NARO, Inc Assessment Report

Prepared by:Jasmine Beale, Ariel Guerrero, Isai Rivas

Death Star Consulting

1 Executive Summary

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. The beginning of our assessment goes over what we could and could not address during our assessment. Many topics were in bounds meaning we could explore and investigate these ideas further. Other subjects were out of bounds meaning we were unable to pursue these areas of discussion.

Once we discover what was in and out of bounds for our assessment we were able to perform a number of activities to further anaylze some of our pervious observations. Using the NIST framework we create a methodology of conducting the assessment. After establishing the methodology we list out a few high level activities that we believed would help us determine some weaknesses within the companies security.

Each team member was able to come up with a set of weaknesses, strengthens and observations found based on our assessment results. We list them out in section 5 of our report. Along with this list and our personal deductions we create a conclusion based on our findings and ways they can improve their internal and external security practices.

In conclusion, we would like to think NARO for allowing us to conduct interviews and evaluate their security infrastructure. We understand the scarifies that companies must make in order to make sure their security needs are met. We appreciate them for listening to and implementing any and all of our recommendations. We hope to do further business with NARO as they grow and develop their company.

Contents

1 Introduction

1.1 Background

The reason for this assessment is NARO has come to realize that their business might be at risk for cyber attacks. The businesses security management is very under staffed and is not reliable when it comes to uploading privacy. Henry, their “IT guy” is responsible for all and any work down on the NARO servers. However, Henry is also involved with another company. In order to uphold integrity it’s important that they only request certain services from Henry to insure sensitive information isn’t mistakenly given off to unauthorized individuals.

1.2 Scope

In-scope:

- password security measures
- backup methods
- physical security
- server room
- employee laptop handling
- servers
- company software
- company hardware

out-of-bounds:

- requesting details about tokens or information related to third party servers
- credit card processing security
- access logs
- real estate records

1.3 Report Organization

The rest of this report is organized as follows: Section 2 provides an overview of the NARO facilities, systems, and processes used. Sections 3 and 4 describe the methodology used by the team and the activities they conducted. The assessment results are found in Section 5, with conclusions and recommended follow-on activities in Section 6. Appendices include additional information related to the assessment.

2 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).

Employees will often work at these stations to connect to company server and software. Along with this NARO has a company network that can be accessed remotely using one of the 4 company laptops. The network is upheld by the storage closet aka the server room. The server room is unlocked at all times so anyone who has accessed to the main office has access to the server room.

2.1 Facility or System 1

The first facility that was analyzed was the main office building. The NARO office is located on the 13th floor of a high rise in downtown San Antonio. The business neighbors a real estate development firm, oil and gas services firm and an empty office that was leased to an investment firm charged with fraud. The company has a one person IT department who currently works with another company along with NARO.

During the interview we noticed major vulnerabilities with the office and building authentication methods. Since there are no intercom systems, anyone with a proxy card can enter the NARO office space. They simply have to pass through the receptionist desk. It's clear that this leaves the ability of individuals who are not authorized to enter the office. Furthermore the company is lacking in proper practices in terms of piggybacking awareness. When asked if the company was concerned with piggybacking they were unaware of the content of the term. There is currently no log to confirm who and who has not entered the office space. When a receptionist needs to let someone in they can simply do so with a press of a button. This becomes a concern because during the receptionist off hours it would be relatively easy for an unknown person to let themselves in the office space.

Key items:

- Staff consist of 20 full time employees
- Manager has their own office
- 3 accounting team members share an office
- there is one receptionist that works 9am - 5pm
- office is open from 6am - 10pm
- one space was formerly leased to an investment firm charged with fraud
- access to NARO office only requires building proxy card

2.2 Facility or System 2

The next system is the employee work stations. Each of the computers at the workstations are running windows operating systems. When employees leave their workstations their systems are left running and if they are using company software there isn't an auto logout feature that triggers after a certain amount of inactivity. Employees do not use proper password safety methods. They sometimes write passwords down and leave it available for anyone to see on their desks. Employees are not required to change their passwords. They will go months without changing their passwords or checking if any of their passwords have been compromised. Employees leave important documents out on their desk when they are in and out of their stations.

Key items:

- Each employee has a workstation
- passwords are changed at various times (every 3 months or so)
- passwords information is left out on desks
- company information is left out on desks when not being utilized
- NARO software does not utilize auto logout technology

2.3 Facility or System 3

The next system is the company's network and servers. In order to connect to company servers outside of the office employees must use either their mobile devices or company laptops. The company servers are not enabling any firewalls or technical security methods. The only security they used is security built into their windows operating systems (windows defender). Since there are only 4 company laptops most employees utilize their personal devices to access information on the network. There are no known authentication methods other than putting in the employees usernames and passwords. All documents can be accessed using the office 365 site.

The NARO company utilizes 3 physical servers that are all located in the office storage room. The storage room is always left unlocked so their IT person Henry can access it during any time of the day. When Henry works in the server room he uses usb drives and other external devices to upload and download data from the servers. Everything is stored on the file server meaning that everything is accessible from one place on the server.

