Esercizio: Infezione malware WannaCry

Intervento immediato sul sistema infetto->

Isolamento del Sistema:

> *Disconnettere immediatamente il computer dalla rete: Questo impedisce al malware di propagarsi ad altri dispositivi sulla stessa rete.*
> *Spegnere il computer infetto: Se disconnetterlo dalla rete non è possibile o non è sufficiente, spegnere il sistema può fermare l'ulteriore cifratura di file.*

Valutazione dell'infezione:

> *Identificare e documentare i segni dell'infezione: Verificare messaggi di riscatto, file criptati e altre evidenze dell'infezione WannaCry.*
> *Informare il team di sicurezza e la direzione aziendale: Assicurarsi che tutti i livelli appropriati dell'organizzazione siano a conoscenza della situazione.*

Elenco delle varie possibilità di messa in sicurezza del sistema ->

- ❖ Ripristino da Backup

Pro:

- *Ripristina i dati al loro stato precedente all'infezione.*
- *Minimizza la perdita di dati se i backup sono aggiornati.*

Contro:

- *Richiede backup regolari e aggiornati.*
- *Il processo di ripristino può essere lungo e può causare tempi di inattività.*
-

- ❖ Rimozione del Malware e Riparazione del Sistema

Pro:

- *Rimuove il malware senza perdita di dati se la rimozione è effettuata correttamente.*
- *Mantiene il sistema operativo e le configurazioni attuali.*

Contro:

- *Può essere difficile garantire la completa rimozione del malware.*
- *Potrebbero rimanere vulnerabilità sfruttabili in futuro.*

❖ Reinstallazione del Sistema Operativo

Pro:

- *Garantisce la completa rimozione del malware.*
- *Il sistema torna ad uno stato "pulito" e aggiornato.*

Contro:

- *Comporta la perdita di tutti i dati e le configurazioni non salvati.*
- *Necessita di tempo per reinstallare e riconfigurare tutte le applicazioni.*

❖ Aggiornamento del Sistema Operativo e Applicazione di Patch

Pro:

- *Rende il sistema meno vulnerabile a future infezioni.*
- *Può essere effettuato insieme alla rimozione del malware o alla reinstallazione.*

Contro:

- *Non garantisce la rimozione dell'infezione attuale.*
- *Richiede verifiche per garantire la compatibilità delle applicazioni esistenti.*

❖ Controllo e Monitoraggio Costante

Pro:

- *Permette di rilevare e rispondere rapidamente a nuove minacce.*
- *Implementazione di strumenti di sicurezza come antivirus, firewall e IDS/IPS.*

Contro:

- *Richiede risorse e tempo per la configurazione e il monitoraggio continuo.*
- *Non è una soluzione definitiva, ma una misura di prevenzione continua.*

Valutazione delle possibilità ->

- ❖ Ripristino da Backup

- *Pro: Rapido ritorno alla normalità con minimi dati persi se i backup sono aggiornati.*
- *Contro: Inefficace se i backup non sono recenti o sono stati anch'essi compromessi.*

- ❖ Rimozione del Malware e Riparazione del Sistema

- *Pro: Mantiene i dati attuali e le configurazioni.*
- *Contro: Non sempre garantisce la completa eliminazione del malware.*

- ❖ Reinstallazione del Sistema Operativo

- *Pro: Pulisce completamente il sistema.*
- *Contro: Comporta la perdita di dati non salvati e richiede tempo per la reinstallazione.*

- ❖ Aggiornamento del Sistema Operativo e Applicazione di Patch

- *Pro: Previene future infezioni simili.*
- *Contro: Non rimuove l'infezione esistente.*

- ❖ Controllo e Monitoraggio Costante

- *Pro: Migliora la sicurezza a lungo termine.*
- *Contro: Non risolve l'infezione corrente e richiede risorse continue.*

Conclusione
La messa in sicurezza del sistema dopo un'infezione da WannaCry richiede un approccio multifase. L'isolamento immediato e l'analisi iniziale sono cruciali per prevenire ulteriori danni. Le soluzioni migliori comprendono il ripristino da backup e la reinstallazione del sistema operativo, integrate con un aggiornamento del sistema e un piano di monitoraggio continuo per prevenire future infezioni.