Traccia:
Infezione malware
Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 ed 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

Intervento Tempestivo sul Sistema Infetto:

Isolamento del Computer Infetto:
- *Pro:* Isolare immediatamente il computer colpito per prevenire la diffusione del malware alla rete.
- *Contro:* Potrebbe interrompere temporaneamente l'accesso ai dati critici per l'utente.

Disattivazione delle Connessioni di Rete:
- *Pro:* Ridurre la possibilità di diffusione del malware attraverso la rete.
- *Contro:* Potrebbe impedire l'accesso a risorse condivise e aggiornamenti di sicurezza.

Spegnimento del Sistema:
- *Pro:* Arrestare il malware e impedire ulteriori danni.
- *Contro:* Potrebbe causare la perdita di dati non salvati e interrompere le attività aziendali.

Messa in Sicurezza del Sistema:

Aggiornamento del Sistema Operativo:
- *Pro:* Installare gli ultimi aggiornamenti di sicurezza per correggere vulnerabilità.
- *Contro:* Potrebbe richiedere tempo e potrebbe essere necessario riavviare il sistema.

Installazione di un Software Antimalware:

- *Pro:* Rilevare e rimuovere il malware, fornendo protezione in tempo reale.
- *Contro:* Potrebbe rallentare le prestazioni del sistema e richiedere risorse.

Backup e Ripristino dei Dati:

- *Pro:* Garantire la disponibilità dei dati senza rischi di perdita permanente.
- *Contro:* Potrebbe richiedere tempo, e i dati del backup potrebbero anch'essi essere compromessi.

Formazione degli Utenti:

- *Pro:* Sensibilizzare gli utenti sui rischi di sicurezza e sull'importanza di comportamenti sicuri.
- *Contro:* Potrebbe richiedere tempo per implementare la formazione e potrebbe essere difficile modificare le abitudini degli utenti.

Monitoraggio del Traffico di Rete:

- *Pro:* Identificare comportamenti sospetti e attività malevole nella rete.
- *Contro:* Potrebbe richiedere risorse significative e generare falsi positivi.

Analisi Forense:

- *Pro:* Identificare l'origine e il percorso del malware per prevenire futuri attacchi.
- *Contro:* Può richiedere competenze specializzate e tempo considerevole.

Implementazione di Politiche di Sicurezza:

- *Pro:* Ridurre le vulnerabilità attraverso restrizioni e regole di sicurezza.
- *Contro:* Potrebbe essere difficile bilanciare la sicurezza con la produttività.

Upgrade del Sistema Operativo:

- *Pro:* Migliorare la sicurezza usufruendo di funzionalità avanzate nelle versioni più recenti.
- *Contro:* Potrebbe richiedere investimenti significativi e la compatibilità con le applicazioni esistenti potrebbe essere un problema.

Gestione delle Password:

- *Pro:* Rafforzare l'accesso al sistema tramite password robuste e policy di gestione delle credenziali.
- *Contro:* Potrebbe causare problemi di usabilità e richiedere la modifica delle pratiche attuali.

Analisi delle Vulnerabilità del Software:

- *Pro:* Identificare e correggere le vulnerabilità del software installato.
- *Contro:* Può richiedere tempo per eseguire l'analisi e ottenere patch o aggiornamenti.

In conclusione, una risposta efficace a un'incidente di malware richiede un approccio integrato, combinando interventi tempestivi con misure di sicurezza a lungo termine. La valutazione dei pro e contro di ciascuna opzione è essenziale per adottare un approccio equilibrato che minimizzi i rischi e protegga l'azienda nel lungo periodo.