fase di recupero, ci si trova spesso a dover **gestire lo smaltimento** o il riutilizzo di un disco o un sistema di storage di un sistema compromesso. In questo caso bisogna accertarsi in prima istanza che le informazioni presenti sul disco/componente **siano completamente inaccessibili** prima di smaltire / utilizzare nuovamente il disco.

Esistono 3 modi per rimuovere i dati di un disco rigido, ma a noi interessa in particolare Purge and Destroy

Purge

Purge, oltre a utilizzare tecniche di pulizia logica, utilizza anche tecniche fisiche, come l'uso di potenti magneti per rendere inutilizzabili i componenti magnetici dei dischi rigidi. Questo processo è chiamato "Smagnetizzazione". Puoi anche eseguire il processo di cancellazione crittografica, in cui tutti i dati vengono crittografati in modo forte e la chiave di crittografia viene distrutta.

Con il metodo di crittografia il disco puo essere ancora utilizatto, meno la partizione che e stata crittografata.



Destroy

Distruggere il disco rigido è l’opzione nucleare. È il più sicuro e il più costoso se fatto correttamente. La distruzione del disco rigido può comportare la sua distruzione a livello molecolare, ad esempio disintegrandolo chimicamente o polverizzandolo con il calore.

Dopo questi processi, i dischi rigidi dovranno essere completamente sostituiti con altri completamente nuovi.