Esercitazione WEEK 14 D1 (2)

Infezione malware

Ettore Farris - 12/02/2024

Descrizione sintetica

Traccia

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows 7 che 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.

Soluzioni

- **Cos'è Wannacry**

WannaCry (chiamato anche WanaCrypt0r 2.0), è un worm, di tipologia ransomware, responsabile di un'epidemia su larga scala avvenuta nel maggio 2017 su computer con Microsoft Windows. Questo malware cripta i file presenti sul computer al fine di chiedere un riscatto in criptovalute per decriptarli. Wannacry essendo un worm si propaga di macchina in macchina eseguendo del codice in automatico e sfruttando una vulnerabilità del protocollo SMBv1 (CVE-2017-0144) presenti in alcune versioni di Windows, come ad esempio Windows 7.

- **Soluzione 1: Aggiornamento del sistema**

Per rimediare alla vulnerabilità, basta aggiornare il sistema dal pannello di Controllo di Windows:

System Security check -—> Windows Update --> Install Updates.

Dopo aver scaricato gli aggiornamenti, isolare la macchina e staccando il cavo di rete o disabilitando il wifi.

- **Soluzione 2: Disabilitare il protocollo SMBv1**

Dato che il malware si propaga tramite il protocollo SMBv1, se questo venisse disabilitato il rasomware non potrebbe entrare nella macchina.

Disabilitare quindi *SMB 1.0/CIFS File Sharing Support* dalle opzioni di Windows e riavviare la macchina.

- **Soluzione 3: Installare un anti-malware**

Per scongiurare la presenza del software malevolo nel sistema, si potrebbe installare un software anti-malware affidabile e aggiornato come Malwarebytes ed effettuare una scansione.

- **Soluzione migliore**

Aggiornare il sistema per prima cosa, poi effettuare gli altri passaggi.