M4 D3

ESERCIZIO 2

COMPUTER CON WINDOWS7 INFETTATO DA MALWARE WANNACRY.
COME METTO IN SICUREZZA IL SISTEMA?

- **INTERVENIRE SUL SISTEMA INFETTO:**

Da limitare la diffusione del malware e proteggere i dati sensibili dell'azienda.

1. **Isolamento: Isolare il computer infetto dalla rete aziendale. Disconnetterlo dalla rete per prevenire la propagazione del malware ad altri dispositivi.**
2. **Disconnessione: Computer deve essere disconnesso da Internet per impedire al malware di comunicare con il server.**
3. **Identificazione del malware: Utilizzare un software antivirus aggiornato per eseguire una scansione completa del sistema e individuare il malware WannaCry. Il software dovrebbe rilevare e segnalare la presenza del malware.**
4. **Rimozione del malware: Seguire le istruzioni fornite dall' antivirus per rimuovere il malware dal sistema.**
5. **Analisi delle vulnerabilità: Dopo aver rimosso il malware, è importante condurre un'analisi approfondita delle vulnerabilità presenti nel sistema. Cercare altre possibili vie di ingresso per i malware e le vulnerabilità che potrebbero essere state sfruttate. Prendere le misure necessarie per rafforzare la sicurezza del sistema.**
6. **Ripristino del sistema: Ripristinare il sistema da un punto di ripristino precedente all'infezione. Può aiutare a eliminare eventuali modifiche indesiderate apportate dal malware e ripristinare il sistema a uno stato precedente.**

Potrebbe essere necessario coinvolgere un esperto di sicurezza informatica per valutare l'entità dell'infezione, identificare le cause e fornire un'assistenza mirata.

- **PREPARARE ELENCO POSSIBILITA' DI MESSA IN SICUREZZA:**

Elenco delle possibili misure per mettere in sicurezza il sistema dopo un attacco di malware:

1. **Aggiornamenti regolari del sistema operativo: Installare tutti gli aggiornamenti di sicurezza disponibili per il sistema operativo. Includere patch, correzioni e aggiornamenti critici forniti dal produttore del sistema operativo. Considerare anche l'upgrade a un sistema operativo più recente e supportato.**
2. **Aggiornamenti del software e delle applicazioni: Mantenere sempre aggiornati tutti i software e le applicazioni installate sul sistema. I malware sfruttano vulnerabilità presenti nel software obsoleto per infiltrarsi nei sistemi. Applicare regolarmente gli aggiornamenti forniti dai produttori del software.**
3. **Firewall e soluzioni di protezione: Configurare un firewall sul sistema per monitorare e controllare il traffico di rete in entrata e in uscita. Utilizzare anche soluzioni di sicurezza aggiuntive come antivirus, antispyware e antimalware per proteggere il sistema da minacce note e sconosciute.**
4. **Backup regolari dei dati: Eseguire regolarmente backup completi dei dati importanti del sistema. Mantenere i backup in una posizione sicura e separata dal sistema principale. In caso di un attacco o di un'altra forma di perdita dei**

dati, i backup possono essere utilizzati per ripristinare i file e le informazioni importanti.

5. **Educazione e consapevolezza degli utenti: Formare gli utenti dell'azienda sulla sicurezza informatica e sensibilizzarli sugli aspetti chiave come l'apertura di allegati o link sospetti, l'uso di password robuste, la segnalazione di attività sospette e l'importanza della sicurezza dei dati.**
6. **Monitoraggio del sistema: Implementare strumenti di monitoraggio del sistema che possono rilevare attività anomale o sospette. Monitorare regolarmente il sistema per individuare eventuali segni di un nuovo attacco o di un'eventuale reinfezione.**
7. **Accesso privilegiato e controllo degli account: Limitare l'accesso privilegiato solo a coloro che ne hanno effettivamente bisogno. Utilizzare politiche di gestione degli account per garantire che gli utenti abbiano solo i privilegi necessari per svolgere le loro attività. Creare password complesse e incoraggiare l'uso dell'autenticazione a due fattori.**
8. **Test di penetrazione e audit di sicurezza: Effettuare test di penetrazione regolari e audit di sicurezza per identificare le vulnerabilità nel sistema e nelle reti. Questo aiuterà a individuare potenziali punti deboli e a prendere le misure correttive necessarie per rafforzare la sicurezza.**

