Trove Inc.

Tabletop Scenarios

Tabletop Goals

This document should provide an effective IR Tabletop. It should be updated consistently based on the condition of Trove Incorporated's cybersecurity conditions and adapted to the most recent threat.

Overall Scenario Goals are as follows:

- Training resource
    - Any threat that poses a critical or high-severity threat to the organization should be used as a training resource for all sectors.
- The tabletop should be an accurate, real-time-adjacent simulation.
    - Hands-on experience is always beneficial.
- Security, sector communication, and organization within departments
- Ensure trust in:
    - External partners.
        - Cybersecurity insurance.
        - MSSPs.
    - Stakeholders and investors.
- Utilize analytical evidence to create a hypothesis.
    - How the threat was determined.
        - Threat type.
        - Threat severity.
- Include metrics.
- Provide how the company's IR procedure was used to mitigate the threat.

- If there is a severe threat:
    - Hold a meeting with the following roles present:
        - Cybersecurity
            - CIO
            - IA
            - IRT Manager
        - IT
            - IT Manager
        - Human Resources
            - HR Manager
            - Communications Manager
        - Legal
            - Legal Council

Tabletop Process

Record and document the findings from this IR Tabletop below:

Identify Threat Type:

Threat Type:

Phishing Attack

Identify Severity Level and Damage Cost:

Severity Level:

Medium severity – Phishing attack compromised sensitive information and data across the network.

Damage Cost:

$48,000 – There was a 3-hour downtime. Fraud charges stemming from Trove Inc. caused chargebacks. Users took their banking information off the site and cancelled subscriptions.

Provide Analytical Evidence and Hypotheses:

Hypotheses:

The culprit was malware installed through a phishing email.

Analytical Evidence:

- A huge load of packet exchanges, connections, and account creations occurred.
    - An audit log indicated this after the network traffic was marked as "unusual."
- The traffic came from a local device.
- The compromised computer suddenly experienced significant performance hindrance.

Procedural Response:

Preparation

- All personnel, as stated by the IR Plan, are assigned their roles.
    - Successfully organized and coordinated with each other.
    - Legal clearance for data access.
    - Damage control was successful with meticulous informing from Communications.
    - All personnel were readily equipped due to their appropriate ease of access to necessary equipment. (Analysts with proper monitoring, and IT with proper hardware)
    - The unusual traffic was quickly reported to IT and cybersecurity, and word spread to other departments.

Identification and Containment

- To contain the incident, the IT Manager acted quickly to separate infected computers from the main network.
    - The compromised devices were turned off and restarted within a safe environment on a separate network.
- As that was happening, the analyst and engineering teams were able to coordinate.
    - During separation, the IAs were able to begin monitoring network activity.
    - After containment and separation, analysts were able to examine the compromised computers in a safe environment.

Eradication

- Upon examination, IAs found that a phishing email from an employee's personal email infected a device, which spread to other devices synchronized with the network.
- To eradicate the threat, the analysts identified the infected device. IT Management then reimaged them all.

Recover

- After reimaging, the device was returned to a functional state.
- Extensive sensitive information on business partners, logistics, and company trade was unfortunately lost. – This caused the bulk of the financial loss.
- The analysts determined that extra precautions in their network needed to be implemented. A checksum was added to resend large amounts of packets and packets with questionable natures.
    - A checksum is a code function that compares packet values from when they were sent and when they arrived.

Lessons Learned

- After the technical writing team registered all findings into an organized document. The additional monitoring (checksum) requirement was explained, along with the ignorance of the employee checking their personal email on company computers. A meeting is now required.

Post-incident Meeting Summary:

Key Meeting Takeaways:

- The phishing email, being the source of the threat, caused a company policy update.
    - The use of company devices for personal reasons is now forbidden.
- A new contingency has been implemented in the network.
    - A checksum code function has been added.
        - This function checks for packet integrity (data validity).
        - If the packets (smaller parts of the big block of data being transmitted) arrive at the host (device running the company server) and do not match the checksum (short value being calculated from the larger block of data) when being sent from the client (user's computer), they will be sent back.
            - This checksum function can also manage network traffic by doing this.