CS-465 Information Assurance Project: Incident Report

Myrna E. Santiago

Old Dominion University

CS 465_23470

Table of Contents

Contents

List of Tables

Introduction

As of 2024, technology has created a revolution in the manufacturing industry. In a move of what experts called the Fourth industrial revolution or Industry 4.0, manufacturers implemented cutting edge technology in the space of 24 years compared to previous manufacturing eras. The last 4 years have seen an exponential technology growth in manufacturing as byproduct of the pandemic of 2020. In a desperate attempt to function despite the population health problem, manufacturing companies found a solution to their problems by integrating the Internet of Things or IoT, Cloud computing, Artificial Intelligence, and Cybersecurity.

The later one being of most important considering that data has become the most important asset in any industry. The ability of a company to acquire and process data in real time to produce goods and services has created a once in a lifetime opportunity of growth for many. Information Assurance or IA provides the necessary blueprint to protect such important assets. By protecting the integrity of the data, IA ensures that the data is not changed or tampered with. By securing its availability, IA guarantees that the data can be accessed when needed. IA makes sure confidentiality is met by allowing only the authorized users to access the data. Lastly IA uses non-repudiation by making sure of the authenticity of the data and its users.

With all this in mind I will provide a report on the results of my investigation and how to move forward from this situation by providing some insights and solutions.

What Happened?

On February 23, 2024, a system administrator at ABC receive communication about ransomware and was blocked out of the system. Upper management was notified. It was decided to bring in experts to investigate the matter and help restore the systems. During the investigation it was discovered that an employee received an email with a spreadsheet attachment. The email looked to be genuine, and the employee opened it not seeing anything amiss. The attachment contained the malware known as Zloader. This malware is a trojan which purpose is to steal cookies, passwords and sensitive information. It took Zloader trojan 4 minutes to infect the computer and start its attack.

Inside the Zloader was a copy of Ryuk, a know ransomware, locked the administrative and financial part of ABC manufacturing. In total, since the start until discovery 3 weeks passed. Another 3 weeks were affected by ransomware demands and restoration of the system. In total, 6 weeks of productivity and security were affected.

Background

ABC Commercial Responsibilities

ABC responsibilities are creation of a high-quality product that meet commercial standards. Production is kept in a time sensitive schedule to meet the needs of the customer base. Raw materials use meet the necessary commercial standards.

ABC Intellectual Properties

Intellectual properties include patents, trademarks, copyrights, and trade secrets. These properties allowed ABC to maintain a niche in the manufacturing industry.

ABC Strategic and Corporate Alliances

These alliances are an agreement between corporations to work together to provide products and services to others. Vendors and customers depend on ABC to acquire or supply their needs in order to have profit.

ABC Network Infrastructure

ABC has a custom Enterprise Resource Planning (ERP) system. This system was clearly implemented with security in mind. ERP is a software solution that help the optimization of production planning and manufacturing operations. It also helps with shop floor control and sale orders. It also collects data necessary for production control, integrations and flexibility.

If it is correctly used improved efficiency, visibility, customer service and profitability. Some of its main features are inventory management, Quality control (QC), and traceability which manage the lifecycle of the products. While this system is ideal, many implementations were lacking and provided a series of weaknesses in the system. Let see some of those weaknesses and also some strengths of the ABC system.

ABC Network Strengths

The system was divided logically which divided into Information Technology (IT) side and Operational Technology (OT) side. The IT side contains the administrative and financial areas of ABC and the OT side contains the engineering and manufacturing processes areas.

This division allowed better allocation of resources and an extra layer of protection for one segment if the other is compromise. Which we observe to be true when the system was breach. During said breach the IT area was affected while the OT area remain relatively safe.