– **PER OGNI POSSIBILITA' DA VALUTARE I PRO E I CONTRO:**

Valutazione dei potenziali vantaggi e svantaggi delle diverse misure:

1. **Aggiornamenti regolari del sistema operativo:**

   • Pro: Gli aggiornamenti regolari del sistema operativo garantiscono l'applicazione delle patch di sicurezza più recenti, che possono correggere vulnerabilità note e migliorare la resistenza del sistema agli attacchi.
   • Contro: Gli aggiornamenti del sistema operativo potrebbero richiedere tempo e interrompere temporaneamente l'utilizzo del sistema. Inoltre, se il sistema operativo è obsoleto, potrebbe non essere più supportato dal produttore e non ricevere aggiornamenti di sicurezza.

2. **Aggiornamenti del software e delle applicazioni:**

   • Pro: Gli aggiornamenti del software correggono spesso vulnerabilità di sicurezza note e migliorano la stabilità e le prestazioni delle applicazioni. Mantenere il software aggiornato riduce il rischio di exploit da parte dei malware.
   • Contro: Gli aggiornamenti del software potrebbero richiedere tempo e potenzialmente causare incompatibilità con altre applicazioni o richiedere l'adattamento dei processi aziendali. Inoltre, alcuni software potrebbero richiedere licenze o costi aggiuntivi per gli aggiornamenti.

3. **Firewall e soluzioni di protezione:**

   • Pro: Un firewall e le soluzioni di sicurezza aggiuntive possono rilevare e bloccare il traffico di rete dannoso o sospetto. Proteggono il sistema da minacce note e sconosciute e possono fornire una difesa in profondità.
   • Contro: Le soluzioni di sicurezza potrebbero richiedere risorse di sistema e

possono generare falsi positivi che richiedono l'intervento dell'amministratore di sistema per valutarli. Non possono garantire una protezione al 100%.

4. **Backup regolari dei dati:**

   • Pro: I backup regolari dei dati proteggono le informazioni aziendali da perdite causate da attacchi informatici, guasti hardware o errori umani. Consentono il ripristino dei dati in caso di incidente.
   • Contro: I backup richiedono spazio di archiviazione aggiuntivo e possono richiedere tempo per il processo di backup e ripristino. Se i backup non vengono eseguiti correttamente o non sono protetti, potrebbero essere soggetti a accesso non autorizzato o corruzione.

5. **Educazione e consapevolezza degli utenti:**

   • Pro: Un'adeguata formazione sulla sicurezza informatica può migliorare la consapevolezza degli utenti e ridurre il rischio di azioni non sicure come aprire allegati o cliccare su link sospetti.
   • Contro: L'educazione degli utenti richiede tempo e risorse per la formazione e il mantenimento della consapevolezza. Con una formazione non adeguata, gli utenti potrebbero commettere errori o essere ingannati da phishing.

6. **Monitoraggio del sistema:**

   • Pro: Il monitoraggio del sistema può rilevare attività sospette o anomalie che potrebbero indicare un nuovo attacco o una reinfezione. Può consentire una risposta tempestiva e limitare i danni.
   • Contro: Il monitoraggio del sistema richiede risorse di sistema per l'esecuzione degli strumenti di monitoraggio e l'analisi dei dati. Inoltre, la configurazione e l'interpretazione dei risultati possono richiedere competenze specialistiche.

7. **Accesso privilegiato e controllo degli account:**

   • Pro: Limitare l'accesso privilegiato e controllare gli account riduce il rischio di abusi o accessi non autorizzati.
   • Contro: La gestione degli account richiede un'adeguata pianificazione e un processo di amministrazione degli account ben strutturato. Potrebbe essere necessario bilanciare la sicurezza con la praticità e l'efficienza operativa.

8. **Test di penetrazione e audit di sicurezza:**

   • Pro: I test di penetrazione e gli audit di sicurezza identificano le vulnerabilità e consentono l'adozione di misure correttive prima che siano sfruttate dagli attaccanti. Aiutano a migliorare la sicurezza complessiva dell'ambiente.
   • Contro: I test di penetrazione e gli audit di sicurezza richiedono tempo e risorse specializzate. Possono generare costi aggiuntivi e possono rivelare problemi che richiedono tempo per essere risolti.

Valutare attentamente i pro e i contro delle diverse misure di sicurezza in base alle esigenze, alle risorse e al contesto dell'azienda.