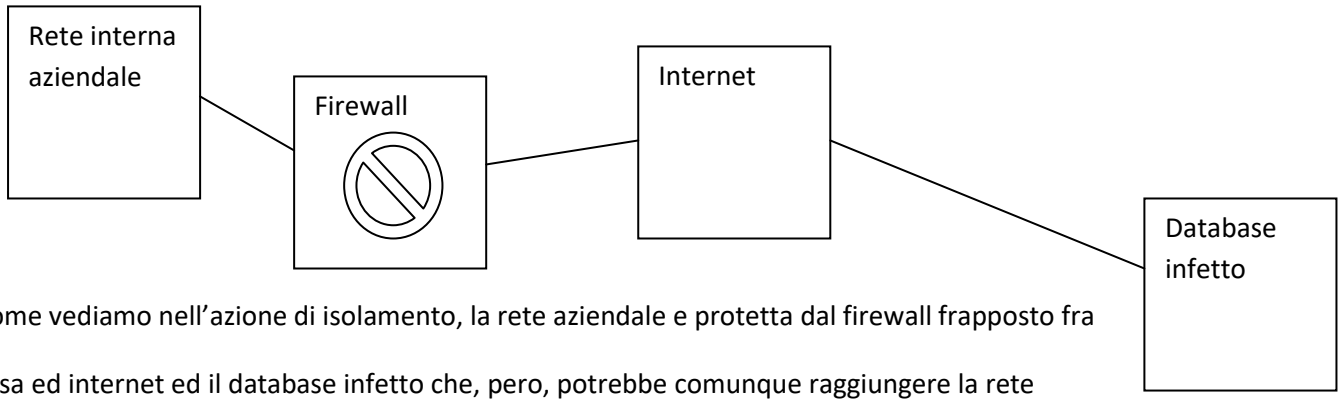
Oggi andremo ad effettuare un azione di incident response per un'azienda che ha subito un attacco tramite internet da un black hater e che ha visto il un suo database, con diversi dischi per lo storage, compromesso.

Noi, membri del csirt designato dall'azienda nella fase della creazione del suddetto, passeremo direttamente alla fase 3 (fase di contenimento,rimozione e recupero) in quanto l'attacco e stato eseguito e l'incidente sull'azienda ha gia impattato. Nello specifico andremo a cercare di ridurre il piu possibile gli impatti dell'incidente, ad eliminare l'incidente dalla rete aziendale e recupereremo i servizi.

La criticita dell'incidente la classificherei come media dato che il database contiene diversi dischi per lo storage ma molti servizi possono continuare ad essere garantiti e l'impatto monetario non e elevatissimo.

Essendo gia infetto il databasee essendo l'attacco proveniente da internet, eviterei di adottare la soluzione della quarantena come azione, ma proporrei azioni piu drastiche quali l'isolamento e la rimozione . Nello specifico, si intende con l'isolamento la condizione in cui il database infetto viene completamente rimosso dalla rete aziendale mentre con rimozione, l'azione piu drastica, si rimuove completamente il database infettato sia da internet che dalla rete aziendale (magari staccando i fili e lasciandolo spento) in modo tale che l'attaccante non solo non abbia accesso alla rete aziendale, ma neanche alla macchina attaccata. Per una piu facile comprensione, illustreremo graficamente i due metodi.

AZIONE DI ISOLAMENTO:

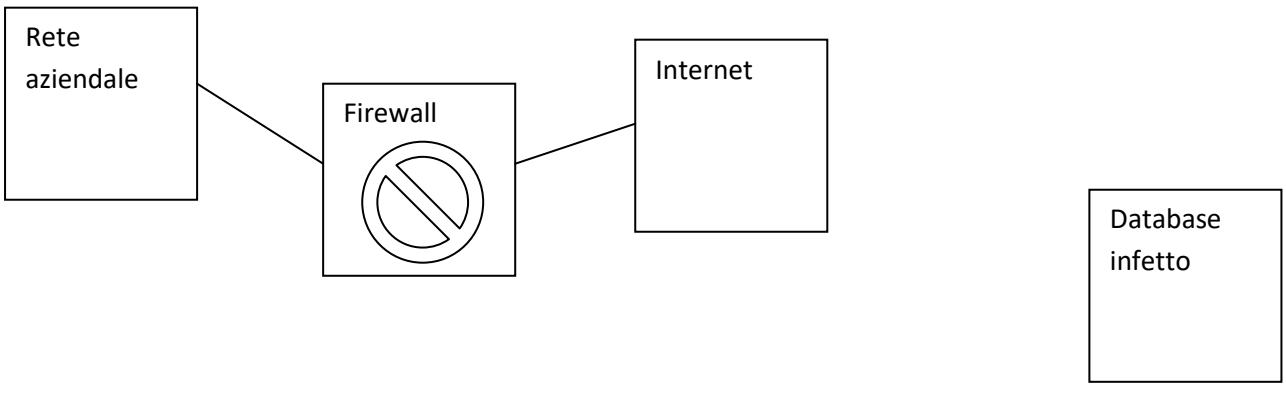


Come vediamo nell'azione di isolamento, la rete aziendale e protetta dal firewall frapposto fra

Essa ed internet ed il database infetto che, pero, potrebbe comunque raggiungere la rete

Attraverso internet.

AZIONE DI RIMOZIONE:



Come si evince dal grafico, con la rimozione si “elimina”, per cosi dire, il database infetto rimuovendolo ovviamente sia da internet che dalla rete aziendale (spegnendolo e non usandolo piu).

A mio parere l’azione migliore e l’isolamento dato che la rete interna e comunque protetta da un firewall. Quindi, una volta capito l’attaccante come e entrato (attraverso una porta aperta vulnerabile o tramite una campagna di phishing) ci si comportera di conseguenza e si creera una policy nel firewall che faccia si che l’incidente non ricapiti, senza rendere inutilizzabile il database.

Fatto questo, andremo ad assicurarci che le info contenute nel database siano inaccessibili e, se cosi fosse, andremo a sceglire una delle 3 seguenti azioni:

CLEAR = il dispositivo viene ripulito con tecniche logiche e quindi puo essere riutilizzabile magari per dati non sensibili

PURGE = e un’azione piu drastica che si effettua quando i dati sono sensibili, si effettuano operazioni logiche ma anche fisiche come potrebbero essere l’uso di forti magneti.

DESTROY = e la tecnica piu drastica che consiste nell’eliminare drasticamente il dispositivo, bruciandolo o polverizzandolo.

Io come azione intraprenderei PURGE, dato che il database contiene informazioni sensibili ed e comunque stato attaccato. Quindi è comunque un metodo piu sicuro rispetto al CLEAR, che resisterebbe in questo caso solamente ad un attacco ben impostato “da tastiera” (come si dice in gergo), ma e meno drastico rispetto all’zione destroy, che eliminerebbe proprio fisicamente il database, bruciandolo o polverizzandolo, rendendolo ovviamente inutilizzabile e quindi mettendo l’azienda nella condizione forzata di comprarne un altro.