Report sull'Incidente di Sicurezza

Introduzione

Come membro del team di CSIRT, mi sono occupato della gestione di un incidente di sicurezza che ha visto il sistema B (un database con diversi dischi per lo storage) compromesso da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L'attacco è attualmente in corso e il nostro obiettivo principale è isolare, rimuovere e analizzare il sistema infetto, nonché eliminare in modo sicuro i dati sensibili.

Fase 1: Isolamento del Sistema B Infetto

Identificazione del Sistema Infetto

La prima fase ha coinvolto l'identificazione precisa del sistema infetto. Abbiamo utilizzato strumenti di monitoraggio della rete e analisi dei log per confermare che il server B fosse la fonte dell'attacco. Questi strumenti ci hanno permesso di rilevare attività anomale e tentativi di connessione non autorizzati.

Disconnessione dalla Rete

Una volta identificato il sistema B come compromesso, abbiamo proceduto con l'isolamento:

1. **Isolamento Fisico**:
    - Ho scollegato fisicamente il cavo di rete del server B, assicurando che non avesse più accesso alla rete interna.
2. **Isolamento Logico**:
    - Ho rimosso il server B dalle VLAN della rete interna e disabilitato il suo indirizzo IP per prevenire qualsiasi tentativo di comunicazione.

Configurazione del Firewall

Per rafforzare l'isolamento, ho aggiunto regole specifiche al firewall:

- Blocco di tutto il traffico in entrata e in uscita dal server B.
- Monitoraggio continuo per identificare e bloccare ulteriori tentativi di connessione.

Monitoraggio delle Connessioni

Utilizzando strumenti come Wireshark e tcpdump, ho monitorato le connessioni di rete per rilevare e bloccare eventuali connessioni sospette ancora attive.

Disegno - Isolamento del Sistema

Fase 2: Rimozione del Sistema B Infetto

Dopo l'isolamento, ho avviato il processo di rimozione del sistema B:

Backup dei Dati Critici

Ho effettuato un backup completo dei dati non infetti presenti sul server B, utilizzando un supporto sicuro e isolato per garantire che nessun dato critico venisse perso durante la rimozione.

Spegnimento del Sistema

Ho arrestato il sistema B in modo sicuro, evitando ulteriori esecuzioni di malware e proteggendo l'integrità dei dati per l'analisi forense.

Rimozione Fisica

Il server B è stato rimosso fisicamente dal datacenter. Questa misura ha assicurato che l'attaccante non potesse più accedere al sistema, nemmeno tramite connessioni remote.

Analisi Forense

Il sistema è stato trasferito in un ambiente sicuro per un'analisi forense dettagliata. Utilizzando strumenti come FTK Imager e EnCase, ho esaminato il server per raccogliere prove dell'attacco, comprendere il vettore di attacco e valutare l'entità del compromesso.

Disegno - Rimozione del Sistema

Fase 3: Eliminazione Sicura dei Dati

Clear

Clear implica l'eliminazione logica dei dati, rendendoli inaccessibili tramite metodi standard di accesso al sistema. Esempi di questa tecnica includono l'uso del comando delete su sistemi operativi. Tuttavia, i dati eliminati in questo modo possono essere recuperati con strumenti specializzati.

Purge

Purge comporta la rimozione dei dati in modo che non possano essere recuperati tramite metodi standard. Le tecniche di purge includono:

- Sovrascrittura multipla dei dati (ad esempio, con il comando shred su Linux).
- Smagnetizzazione dei dischi.

