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?

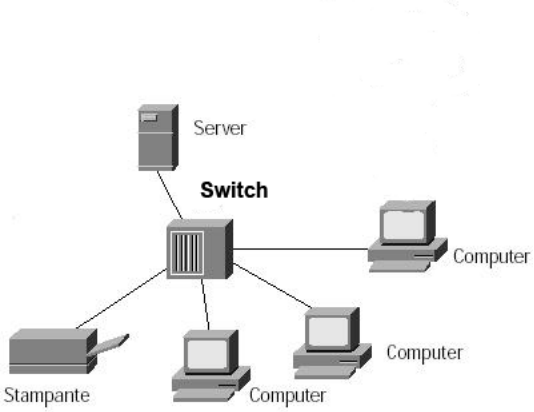
Consegna:

- 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

Svolgimento:

Si ipotizza un modello di rete semplice di una PMI dove esiste un'unica LAN aziendale. Abbiamo i PC dell'amministrazione e degli uffici che hanno Windows 10 oppure 11 mentre i PC dei macchinari tecnici anch'essi collegati alla medesima LAN utilizzano Windows 7. L'unico Server che svolge la funzione di spazio di condivisione e dove girano gli applicativi che sono extra singolo utente con lavoro specifico ma di utilità per tutta l'azienda (come ad esempio il gestionale ecc…)

Soluzione di Backup una Nas che viene acceso dal responsabile dell'ufficio prima della chiusura serale, fa il backup alle 22:00 e poi in automatico si spegne.



Analizzando il funzionamento di WannaCry si apprende che per la sua " installazione " non è necessario un intervento umano in quanto il malware sfrutta una debolezza del protocollo smb v1. Una volta che una macchina si è infettata il malware si diffonde a tutte le macchina Windows della rete che sfruttano il protocollo smb v1.

Per la ns rete target il protocollo smb v1 non è installato/abilitato di default sulle macchine Windows 10, quindi ci sono ottime probabilità che la parte amministrativa non venga infettata.

Diversa è invece la parte che riguarda il Windows Server 2008 ed i PC Windows 7.

La prima operazione da fare è l'isolamento dalla rete di tutte le macchine che sono state infettate o che potrebbero essere infette. Con la ns soluzione di backup siamo sempre aggiornati alla sera precedente ed il nas (ammesso che monti windows anche se poco probabile) era spento al momento dell'infezione.

Quindi con le macchine più nuove procediamo con un controllo di non infezione.

Le macchine che invece sono state infettate passeranno dalla fase di re installazione dei sistemi e dei programmi con annessa la fase di aggiornamento o dove non possibile con la disattivazione del protocollo smb in attesa di valutare soluzione di sostituzione macchine o aggiunta firewall ecc…

A completamento delle operazioni con verifiche di non presenza del codice malevolo possiamo andare a ricollegare l'intera rete.

Con questa soluzione abbiamo ripristinato il business al giorno precedente.

Cambiamenti:

Spostiamo il backup dalla soluzione fisica ad una cloud quale ad esempio One Drive / Share Point Microsoft dove viene salvato tutto il lavoro che andiamo a svolgere. Così avremo delegato alla Microsoft la gestione dei backup.

Tutte le Macchine che hanno software specifici che possono girare anche con Windows 10 e successivi vengono aggiornate / sostituite.

Se i fornitori del ns gestionale ci offrono una soluzione anche in cloud ci spostiamo, altrimenti andiamo ad aggiornare / sostituire la macchina server.

Spacchettiamo l'unica LAN in reti più piccole divise per reparti, così che possiamo usare router e firewall (anche software) per rendere un'eventuale infezione meno efficace.