Incident Handler’s Journal

Date:

Tuesday, 9:00 a.m. (Incident Day)

Entry:

Journal Entry #02

Description

This journal entry documents a **ransomware attack** that occurred at a **small U.S. health care clinic**. The incident originated from a **phishing email containing a malicious attachment**, which led to the encryption of critical organizational files. The attack caused **severe disruption to business operations**, impacting patient services and internal systems.

Tool(s) Used

- Email Security System
- Endpoint Detection and Response (EDR)
- Antivirus Software
- SIEM (Security Information and Event Management)

- Backup and Recovery Systems

The 5 W’s of the Incident

Who caused the incident?

The incident was caused by an **organized group of unethical hackers** who launched a targeted ransomware attack through a phishing campaign.

What happened?

A phishing email containing a **malicious attachment** was sent to an employee at the clinic.
When the attachment was downloaded and opened, **ransomware was deployed** on the system.
The ransomware encrypted the clinic’s computer files and displayed a **ransom note**, demanding payment in exchange for a decryption key.

When did the incident occur?

The security incident occurred on **Tuesday at approximately 9:00 a.m.**

Where did the incident happen?

- **Organization:** Small U.S. health care clinic
- **Initial infection point:** Employee workstation

- **Affected systems:** Internal computers and file storage systems

---

Why did the incident happen?

- The employee **opened a phishing email attachment**
- Lack of awareness about phishing threats
- Inadequate email filtering controls
- Insufficient endpoint protection against malicious attachments

---

Impact of the Incident

- Critical patient and administrative files were encrypted
- Clinic operations were severely disrupted
- Staff were unable to access essential systems
- Potential risk to sensitive health care data

Response Actions Taken

- Affected systems were immediately isolated from the network

- SOC team was notified and incident escalated
- Ransomware file and email attachment identified
- Backups were reviewed to assess data recovery options
- Law enforcement and relevant authorities were informed

Recovery

- Systems were restored using secure backups
- Compromised devices were cleaned and reimaged
- Normal operations were gradually resumed
- No ransom payment was made

Additional Notes

- Phishing awareness training should be mandatory for all staff
- Email attachments should be scanned automatically
- Regular offline backups are critical for ransomware recovery
- Incident highlights the importance of cybersecurity controls in healthcare environments