ESERCITAZIONE W14D1(2)

EPICODE

Esercizio
Infezione malware

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

Per prima cosa, intervenire tempestivamente sul sistema infetto è fondamentale per limitare i danni e prevenire la diffusione del malware WannaCry. Ecco una serie di azioni da intraprendere:

1. Isolare il sistema infetto: Rimuovere immediatamente il computer dalla rete per prevenire la diffusione del malware ad altri dispositivi.

2. Disconnettere dalle risorse di rete: Interrompere ogni connessione di rete del sistema infetto, inclusi Wi-Fi e cavi Ethernet, per evitare la propagazione del malware su altri dispositivi.

3. Avviare una scansione antivirus e anti-malware: Utilizzare un software antivirus aggiornato per eseguire una scansione completa del sistema e rimuovere il malware WannaCry.

4. Applicare patch di sicurezza: Installare immediatamente tutte le patch di sicurezza disponibili per Windows 7, compresi i patch relativi alle vulnerabilità utilizzate da WannaCry per diffondersi. Microsoft ha rilasciato patch di sicurezza per proteggere contro WannaCry anche su Windows 7, nonostante il sistema operativo non sia più supportato ufficialmente.

5. Backup dei dati: Nel caso in cui il sistema sia stato danneggiato irreparabilmente, è importante disporre di un backup aggiornato dei dati importanti per ripristinarli una volta che il sistema è stato ripulito.

6. Monitoraggio attivo: Dopo aver eseguito la rimozione del malware, monitorare attentamente il sistema per individuare eventuali segni di reinfezione o altri comportamenti sospetti.

7. Educazione degli utenti: Fornire formazione agli utenti sull'importanza di non aprire allegati o link sospetti e sull'uso sicuro di Internet per prevenire future infezioni da malware.

Ora, per ogni possibilità, valutiamo i pro e i contro:

1. Isolare il sistema infetto:

- Pro: Impedisce la diffusione del malware ad altri dispositivi.

- Contro: Potrebbe interrompere temporaneamente l'accesso alle risorse di rete necessarie per il lavoro.

2. Disconnettere dalle risorse di rete:

- Pro: Riduce il rischio di diffusione del malware.

- Contro: Potrebbe interrompere temporaneamente l'accesso a risorse di rete necessarie per il lavoro.

3. Avviare una scansione antivirus e anti-malware:

- Pro: Identifica e rimuove il malware dal sistema.

- Contro: Potrebbe richiedere del tempo e non sempre garantisce la completa rimozione del malware.

4. Applicare patch di sicurezza:

- Pro: Corregge le vulnerabilità utilizzate dal malware per infettare il sistema.

- Contro: Potrebbe essere necessario riavviare il sistema e potrebbe esserci il rischio di incompatibilità con altre applicazioni.

5. Backup dei dati:

- Pro: Assicura la disponibilità dei dati importanti in caso di danni al sistema.

- Contro: Richiede tempo e spazio di archiviazione aggiuntivo per eseguire e mantenere i backup.

6. Monitoraggio attivo:

- Pro: Aiuta a individuare tempestivamente eventuali reinfezioni o comportamenti sospetti.

- Contro: Richiede risorse umane per monitorare costantemente il sistema.

7. Educazione degli utenti:

- Pro: Riduce il rischio di future infezioni da malware attraverso azioni degli utenti.

- Contro: Potrebbe richiedere tempo e risorse per fornire formazione agli utenti.