NARO, Inc

Assessment Report Presentation

Ariel Guerrero, Isai Rivas, Jasmine Beale

Overview

- Introduction
- System Overview
- Assessment Methodology
- Assessment Activities
- Assessment Results and Recommendations
- Conclusions and Follow-on Activities

Introduction

In this report we cover information regarding our interviews with NARO inc, activities we used to better assess their security, strengths and weaknesses that the company exhibited as well as a summary of the results of our assessment.

System Overview

The NARO is a company that consists of a main facility (the office), workstations, a storage closet and company network (remote work). The main office is where the majority of company business takes place. Individuals can enter this office between the hours of 6am and 10pm on business days. Inside the office there are a total of 20 workstations (one for each employee).

Assessment Methodology

- **Protect**
  - What do you currently use in the way of protection against cyber security threats?
  - Is your business and customers private information properly encrypted?

- **Detect**
  - What type of anti-virus protection does your business run?
  - How often is your network checked for any intrusions?
  - Are there logs that record any suspicious activity?

- **Respond**
  - What step by step process does your business currently have if an intrusion was to be detected?
  - Who is your current point of contact when an intrusion occurs?

- **Recover**
  - What is your current state of information and systems backup?
  - How often are systems backed up?
  - Where are your backups stored?
  - Are your backups encrypted?

Assessment Activities

- Least Privilege
- Concurrent Session Control
- Remote Access
- Access Control for Mobile Devices
- Information Sharing
- Policy and Procedure
- Training and Awareness

Assessment Results and Recommendations

Observations

Strengths

Weaknesses

Assessment Results and Recommendations

Observations

- Employees are limited by the amount of company devices
- Server rooms are left unlock during and after operational hours
- NARO does not utilize intercom system

Assessment Results and Recommendations

Strengths

- Personal workstations
- Company devices
- Credit Card Handling

Assessment Results and Recommendations

Weaknesses (set 1)

- Employees leave files out on desk
- Employees use their own mobile devices to access company files.
- External devices such as usb drivers are often connected to servers.

Assessment Results and Recommendations

Mitigations (set 1)

- Employees should be trained on how to protect their workspaces in and outside the office.
- In order to ensure privacy employees should only access company files when connected to company networks or when utilizing authorized company devices.
- If a usb device must be utilized it should be inserted on a computer rather than directly into the server.

Assessment Results and Recommendations

Weaknesses (set 2)

- Password policy only using 10 characters
- Employees are not required to change their passwords, they are currently changing passwords as little as possible
- Everything is on the file server

Assessment Results and Recommendations

Mitigations (set 2)

- Require employees to follow best practices when creating a password and update company policies to those best practices.
- Require Employees change their password at set intervals and insure they follow company password policy that is implemented as a best practice.
- Use the file server as intended and leverage the other servers for their intended purposes as well.

Assessment Results and Recommendations

Weaknesses (set 3)

- No firewalls on servers
- There aren't any official logs of who enters the NARO office at any time
- Proxy card that is used to unlock building also unlocks NARO office space

Assessment Results and Recommendations

Mitigations (set 3)

- The company should exercise its due diligence and be sure to enable a firewall not only on the servers but on the entire network to mitigate against attackers.
- The company should implement an electronic log system so every employee is properly accounted for when entering and leaving the office space.
- NARO should disable the use of the building proxy card and implement company specific security measures.

Conclusions and Follow-on Activities

The assessment that was conducted for NARO includes a view of the possible risks that the company is exposed to. Although NARO has strived to cover the majority of its bases, our team discovered several vulnerabilities through which intruders and attackers can compromise the site both physically and virtually. Our team suggests that the deficiency of employee cybersecurity and security practices be prioritized among all risks.

- NARO uses best industry practices for data backups
- NARO's can further improve upon their employees cyber security knowledgebase
- Moving forward, NARO can implement knowledge checks and retention policies