Key items:

- Company has 4 employee laptops
- Company can access server files through office 365 from their personal devices
- Company servers do not use firewalls
- NARO has 3 servers located in the storage room
- The storage room is always left unlocked
- usb and external devices are often connected to the physical servers

3 Assessment Methodology

The **Information Technology Laboratory** at the National Institute of Standards and Technology promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. [1] Information Technology Laboratory developed tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. Information Technology Laboratory's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. ***This Security framework is based on NIST SP800-53 revision 5 and the NISTIR 7621 revision 1*** published by The Information Technology Laboratory, with the purpose of serving a concise yet robust and easy to understand security model for small business who may not have the expertise or understanding to answer many of the items found in detailed checklists, may not have a lot of time to dedicate to the process, or may not have the funding to bring in a 3rd party to conduct the audit. Organizations must exercise ***due diligence*** in managing information and privacy risk. Employing effective risk-based processes, procedures, methods, and technologies ensures that information systems and organizations have the necessary trustworthiness to support business functions.

4 Assessment Activities

4.1 NARO Documentation Review

- Least Privilege Users should only be allowed to use privileged software based on their role in the business. By limiting the amount of privilege that a user has access to, if, theoretically, the user's account was compromised, it would limit the number of systems that are impacted and could be used for malicious purposes. Within the least privilege control, we could also employ enhancement 3 which includes authorizing network access commands for certain operational needs while also documenting the reasoning behind such needs.

- Concurrent Session Control: A small business should take care of how many concurrent sessions its employees have access to based on the role of the employee. By closely monitoring the attempts that an employee has made in having various sessions open, a small business can use this as a detection measure to see if high levels of attempts are caused by a compromised user, this also limits the attackers window of operation as it would be easy to trigger such a detection measure.

- Remote Access: As more and more employers have shifted to remote work, it can be deduced that an attacker will attempt to compromise a user's account using the employee's personal computer, as a personal device has less security than that of an enterprise device. We can further strengthen this control by implementing enhancement 10 (Authenticate remote commands) by implementing a two-factor authentication process that requires an employee to input a pin and a token so that specific commands and logins can be verified; this provides strong protection in assuring that an employee and not an attacker is the individual that is logging in.

- Access Control for Mobile Devices: Personal handheld devices are the most prevalent form of communication, and if an attacker was to compromise an employee's mobile device, the attacker would have an array of sensors and tools that could be used to spy and further advance their attempts of intrusion. Implementing policies that limits mobile device usage can further enhance the security of a small business the rationale behind such policies is due to the possibility of employees not having the lates security patches updated to their mobile devices, such lack of patches can cause an attacker to exploit the employee's mobile device and use it to compromise any system an employee connects their device to.

- 21 Information Sharing: Information sharing can be an easy oversight, if an employee has the privilege to send emails with sensitive information outside of the organization, this can cause huge regulatory issues, along with providing attackers the ability to send mass amounts of information outside of the business without raising suspicion. This can further be enhanced to include the restriction of external communication, only specified users can have access to send out external emails which would require that the emails sent out along with the users account have extra scrutiny in case the account is ever compromised.

- Policy and Procedure: This control falls under the category of awareness and training, and the purpose of such a control is to build policies that reduce the possibility of an attacker compromising a system or network. Management can create awareness information and develop training materials that users can learn upon.

- Literacy Training and Awareness: The purpose of such a control is to raise employee awareness of disguised cybersecurity threats. Human error is usually the biggest weakness, and for a small business, it can be easier to assure that most if not all employees are aware of the tactics used to compromise a network. By having quarterly training sessions and knowledge checks along with mock attack, the human error can be greatly reduced.

4.2 In-person Interviews

On whatever date, the team met with WHOEVER from NARO, Inc. to discuss…

The team met with the CEO on NARO; the following items were extrapolated from the interview:

- The proxy card used to open the building can also be used to unlock the NARO office
    - We should design a stronger authentication technique
- There are no official logs of who can enter and exit the NARO office
- Employees are known to leave sensitive files on their desk
- The password policy must be revised, currently, only 10 characters are used, increasing the number to 14 characters (including numbers, special characters, and upper-case letters)
- No activity logs are kept
- External drives, such as USB drivers, are frequently utilized
- The only security Program used is Windows Security
- Employees use their personal mobile devices to access and view NARO documents via the Office 365 website
- Employees are not compelled to update their passwords, in addition, the rate of which they change their password is low
- There are no firewalls on servers
- Henry, the CEO, also works for other companies other than NARO
- After hours, the computer room is left available for cleaning personnel
- Retention policy for real estate records is seven years
- Everything is stored on a single file server
- NARO uses WordPress website

5 Assessment Results and Recommendations

The assessment resulted in a concise understanding of various policy and procedures that can be summarized in 3 main categories. The first category is user access control. The activities performed were able to give us a better understanding of how employees were able to interact with the NARO software and servers. Secondly, we examined remote access. Methods of access were analyzed and evaluated based on the usage and type of information that could be obtained outside the perimeters of the NARO office facility. Lastly we accessed if there were any training and awareness practices that NARO was implementing to protect their employees and company integrity as a whole. From each of our assessment activities we made a number of observations listing out a few strengthens while focusing on the company's weaknesses and areas it needs to improve in. The following is a list of all three (observations, strengthens, and weaknesses) as well as some recommendations we deemed appropriate for each weakness.

