Traccia: infezione malware

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 è stato infettato dal malware WannaCry.

Cosa fai per mettere in sicurezza il tuo sistema?

Consegna:

- Per prima cosa occorre intervenire tempestivamente sul sistema infetto
- In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
- Per ogni possibilità valutare i pro e i contro

Svolgimento :

WannaCry è un malware che cripta i file e chiede un riscatto per decriptarli, diffondendosi tramite una vulnerabilità di Windows. Patch di sicurezza e backup sono essenziali per la prevenzione.

Per affrontare un'infezione da malware WannaCry su un computer Windows 7, prepareremo un elenco delle possibilità di messa in sicurezza del sistema, valutandone i pro e i contro.

- **Isolare il Sistema Infetto**
  - **Passo**: Scollega immediatamente il computer dalla rete per prevenire ulteriori propagazioni del malware.
  - **Pro**: Impedisce che il malware si diffonda ad altri dispositivi sulla rete.
  - **Contro**: Il computer infetto non sarà più accessibile per operazioni di pulizia o backup da remoto.
- **Disabilitare la Connessione Wi-Fi/Bluetooth**
  - **Passo**: Disattiva tutte le connessioni wireless per evitare ulteriori infezioni.
  - **Pro**: Maggior isolamento del dispositivo.
  - **Contro**: Può complicare la comunicazione per le operazioni di recovery se non ci sono alternative di connessione sicura.
- **Verificare la Presenza di Backup Recenti**

- **Passo**: Verifica la disponibilità di backup recenti e integri dei dati importanti.
- **Pro**: Permette un recupero più rapido dei dati senza necessità di decriptare quelli cifrati dal malware.
- **Contro**: Se i backup non sono aggiornati, si rischia di perdere dati recenti.

1. Rimuovere il Malware e Recuperare il Sistema

- **Passaggi**:
  - Utilizzare un software di rimozione malware affidabile.
  - Scansionare e pulire il sistema.
  - Applicare patch di sicurezza e aggiornamenti.
- **Pro**:
  - Può risolvere il problema senza necessità di reinstallare il sistema operativo.
  - Mantiene le configurazioni e le installazioni software correnti.
- **Contro**:
  - Non garantisce la rimozione completa del malware.
  - Il sistema potrebbe rimanere instabile o vulnerabile.

2. Ripristinare da Backup

- **Passaggi**:
  - Ripristinare i dati e il sistema operativo da un backup precedente all'infezione.
  - Applicare tutte le patch di sicurezza.
- **Pro**:
  - Ripristina il sistema a uno stato sicuro e funzionante.
  - Garantisce la rimozione del malware se il backup è integro.
- **Contro**:
  - Potrebbe comportare la perdita di dati non salvati dopo l'ultimo backup.
  - Richiede tempo per il ripristino e la verifica dei dati.

3. Reinstallare il Sistema Operativo

- **Passaggi**:

    - Formattare il disco rigido e reinstallare Windows 7.
    - Reinstallare tutti i software necessari.
    - Applicare patch di sicurezza e aggiornamenti.
    - Ripristinare i dati dai backup.
- **Pro**:
    - Garantisce un sistema pulito e privo di malware.
    - Elimina tutte le vulnerabilità presenti sul sistema infetto.
- **Contro**:
    - Processo lungo e complesso.
    - Necessità di reinstallare e riconfigurare tutti i programmi.

- Valutazione dei Pro e dei Contro

Rimozione del Malware

- **Pro**: Rapido, mantiene la configurazione corrente.
- **Contro**: Non sempre efficace, potenziale instabilità.

Ripristino da Backup

- **Pro**: Restituisce un sistema funzionante e sicuro.
- **Contro**: Possibile perdita di dati recenti, tempo necessario per il ripristino.

Reinstallazione del Sistema Operativo

- **Pro**: Sistema completamente pulito e sicuro.
- **Contro**: Richiede molto tempo, complessità di reinstallazione e configurazione.

Raccomandazioni Finali

1. Isolare immediatamente il sistema infetto per prevenire la diffusione del malware.
2. Valutare la disponibilità e l'integrità dei backup per decidere tra ripristino o reinstallazione.
3. Applicare tutte le patch di sicurezza e aggiornamenti per prevenire future infezioni.

Prevenzione a Lungo Termine

- Aggiornare regolarmente il sistema operativo e il software.

- Utilizzare soluzioni di sicurezza avanzate, come antivirus e firewall.
- Eseguire backup regolari e verificarne l'integrità.
- Formare il personale sulla sicurezza informatica e sulle migliori pratiche di prevenzione.