ABC Network Weaknesses

Some of the weakness observe during the investigation are the lack of updates and hotfixes applied to the security system. Also, the firewalls were not properly set to block any incoming traffic. There were not Intrusion Detection/ Prevention systems set up to deal with the incoming traffic. The most important one was the lack of awareness training that cause the person to open the email and download the attachment. These weaknesses provided the best opportunity for the phishing attack.

Attack Consequences

The attack affected the financial operations of ABC manufacturing. For 3 weeks profits were affected because billing could not go to customers and vendors could not get paid. These problems created others like loss of reputation because of the inability to pay on time and meet customers deadlines as well as fear of compromise sensitive information. It will take hard work and time to recover from the losses the attack cause.

Vulnerability Assessment

The National Cyber Security Centre (2024) define vulnerability as a weakness that can be exploit by an attacker to deliver a successful attack. Some vulnerabilities are flaws like a poor design or implementation, zero-day vulnerabilities, features in the system that can be use by an attacker, and user error, which account for 95% of the successful attacks.

The National Institute of Standards and Technology (2024) define vulnerability assessment as the formal description and evaluation of the vulnerabilities in an information system. In a vulnerability assessment the vulnerabilities are identify and provided with a more detailed description. In it is also determine if the vulnerability is critical, essentials or ancillary (supplementary). Table 1 provides a vulnerability assessment according to the findings of the investigation and how important they are.

Vulnerability assessments

Vulnerability	Description	Category
Lack of firewall rules	The lack of firewall rules allowed the email to pass to the internal network.	Critical
Lack of Intrusion Prevention/Detection mechanisms	These mechanisms will have raised the alarm to prevent or mitigate the attack. The lack of said mechanisms allowed the malware to enter the network.	Critical
Lack of malware/ransomware monitoring services	The absence of these mechanisms allowed Zloader and Ryuk to reside in the network for a prolonged period of time.	Critical
Lack of cybersecurity training for users and employees	The lack of security training provided the attacker with the best tool to enter the network. An uneducated user can cause lots of damage without meaning to.	Critical
Lack of rules and policies for control and mitigation	The lack of rules and policies allowed the user to open an	Essential

	infected spreadsheet that spread the trojan and affected more systems.	
Lack of recovery plan	A proper plan in place would have allowed for a faster recovery to bring affected system back in working conditions.	Essential
Lack of fault tolerance	The absent of a fault tolerance mechanism prevented ABC from a prompt recovery and delay proper functionality	Essential

***Table 1 Vulnerabilities Assessment**: This table provides a list of the vulnerabilities that play a part in the attack and were classified in level of importance. With this table we can address each one and use it as reference for future projects.*

Threat Matrix

Irwin (2023) defines threat matrix as a risk assessment tool that is crucial for organization protection of sensitive data and prevention of data breaches. It is a way to compare and measure threats and vulnerabilities. This type of assessment quantifies the vulnerability and security threat on a scale of 1 to 10, with 10 being critical risk and 1 being acceptable levels. High Impact and likelihood scale: 50-70, Medium impact and likelihood: 30-50, Low impact and likelihood: below 30.

Vulnerabilities

Threats	1	2	3	4	5	6	7	Total	Likelihood	Impact
A	8	9	10	9	9	9	7	61	high	high
B	8	10	10	9	9	9	8	63	high	high
C	7	7	7	10	8	7	8	54	high	high
D	8	7	9	10	6	5	5	50	medium	medium
E	6	6	6	10	9	5	4	46	medium	medium

Table 2 Threat Matrix: It is a quantitative way to assign resources and secure critical infrastructure. By addressing the information on this matrix, the systems can be updated and protected in a timely manner.