5.1 Weaknesses

Employees leave files out on desk

Justification: This can be troublesome if desks are left unattended. Leaving files on desk gives unauthorized individuals opportunities to see and possibly use information for malicious purposes.

Mitigations: Employees should be trained on how to protect their workspaces in and outside the office. When they are away from their workstations they should secure all files and log out of company software. Auto log out should also be implemented to cover for employees who may forget to log out when leaving their desks

Employees use their own mobile devices to access company files.

Justification: As the NARO company can not control how employees use their personal devices, the use of them can open up a variety of security risks. Mobile devices can be used on secure networks but are oftentimes used in non secure environments. If an attacker wished to scan a public network that an employee was utilizing they could possibly find ways to view and disclose any information being sent or received while on the network.

Mitigations: In order to ensure privacy employees should only access company files when connected to company networks or when utilizing authorized company devices.

Conducting business in controlled environments limits the possibility of threats and allows easier monitoring of activity.

External devices such as usb drivers are often connected to servers.

Justification: Attackers can easily use external drives to infect hardware. If a trojan or other malware was unknowingly present on an external device, using it on the servers could cause significant harm to major sectors of the system. Furthermore, carrying around sensitive information on a usb drive can be detemential if the device was lost, stolen or physically damaged.

Mitigations: If a usb device must be utilized it should be inserted on a computer rather than directly into the server. Inserting it in a computer provides more protection as usb drives can automatically be scanned through the assistance of different software and alert users if there is something on the device that can severely harm the machine.

Password policy only using 10 characters

Justification: One of the weakest points of an IT system is the authentication system, mostly due to the fact that many users will disregard best practices.

Mitigations: Require employees to follow best practices when creating a password and update company policies to those best practices.

Employees are not required to change their passwords, they are currently changing passwords as little as possible

Justification: Training employees should include creating and maintaining a strong secure password and how to use different passwords for each account the employee may posses.

Mitigations: Require Employees change their password at set intervals and insure they follow company password policy that is implemented as a best practice.

Everything is on the file server

Justification: Because all the data is on the single file server there is a huge risk of loss. Important documents could be lost for good and considering some have to be held for a period of time there is even a risk of legal trouble. Not to mention the ease of access to all the company data that an attacker has.

Mitigations: Use the file server as intended and leverage the other servers for their intended purposes as well.

No firewalls on servers

Justification: Firewalls are used to block malicious communications or browsing of inappropriate websites

Mitigations: 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.

There aren't any official logs of who enters the NARO office at any time

Justification: It can be dangerous if unauthorized individuals enter the NARO office via methods such as piggybacking.

Mitigations: The company should implement an electronic log system so every employee is properly accounted for when entering and leaving the office space.

Proxy card that is used to unlock building also unlocks NARO office space

Justification: Only utilizing a building proxy card creates many physical vulnerabilities for the company.

Mitigations: NARO should disable the use of the building proxy card and implement company specific security measures.

5.2 Strengths

Personal workstations:

- Each employee has their own workstation. This is a good measure for personal and company privacy.

Company devices:

- NARO uses company devices. This is important as there are many tasks related to the business that should only be conducted on authorized devices.

Credit Card Handling:

- The credit card information is being handled through a third party application which is good as their physical and server security is vulnerable.

5.3 Observations

Employees are limited by the amount of company devices

Description: Employees only have 4 employee laptops to use when they're away from the NARO office.

Recommendation: It would be wise for NARO to invest in more company devices with special security installed to ensure the safely of their company files.

Server rooms are left unlock during and after operational hours

Description: NARO does not implement any measures to secure their server room.

Recommendation: NARO should lock the server room when it is not actively being utilized. The company should also ensure that unauthorized devices that can physically connect to the server are not on any personnel who enters the room.

NARO does not utilize intercom system

Description: NARO does not have a proper system of checking who enters and leaves their facility.

Recommendation: The company should implement a intercom system along with company specific cards that limits who is allowed in the office space and to keep track off which individuals are present at any given time.

6 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.

When it came to data backup, NARO came out on top. NARO mitigates ransomware attacks using industry standards and has established resiliencies to ensure minimal disruption.

NARO fared poorly, particularly in terms of staff cybersecurity understanding. From the standpoint of the firm, this is readily manageable. According to Cybint, a cybersecurity education provider, 95 percent of breaches are caused by human error. Most assaults may be prevented by boosting employee education on cybersecurity and improving basic procedures such as locking up vital information and changing passwords on a regular basis.

Moving ahead, we propose that NARO performs frequent knowledge checks for its employees, which may include internal phishing tests and potentially data retention policies to ensure that crucial compromising material is not held on to for too long.