**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

**My Incident Overview**

Yesterday afternoon, the IT helpdesk received multiple reports from employees stating that their computers were running unusually slow, and some users experienced repeated disconnections from the internal file server. A network scan revealed a significant increase in outbound traffic from an internal workstation belonging to an accountant, identified as John Smith. Upon further investigation, IT staff discovered that John's workstation was actively transmitting large amounts of data to an unfamiliar IP address outside the network.

When contacted, John mentioned that earlier in the day, he received an email claiming to be from the company's CEO, urging him to urgently review and approve a financial report linked in the email. The email included a link to a file hosted on an external cloud storage service. After John clicked the link and downloaded the file, his computer froze momentarily before resuming normal operation.

Shortly after, a few employees in the Finance department reported that key financial documents on the shared drive were missing or replaced with files named “READ\_ME\_IMPORTANT.txt”, containing a ransom demand in exchange for restoring the files. The ransom note also mentioned that sensitive financial data had been exfiltrated and would be released publicly if the demand wasn’t met.

**Key Findings:**

**Phishing Email:** The malicious actor impersonated the CEO to trick John into clicking a phishing link and executing a malicious file.

**Compromised Workstation**: John's workstation appears to have been infected with ransomware that encrypted files on the shared drive and enabled data exfiltration.

**Data Exfiltration**: Outbound traffic logs confirm that sensitive financial data was transmitted to an external IP address.

**Missing and Altered Files:** Important financial records were encrypted or replaced with ransom notes on the shared network drive.

**Investigation Goals:**

**Identify the Phishing Email:** Analyze the email headers, links, and attachments to determine the source and method used to deliver the malicious payload.

**Trace Network Activity:** Review logs to trace the origin and destination of the outbound traffic, confirming what data was exfiltrated.

**Assess Ransomware Impact:** Determine the extent of file encryption and whether backups can restore the affected data.

**Evaluate Other Potentially Compromised Systems**: Ensure the ransomware or malware hasn’t spread to other devices in the network.

**Mitigation Plan:** Provide recommendations to improve email filtering, user training, and network monitoring to prevent future incidents.

|  |  |
| --- | --- |
| **Summary** | The company employee received a phishing email containing a link upon opening, which led someone to gain access to other endpoints and create a ransomware attack on some key financial documents. They found “READ\_ME\_IMPORTANT.txt”, containing a ransom demand in exchange for restoring the files. The note also mentioned that exfiltrated sensitive data would be released publicly if the demand wasn’t met. |
| Identify | The incident management team investigated the ransomware attack that originated from a phishing email sent to multiple employees. The email contained a malicious link, and John’s workstation was infected when the link was clicked. This infection encrypted financial records on a shared drive, making them inaccessible. An audit of access logs revealed unusual outbound network activity, indicating potential data exfiltration. The team identified that the malicious payload spread to other systems via shared network resources, exploiting insufficient endpoint controls. |
| Protect | To prevent similar incidents in the future, enhanced email security, restricted access control, endpoint security, backups, and employee training shall be conducted. |
| Detect | To detect future threats, the team shall deploy a network monitoring IDS, SIEM tool, and file integrity monitoring. |
| Respond | Immediate actions were taken by isolating the infected workstation from the network to prevent further spread of the ransomware. Management was notified, and they informed relevant stakeholders of the breach. Whereas incident responders conducted a forensic investigation to trace the origin of the phishing email and block the associated domains and IPs. Lastly, law enforcement and regulatory authorities were notified as required by data breach reporting guidelines. |
| Recover | The team restored encrypted financial records from the most recent, unaffected backup stored offline. To ensure data integrity they also conducted a post-restoration audit to confirm that all files were properly restored and that no residual malware was present. Improvements in the organization’s incident response plan were made. |

|  |
| --- |
| Reflections/Notes: This incident served as a critical wake-up call for the organization as it highlighted the urgent need to address and remediate existing security flaws. |