**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** 23, January,2024 | **Entry: #1** |
| **Description:** | Documentation a Cyber security incident against a small U.S. health care clinic. |
| **TOOL(S)USED:** | NONE |
| The 5 W's | Capture the 5 W's of an incident.   * **Who :** organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. * **What :**  group of unethical hackers made ransomware attack against the organization * **When :** Tuesday at 9:00 a.m. * **Where:** Small U.S. health care clinic . * **Why :** the unethical hackers made ransomware attack because they want to demand a large amount of money to decrypt the data they encrypted . |
| Additional notes | The unethical hackers send a phishing emails to the employees , The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded, after they gain access they deployed the ransomware and encrypted critical data and they left a message for restore the data the organization must pay large amount of money.  In my opinion: the company must negotiate about the sum of money and pay it and don’t attack them because we don’t know what they will do if we attack.  Some advices for this incident:   1. Employee training on social engineering ways specially the phishing. 2. Restrict the critical data in restricted security zone with (NGFW) with advanced encryption. |

|  |
| --- |
| Reflections/Notes: Record additional notes : training the employees about this kind of attacks is so important because they can jump over all the tech we implants by gain access with phishing methods . |