AFTER ACTION REPORT

INTRODUCTION

A Tabletop exercise was conducted for the TowerView Health Incident Response plan on 9/15/2016

The participants and their assigned roles are below:

Name	Organization	Role	Phone Number
Hareesh Ganesan	TVH	Exercise Facilitator	301-943-6475
Rahul Jain	TVH	Plan coordinator	715-771-9831
Emily Cerciello	TVH	Data gatherer	610-573-6809
Osuvaldo Ramos	TVH	Technical Lead	817-914-8218

The exercise was conducted in accordance with the TowerView Health Incident Response Exercise plan, dated 9/1/2016

The exercise was developed around the following scenario:

Upon weekly review of the system logs, the technical lead discovers that organization's servers have been hit by ransomware. This ransomware seems to have infected and then encrypted all the data, including backups, of two of your servers. According to the ransom you received, you must pay the ransom in a week or the encryption key will be deleted and the data lost forever. The cause of the issue was a version update vulnerability on OpenSSL that allowed unauthorized database access.

The IRP exercise looked to evaluate the organization's preparedness for a security incident, seeking to verify 1) correct reporting procedures were followed 2) the technical safeguards necessary to eradicate and recover were followed and 3) ensure overall preparedness for any third-party reporting necessary.

Summary of Exercise Results:

The incident response plan details 4 phases that must be executed in the event of an incident: Identification, Containment, Eradication, and Recovery. As such, the results of the test are determined according to performance in each phase.

Identification

- Upon identification of the issue, the technical lead began filling out the Incident Identification form available through Google Drive.
    - As the issue was a high-priority technical issue, Senior Management was notified through direct report by the technical lead.
- A rigorous search was performed to determine the extent of the compromise.
- The Plan Coordinator reviewed appropriate notification policies and began preparing a report to notify the Customers and Partners.

    - This process required a manual review of the various reporting requirements on a per partner basis. In incident, this would have required review from counsel. A more clearly defined record of reporting requirements for Customers and Partners would speed up the reporting process.

Containment

- The technical lead and the Security Officer began to contain the issue by:
    - Logging in using a secure SSH connection
    - Closing off all public ports for affected instances
    - Changing the access keys in the authorized_keys config
- This stage would have been administrated using Amazon Web Services for the instances. It was determined that AWS would provide adequate support for the necessary quarantine configurations.
- The Plan Coordinator continued to drive through the Incident response form, adding technical detail as necessary.

Eradication

- The cause was determined to be a version update vulnerability in one of the packages that allowed for remote access to the DB.
- The packages were successfully updated, and redeployed manually on each DB
    - Automated deployments using a container service would allow for much faster configuration.
- Logs of SSH, unauthorized log-in attempts, DB access logs were reviewed to determine the extent of the attack.
    - It was found that Amazon could also be used to review logs in the event of server lockout through Amazon Cloudwatch monitoring.

Recovery

- New servers were spun up with the patched update and addresses to these services were updated across any other communicating components.
    - Addresses and servers had to be updated manually. Using load-balanced Dockerized containers would allow for a much more rapid spin-up process.
- Functional tests were run to confirm that all functionality was restored.
- All critical data was restored from off-site Amazon S3 backups.
- A risk assessment of the data compromised was performed, and the Plan Coordinator notified appropriate parties.

Overall Performance/Follow-Up

Overall, the TowerView Incident Response plan was executed successfully. Through each step, the team remained aware of the necessary procedures and responses to follow and provide to ensure the incident was contained and handled correctly.

That said, improvements to the process have been identified below:

1. Reporting documentation: A record of all reporting requirements for each contract should be prepared to ensure all parties are notified in a timely fashion (Scheduled Completion: 10/1/2016) Completed: 10/7/2016
2. A report on containerized architecture to improve speed of deployment and better handle patch updates that caused the vulnerabilities. (Scheduled Completion: 12/1/2016) Completed: 12/13/2016
3. A centralized logging infrastructure to review logs offsite must be implemented. While backups of logs already exist, a utility to view and analyze logs must be present as well. (Scheduled Completion: 12/1/2016) Completed: 12/13/2016
    a. Logging infrastructure moved to Amazon Cloudwatch.

Approved By:

Signature

Date