W14D1 - Pratica (2)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 2 – Infezione malware

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

****

L'azienda Rossi è stata infetta dal virus Wanna Cray.

1. Per prima cosa si fa scollegare tutti i pc dalla rete cavo e wifi. Staccare anche i dispositivi come router, switch e eventuali connessioni di backup.

2. Una volta staccati, cerco di individuare il pc infettato per primo, quello che ha dato i primi sintomi, non è possibile in questo momento capire se ci sono altri pc infetti.

3. Valuto l'entità del problema, se il pc funziona ancora oppure se siamo già in una situazione critica.

4. Si identifica come possa essere entrato il virus nel sistema, Email, chiavette usb, file scaricati da internet, ecc…

5. Valuto un piano di difesa della rete, cerco di capire se altri pc possano aver lo stesso problema eseguendo una scansione approfondita della ricerca malware, virus e qualunque problema possano avere, con dei tool specifici, come Antivirus, software per la rimozione specifici e aggiorno tutti i sistemi alle versioni dei sistemi operativi più recenti (questo dove possibile).

6. Si elimina la macchina infetta, reinstallandola e recuperando il backup solo se sicuro dopo aver eseguito tutte le dovute precauzioni (Scan. antivirus, Scan. Malware, ecc..)

7. Si cerca di avviare alcuni pc per volta, e si analizzano tutti come il precedente punto

8. Aumento la sicurezza dei permessi con autenticazione a doppio fattore e faccio cambiare password a tutti.

9. Fatto questo si ripete la stessa cosa nei pc dedicati al Backup, per evitare che si sia fatta una copia, altrimenti il danno potrebbe diventare disastroso.

10. Rinforzo le difese del sistema per cercare di evitare lo stesso problema in futuro

11. Si cerca di eseguire una campagna di formazione aziendale, si spiega come individuare eventuali problemi di questo tipo e si forma il personale su come segnalare la problematica nel più breve tempo possibile.

12. Una volta messo in sicurezza, si cerca di tenere monitorata la rete per verificare un eventuale traffico di dati anomalo.

Cybersecurity Analyst 2023