Vulnerabilities list

1) Lack of Firewall rules

2) Lack of Intrusion Detection/Prevention mechanisms

3) Lack of malware/ransomware monitoring mechanisms

4) Lack of security training

5) Lack of rules and policies for control and mitigation

6) Lack of recovery plan

7) Lack of fault tolerance

Threat list

A. Malware

B. Ransomware

C. Insider threats

D. Social Engineering

E. Poor security training

Recommended Communication Plan

The following plan should be implemented in order to address future concerns or situations:

1) Creation of an incident response team. This team will handle any communication pointing at a breach or attack. By creating appoint of contact the team will promptly take over in investigating the situation and provide the first steps of response needed for mitigation.
2) Appointing a specific person for external communication save time and resources by allowing that person to handle inquiries and rumors as well as handling of media.
3) Determine the criteria needed for law enforcement involvement. There are situations were investigations can be handled internally, while others require the expertise of the professionals. Especially in situations were fraud or use of resources appoint to human trafficking or child abuse.
4) Creation of communication template for customers. This way the limited resources can be appointed correctly and customers satisfaction will be met. Creating a template of notification message in advance save time and resources.
5) Monitor social media. In a crisis rumors and misinformation is spread rapidly through social media. In order to be a step ahead, a person from the response team should be in charge of dispel rumors and provide the correct information according to the plan. This way panic can be prevented and the company keep control of the situation.

Recommendation to prevent future attacks

The first order of business is to address the vulnerabilities and threats pointed before in this report. We need to implement best cybersecurity practices and follow a framework as a roadmap for the future. We have some of the mechanism at hand but they need to be properly set and deploy. We also need to change email communication by centralizing and securing the email server. We need to provide extensive training that will be design as a routine that anyone can follow and compensate those who excel in helping secure the network. This will provide motivation for others to try harder in keeping up with security.

Conclusion

In conclusion while the mechanisms for defense are available through ERP systems, they were never properly implemented. The lack of proper training and security best practices allowed the attacker to enter the system and compromise the area that contain sensitive information about employees, vendors, and customers. This created a loss of credibility and reputation as well as profit. The integrity, confidentiality, availability and non-repudiation of the company suffered a great blow that will take hard work to recover from. I believe that applying the recommendations in this report we will be able to take a step in the right direction and bring the company back to good standing.

References

Blyth, A. & Kovacich, G.L. (2024, January 6). Information Assurance Security in the Information Environment. (2nd ed.). *Springer*. Middletown, DE.

Chapple, M. (2024). *Incident response: How to implement a communication plan.* *https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan*.

Harrington, D. (2023). *Ryuk Ransomware: Breakdown and Prevention Tips.* https://www.varonis.com/blog/ryuk-ransomware.

IBM. (n.d.) *What is Industry 4.0?* https://www.ibm.com/topics/industry-4-0#:~:text=the%20next%20step-,What%20is%20Industry%204.0%3F,improve%20and%20distribute%20their%20products.

Irwin, L. (2023). *What is a Cyber Security Risk Assessment Matrix.* *https://www.vigilantsoftware.co.uk/blog/what-is-a-cyber-security-risk-assessment-matrix#:~:text=A%20cyber%20security%20risk%20assessment%20matrix%20is%20a%20crucial%20tool,risk%20assessment%20to%20the%20board*.

National Cyber Security Centre. (2024). *Vulnerability Management.* *https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities#:~:text=A%20vulnerability%20is%20a%20weakness,to%20achieve%20their%20end%20goal*.

National Institute for Standards and Technology. (2024). *Vulnerability Assessment.* *https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-*

vulnerabilities#:~:text=A%20vulnerability%20is%20a%20weakness,to%20achieve%20their%20end%20goal.

No author. (2024). *The comprehensive guide to manufacturing ERP systems*. Katana. https://katanamrp.com/manufacturing-erp-system/.

Tavares, P. (2022). *Zloader: What it is, how it works and how to prevent it | Malware spotlight [2022 update]*. *https://www.infosecinstitute.com/resources/malware-analysis/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/*.

Uzialko, A. (2024) *Industry 4.0: How Technology Is Revolutionizing the Manufacturing Industry.* https://www.businessnewsdaily.com/10156-industry-manufacturing-iot.html.