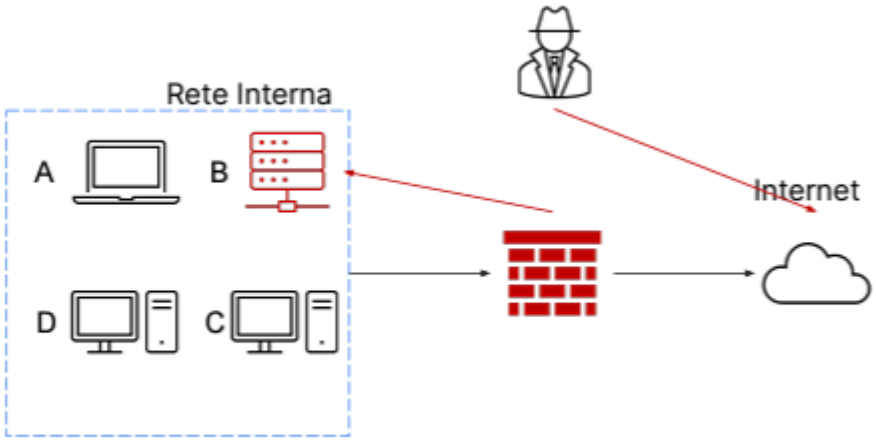
Report sull'Incident Response

Data 1/02/24

Introduzione

Nel panorama sempre più interconnesso della sicurezza informatica, la minaccia di intrusioni malevole rappresenta una sfida costante per la sicurezza delle reti e dei sistemi informatici. In questo contesto, l'incidente in esame rivela una vulnerabilità significativa all'interno del sistema B, un robusto database per lo storage. Il nostro scenario si apre con l'allarmante constatazione che il sistema è stato compromesso integralmente da un attaccante, il quale ha saputo sfruttare le vie di accesso tramite internet.

Lo scenario in esame è il seguente:



Abbiamo lavorato mentre l'attacco era in corso. Gli obiettivi del lavoro sono stati essenzialmente due:

- Mostrare le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Analisi dell'Incidente

Misure di Isolamento e Rimozione

I) Isolamento:

L'obiettivo primario è implementare un efficace processo di isolamento per contenere la diffusione delle minacce all'interno del sistema e prevenire ulteriori danni.

Questo richiede l'adozione di misure tempestive e mirate per separare il sistema B compromesso dalla rete e da altri asset critici. Attraverso l'implementazione di tecniche di isolamento è possibile limitare l'accesso dell'attaccante e a prevenire la propagazione dell'attacco a sistemi adiacenti.

II) Rimozione del Sistema B Infetto:

L'obiettivo successivo consiste nell'eseguire una rimozione completa e sicura del sistema B infetto.

In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata. Questo processo richiede un'analisi forense approfondita per identificare il malware e gli artefatti correlati, garantendo che ogni traccia dell'attacco sia completamente eliminata.

Questa attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette usb compromesse. La rimozione deve essere eseguita con precisione per evitare danni collaterali e preservare eventuali prove digitali che potrebbero essere utili nelle fasi successive dell'indagine. La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso. Una lista dettagliata delle attività da seguire per macro-casistica deve essere elencata nei «playbooks».

Spiegazione delle misure adottate per la pulizia sicura delle informazioni sensibili

Spiegazione della Differenza tra Purge e Destroy nell'Eliminazione delle Informazioni Sensibili

Purge (Pulizia):

Il termine "purge" denota il processo di pulizia sicura delle informazioni sensibili dal sistema o dai dispositivi compromessi. Durante questa fase, vengono adottate misure per sovrascrivere in modo sicuro i dati sensibili, garantendo che siano irreversibilmente cancellati e non possano essere recuperati. Questa procedura consente di mantenere il supporto di archiviazione fisico o logico intatto, ma libera i dati da qualsiasi traccia di informazioni riservate o potenzialmente dannose.

Destroy (Distruzione):

Al contrario, il termine "destroy" implica un approccio più radicale, che prevede la distruzione fisica del supporto di archiviazione, come ad esempio i dischi rigidi. In questo caso, la sicurezza delle informazioni è garantita mediante la demolizione fisica del mezzo di archiviazione. Questa misura è spesso adottata quando la protezione delle informazioni è di massima priorità e non vi è alcuna necessità di conservare fisicamente il supporto di archiviazione.

In entrambi i casi, la scelta tra "purge" e "destroy" dipende dalle esigenze specifiche di sicurezza dell'organizzazione e dalle leggi e normative applicabili che governano la gestione delle informazioni sensibili. La decisione deve essere ponderata, considerando attentamente gli aspetti legali, etici e pratici relativi alla gestione delle informazioni sensibili durante e dopo un incidente di sicurezza.

Conclusioni

In conclusione, la gestione efficace di questo incidente ha richiesto una combinazione di competenze forensi, tempestività nell'azione e una valutazione oculata delle opzioni di eliminazione delle informazioni sensibili. Questo report sottolinea l'importanza di piani di risposta agli incidenti ben definiti, inclusi protocolli di isolamento, rimozione e gestione sicura delle informazioni sensibili, per preservare la sicurezza e l'integrità dei sistemi informatici.