M4_W14D1(2)

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

WannaCry è un software malevolo appartenente alla famiglia dei Ransomware.
La particolarità dei ransomware risiede nella capacità di prendere in ostaggio l'intero sistema informatico crittografando tutti i dati contenuti al suo interno.
Le informazioni diventano inaccessibili per tutti gli utenti che vogliano utilizzare la macchina. L'unica soluzione apparente per questo tipo di software dannoso è il pagamento di un riscatto (appunto ransom) in cambio della chiave di decrittazione necessaria per ripristinare i file.
I malware di tipo Ransomware possono diffondersi attraverso una rete locale o tramite exploit di vulnerabilità nei servizi di condivisione di file. Questo significa che se un computer nella rete è infetto, c'è il rischio che il ransomware si diffonda ad altri computer collegati alla stessa rete.
Il malware in analisi, ovvero WannaCry, sfrutta una vulnerabilità nei sistemi Windows non aggiornati, servendosi di un exploit chiamato EternalBlue.

L'azienda colpita da WannaCry deve isolare l'host infetto per evitare che il malware possa diffondersi all'interno di tutta l'infrastruttura di rete rendendo inaccessibili anche altri host.

Su tutti i dispositivi non ancora infetti è necessario aggiornare il software (**) in maniera tempestiva.
****Fare lo stesso con firewall e antivirus.**

Eseguire un backup dei dati importanti in modo da poterli ripristinare nel caso in cui altri host vengano compromessi.

I rischi per il computer o la rete infetti da WannaCry sono davvero significativi e comprendono un fattore chiave per ogni azienda: Danni alla reputazione.

Bisogna valutare quanto i dati all'interno dell'host compromesso siano importanti e procedere dunque con un'analisi mirata che possa fornire dettagli mirati (anche in termini economici) per cercare di scongiurare la minaccia.

Bisogna ricordare che il pagamento del riscatto non garantisce in nessun modo il rilascio dei dati in ostaggio e potrebbe incoraggiare ulteriori attività criminali.
Alla luce di queste valutazioni bisognerebbe in primis scegliere un supporto professionale ed adottare misure preventive future.