WannaCry

W14D1 - Pratica (2)

Traccia:

infezione malware Esercizio 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:

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

Cos'è WannaCry?

WannaCry è un tipo di ransomware, un malware, che cifra i file sul computer della vittima e chiede un riscatto in Bitcoin per sbloccarli.
Il nome "Wanna Cry" deriva dal messaggio visualizzato sullo schermo delle vittime, che le invita a pagare il riscatto per riavere i propri file.

Come si diffonde?

WannaCry si diffondeva principalmente sfruttando una vulnerabilità nel sistema operativo Windows. Questa vulnerabilità, nota come Eternal Blue, era stata scoperta dalla NSA (National Security Agency) statunitense e poi resa pubblica da un gruppo di hacker noto come Shadow Brokers. Microsoft aveva rilasciato una patch per questa vulnerabilità un mese prima dell'attacco, ma molti sistemi non erano stati aggiornati.

Come funziona?

1. Infezione iniziale:
WannaCry si diffonde tramite e-mail di phishing o utilizzando la vulnerabilità Eternal Blue per entrare nei sistemi non aggiornati.

2. Cifratura dei File:
una volta infettato un sistema, il ransomware cripta i file dell'utente e aggiunge l'estensione ".WNCRY" ai file cifrati.

3. Richiesta di riscatto:
viene visualizzato un messaggio che chiede un riscatto in Bitcoin per decriptare i file. La somma richiesta era solitamente intorno ai 300-600 dollari.

4. Diffusione automatica:
WannaCry includeva un componente worm che gli permetteva di propagarsi automaticamente ad altri computer vulnerabili nella stessa rete.

Valutazione dei pro e contro

1. Intervento tempestivo sul sistema infetto
Il primo passo è agire prontamente per contenere il computer infetto dalla rete aziendale per impedire la diffusione del malware.
Isolamento del computer infetto dalla rete aziendale, questo è utile per prevenire la diffusione del malware. Inoltre, bisogna assicurarsi che gli dispositivi non siano collegati alla stessa rete per evitare ulteriori infezioni.

2. Aggiornamento del sistema operativo
Dopo aver contratto l'infezione iniziale, è importante implementare misure per migliorare la sicurezza del sistema e prevenire futuri attacchi.
Verificare e installare le patch di sicurezza più recenti rilasciate da Microsoft per proteggere il sistema dalle vulnerabilità sfruttate da WannaCry. Riavviare il sistema se richiesto.
Installare un software di sicurezza affidabile e aggiornato sul computer infetto per eseguire una scansione approfondita e rimuovere il malware WannaCry
Configurare e attivare un sistema di rilevamento delle minacce per analizzare costantemente le attività del sistema alla ricerca di eventuali segnali di attacchi informatici o comportamenti anomali.
Utilizzare strumenti di monitoraggio delle attività del sistema per rilevare comportamenti non autorizzati o anomalie, consentendo una risposta tempestiva alle minacce.