FACOLTATIVO

1. Intervento tempestivo sul sistema infetto

La prima cosa che farei è isolare immediatamente il computer infetto, staccandolo dalla rete, sia quella aziendale che internet, per evitare che il malware si diffonda ad altri dispositivi. WannaCry si propaga rapidamente sfruttando una vulnerabilità nel protocollo SMB di Windows; quindi, isolare il sistema è cruciale per fermare l'infezione.

Se possibile, spegnerei il computer o lo scollegherei dalla rete elettrica. Questo passo può fermare qualsiasi attività del malware e prevenire ulteriori danni o la crittografia di più file.

Prima di procedere ulteriormente, farei un'analisi dell'infezione per capire l'entità del danno: quali file sono stati criptati e se altre parti della rete sono state compromesse. Conoscere l'estensione dell'infezione mi aiuterà a scegliere la migliore strategia di recupero.

2. Possibili soluzioni per mettere in sicurezza il sistema

2.1 Ripristino da backup:

Se ci fossero backup disponibili, potrei ripristinare il sistema e i dati a uno stato precedente all'infezione. Questo è un metodo rapido e garantisce la rimozione completa del malware, ma c'è il rischio di perdere dati non inclusi nei backup. Inoltre, se i backup sono obsoleti o compromessi, questa opzione potrebbe non funzionare.

2.2 Installazione di patch e aggiornamenti:

Applicherei tutte le patch di sicurezza necessarie per Windows 7, in particolare quella (MS17-010) che risolve la vulnerabilità sfruttata da WannaCry. Questo aiuterà a proteggere il sistema da future infezioni simili ed è facile da implementare. Tuttavia, questa soluzione non rimuove il malware già presente e, dato che Windows 7 è un sistema operativo obsoleto, potrebbe non offrire una protezione completa.

2.3 Formattazione e reinstallazione del sistema operativo:

Un'opzione drastica, ma efficace, sarebbe formattare completamente il sistema e reinstallare il sistema operativo. Questo garantirebbe la rimozione completa del malware e mi permetterebbe di ripartire da zero con un sistema pulito. Però, è un processo lungo e richiede di reinstallare tutti i dati e le applicazioni, con il rischio di perdere informazioni se non ci sono backup recenti.

2.4 Rimozione del malware con strumenti specifici:

Potrei anche utilizzare software antivirus o strumenti specializzati per rimuovere WannaCry dal sistema infetto. Questa soluzione è meno invasiva rispetto alla formattazione e può essere fatta rapidamente senza la necessità di reinstallare tutto. Tuttavia, non c'è garanzia che il malware venga rimosso completamente, e potrebbero rimanere vulnerabilità.

2.5 Sostituzione del sistema operativo con una versione più sicura:

Aggiornare il sistema a una versione più recente di Windows, come Windows 10, è un'altra opzione che considererei. Questo offrirebbe una protezione migliore contro attacchi futuri e darebbe accesso a nuove funzionalità di sicurezza. Però, potrebbe essere necessario formare il personale all'uso del nuovo sistema operativo, e alcuni software aziendali più datati potrebbero non essere compatibili.

3. Il contributo di Marcus Hutchins alla risoluzione di WannaCry

Un aspetto importante da ricordare è che l'infezione da WannaCry è stata fermata grazie all'intervento di Marcus Hutchins, un ricercatore di sicurezza. Hutchins ha scoperto un "kill switch" nel codice del malware, una sorta di interruttore che, una volta attivato, bloccava la diffusione di WannaCry. Ha notato che il malware tentava di contattare un dominio web non registrato. Hutchins ha quindi acquistato e registrato quel dominio, attivando involontariamente il kill switch e fermando la diffusione del malware su scala globale.

Questo episodio evidenzia quanto sia importante monitorare il comportamento del malware e comprendere il suo funzionamento. Anche se registrare un dominio non è una soluzione diretta per un'infezione specifica, l'approccio di Hutchins ha bloccato la diffusione ulteriore di WannaCry, dando alle aziende il tempo di mettere in sicurezza i propri sistemi.

4. Valutazione dei pro e contro delle opzioni

- Ripristino da backup: È rapido e risolutivo, ma c'è il rischio di perdere dati se i backup non sono aggiornati.
- Installazione di patch e aggiornamenti: Protezione migliorata e facile da implementare, ma non risolve il problema dell'infezione attuale e la protezione su Windows 7 potrebbe essere limitata.
- Formattazione e reinstallazione del sistema operativo: Sicurezza garantita e sistema pulito, ma è un processo lungo e c'è il rischio di perdita di dati.
- Rimozione del malware con strumenti specifici: È meno invasivo e veloce, ma la rimozione non è sempre garantita e potrebbero restare delle vulnerabilità.
- Sostituzione del sistema operativo con una versione più sicura: Offre maggiore sicurezza e nuove funzionalità, ma richiede aggiornamenti software e formazione del personale.

5. Raccomandazione finale

Dopo aver valutato i pro e i contro di ciascuna opzione, sceglierei la strategia migliore in base al contesto dell'azienda. Considererei la criticità dei dati, la disponibilità di backup, il budget, e le competenze tecniche del team.

6. Piano di prevenzione per il futuro

Per evitare che si ripeta una situazione simile, è essenziale implementare un piano di prevenzione. Questo dovrebbe includere:

- Backup regolari e sicuri: Mi assicurerei che i backup siano sempre aggiornati e protetti.
- Aggiornamenti regolari e gestione delle patch: Mantengo tutti i sistemi operativi e i software aggiornati con le ultime patch di sicurezza.
- Formazione del personale: Educarei il personale sui rischi del malware e sulle buone pratiche di sicurezza informatica.
- Utilizzo di sistemi operativi supportati: Passerei a versioni di Windows che ricevano ancora aggiornamenti di sicurezza.

Seguendo questa struttura, posso affrontare in modo dettagliato e organizzato l'infezione da WannaCry, mettendo in sicurezza il sistema infetto e prevenendo future minacce.