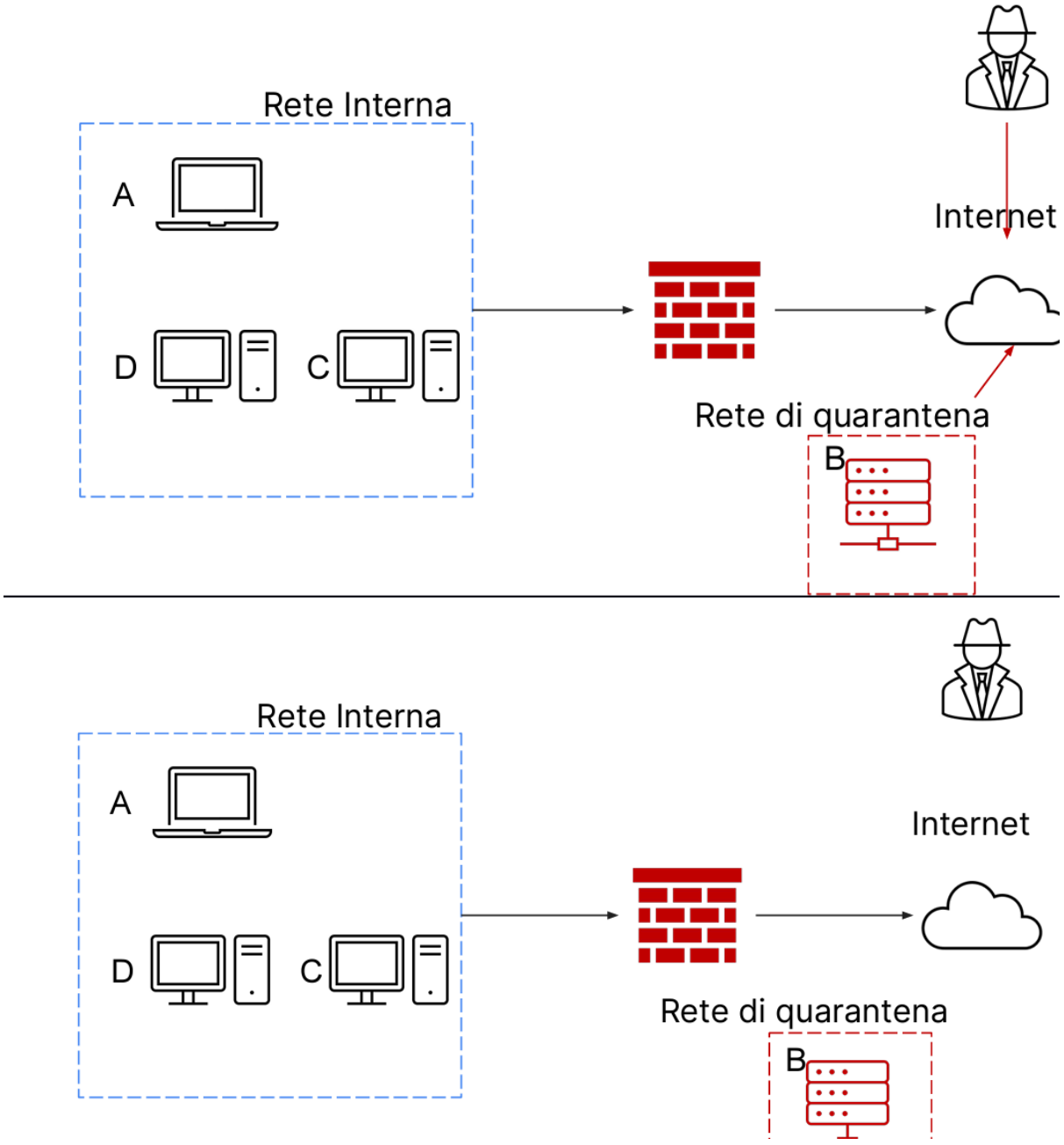
Destroy

Destroy comporta la distruzione fisica del supporto di memorizzazione, garantendo che i dati non possano essere recuperati in alcun modo. Le tecniche di destroy includono:

- Frantumazione dei dischi.
- Incenerimento.
- Uso di strumenti di distruzione certificati.

Questi passaggi dettagliati, accompagnati dai disegni, illustrano in modo chiaro e comprensibile le azioni intraprese per gestire e mitigare l'incidente di sicurezza, proteggendo così l'integrità della nostra rete e dei nostri dati aziendali.

SCREENSHOT


Rete Interna
A
D
C
Internet
Rete di quarantena
B
Rete Interna
A
D
C
Internet
Rete di quarantena
B