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

1. Isolare il computer infetto dalla rete: La prima azione urgente sarebbe isolare il computer infetto dalla rete aziendale per impedire la propagazione del malware ad altri dispositivi.

2. Arrestare il processo del malware: Utilizzerei il Task Manager o un software di gestione dei processi per arrestare il processo del malware, se possibile. Questo potrebbe impedire al malware di continuare a danneggiare il sistema o di diffondersi ulteriormente.

3. Avviare una scansione antivirus approfondita: Utilizzerei un software antivirus aggiornato per eseguire una scansione completa del sistema al fine di individuare e rimuovere tutti i file e le componenti del malware WannaCry presenti sul computer.

4. Applicare le patch di sicurezza: Assicurerei che il sistema operativo Windows 7 abbia tutte le patch di sicurezza più recenti installate, compresa la patch MS17-010, che è stata rilasciata da Microsoft per mitigare la vulnerabilità utilizzata da WannaCry.

5. Eseguire un ripristino da un backup sicuro: Se disponibile, ripristinerei il sistema da un backup recente e pulito per eliminare completamente il malware e ripristinare il sistema a uno stato noto sicuro. È importante assicurarsi che il backup sia stato effettuato prima dell'infezione da WannaCry.

6. Verificare l'integrità dei file di sistema: Dopo aver rimosso il malware e applicato le patch di sicurezza, eseguirei una scansione per verificare l'integrità dei file di sistema critici per assicurarsi che non siano stati danneggiati o compromessi durante l'infezione da WannaCry.

7. Implementare misure di sicurezza aggiuntive: Una volta ripristinato il sistema, implementerei misure di sicurezza aggiuntive come aggiornamenti regolari del software, utilizzo di firewall e software di protezione endpoint, e istruirei gli utenti su pratiche di sicurezza informatica migliori.

8. Monitorare l'attività di rete: Monitorerei attentamente l'attività di rete per individuare eventuali segni di ulteriori attacchi o infezioni da malware e adotterei misure preventive appropriate per mitigare tali minacce.

9. Educare gli utenti: Infine, educare gli utenti sull'importanza di pratiche di sicurezza informatica, come l'evitare di aprire allegati email sospetti o fare clic su link non attendibili, per ridurre il rischio di futuri attacchi malware.

1. Isolare il computer infetto dalla rete: Questo aiuterà a prevenire la diffusione del malware ad altri dispositivi nella rete.
- Pro: Limita la diffusione del malware.
- Contro: Potrebbe interrompere temporaneamente l'accesso alla rete per il computer infetto, compromettendo la produttività.

2. Avviare una scansione antivirus approfondita: Utilizzare un software antivirus aggiornato per individuare e rimuovere il malware WannaCry.

- Pro: Può individuare e rimuovere il malware in modo efficace.
- Contro: Potrebbe richiedere tempo per completare la scansione, durante il quale il sistema potrebbe essere vulnerabile.

3. Applicare patch di sicurezza: Assicurarsi che il sistema operativo Windows 7 abbia tutte le patch di sicurezza più recenti installate, inclusa la patch per la vulnerabilità utilizzata da WannaCry (MS17-010).

- Pro: Corregge la vulnerabilità che ha permesso l'infezione.
- Contro: Potrebbe essere necessario riavviare il sistema e applicare le patch potrebbe richiedere del tempo.

4. Ripristinare da un backup sicuro: Ripristinare il computer da un backup anteriore all'infezione per eliminare completamente il malware e ripristinare i dati non compromessi.

- Pro: Rimuove completamente il malware e ripristina il sistema a uno stato noto sicuro.
- Contro: Potrebbe causare la perdita di dati recenti se il backup non è stato eseguito di recente.

5. Monitoraggio dell'attività di rete: Monitorare l'attività di rete per individuare eventuali tentativi di comunicazione del malware con server di comando e controllo.

- Pro: Può rilevare l'attività del malware e aiutare a identificare ulteriori punti di infezione.
- Contro: Potrebbe richiedere strumenti specializzati e competenze per l'analisi dei dati di rete.