Post-Incident Review

Incident Overview

Incident Name: Ransomware Attack On VATI Financial Services

Date & Time: 5th of March,2025

Duration:

Reported By: Abdulmalik Salamah Attahiru

Summary

Severity: 5-High

Description:

- Briefly summarize the incident.

VATI Financial services was hit by a ransomware attack that originate from a phishing mail with a malicious attachment demanding for a ransom of 50 bitcoin as ransom to decrypt their files, the attack was a severe one as the attacker had elevated privilege that made it possible to compromise the systems backup resulting to a lot of damages.

Business Impact:

- What was the impact of the incident on clients, operations, and services?

An incident that affected multiple systems in the institution, prevents them of access to their systems, disrupt their business operations, access to their data.

The clients suffered multiple setbacks trying to carry out transaction on the institution's server leading to loss of client's trust and interest in the institution's services.

The institution suffered a great fall in their profit margin that was to be generated during the incident.

Incident Timeline

Post-Incident Review

Initial Detection:

- How and when was the incident first detected?

The incident was first detected when the employees noticed their files were modified by “LOCKED EXTENSION” on their systems.

Incident Timeline (Continued…)

Key Actions Taken:

- What were the actions taken to mitigate the incident, in chronological order?

1. Identification
2. Isolation and Notification
3. Disconnection and Decryption
4.Clean and Secure Back up
5. Vulnerability patches and security updates
6. Complete recovery.

Resolution:

- What actions were taken to resolve this incident?

1. The backup strategies were enhanced
2. The patch management processes were improved and refining communication protocols
3. Employee security training and awareness was increased.

Root Cause Analysis

Primary Cause:

- What was the main cause of this incident?

A phishing email that was sent with a malicious attachment to the employees systems.

Post-Incident Review

Contributing Factors:

- Were there any additional factors that contributed to the incident?

Lack of proper security awareness to alert staffs of phishing mails and how careful they should be before clicking any link sent to their systems.

Discovery Method:

- How was the root cause determined?

The root cause was determined by the security logs where it appeared that there was an unauthorized remote access from an unfamiliar IP indicating that the network has been breached.

Impact Assessment

Affected Services & Systems:

- Which specific services, systems, or processes were impacted by the incident?

Business Impact:

- What were the business impacts? (Downtime, Financial Losses, etc.)

Their was serious service downtime which affected the institution's wibesite
The institution suffered a great fall in their profit margin that was to be generated during the incident leading to great financial loss.

Client Impact:

- How were clients affected, and how many?

Clients were affected financially as they couldn't assess their funds due to server downtime.
About 70% of their clients faced this challenge due to the attack the institution suffered.

Post-Incident Review

Response & Recovery

Immediate Response:

- What actions were taken immediately after incident detection?

The affected systems were isolated and the team members were immediately notified

To prevent further connections ,the affected systems were immediately disconnected.

Backups were cleaned before long term fixes were made.

Short-Term Fixes:

- What were the temporary measures implemented to mitigate the issue?

Isolation

Containment and Notification

Disconnection

Response & Recovery (Continued…)

Long-Term Fixes:

- What are the permanent fixes that will prevent incident recurrence?

Backup the data to an external hard drive or cloud server.

Complete wipe of the device and OS re installation.

Communication Plan

Internal Communication:

- How and when did the response team communicate with internal stakeholders? (Alerting Tools, Mass Notifications, etc.)

The incident response team communicated with the internal stakeholders immediately when the incident was detected and contained.

The response team communicated to the internal stakeholders through secure channels like a dedicate incident response platform, out-of-band communication methods like text messages ensuring rapid notification and updates.

Post-Incident Review

External Communication:

- How and when did the response team communicate with external stakeholders? (Alerting Tools, Mass Notifications, etc.)

The incident response team communicated with the external stakeholders immediately when the incident was detected and contained.

The external stakeholders were communicated to via designated channels like press releases,direct communication with key contacts issuing a timely, transparent ,and concise statement acknowledging the incident, outlining the steps being taken to address it and providing updates on the situation while avoiding unnecessary details that could compromise the investigation they are carrying out.

Findings

Went Well:

- What went well when resolving this incident?

Communication to the stakeholders.
Successful isolation and containment.
Disconnections of systems from other networks.

Findings (Continued…)

Needs Improvement:

- What areas of the response plan could be improved?

Enhancing backup strategies
Improving patch management process
Refining communication protocols
Increasing employees security awareness training
Regularly testing recovery procedures

Post-Incident Review

Preventative Measures:

- What steps can be taken to prevent similar incidents in the future?

Cybersecurity training
Staying vigilant about emerging ransomware tactics
Actively patching vulnerability
Backup strategy

Action Items

Task List:

- What steps must be taken based on the findings?

Employee education and awareness
Updates and patch management
Backup strategies
Security tools

Task Assignments:

- Who is responsible for what assignments and when are they due?

Head of information technology
Notify response team of incidents and provide updates – first hours of the incidents.
Executive level manager in charge of physical security.
Building access and control – A day after the incidence.

Task Status: In Progress

Approval

Post-Incident Review

Review Conducted By:

Abdulmalik Salamah Attahiru

Date of Review: 10th of March,2025

Incident Manager Name: Aregbesola irorunoluwa

Incident Manager Signature: A.R

Date: 10TH Of March,2025