2024

CS 465 Information Assurance Project

ABC MANUFACTURING COMPANY REPORT

ALANNA RICHERSON

Table of Contents

List of Figures **1**

Introduction 2

Background 3

Assignment **4**

Deliverable 5

References 6

Introduction

The manufacturing company ABC Inc. has approximately 1000 individuals employed. The company is composed of a segmented network that divides financial/administrative operations (IT operations) and engineering/manufacturing processes (OT segment), with a customized enterprise resource planning (ERP) system connecting them. A ransomware attack recently occurred at ABC Inc. disrupting the company's financial and administrative operations for three weeks. The ransomware attack was found rooted within a phishing email which contain a malware called Zloader, which collected logins and passwords eventually led to Ryuk ransomware being deployed. These ransomware attacks compromised over 40 computers in the IT sector.

ABC Inc. addressed this incident by partnering with cybersecurity experts outside of the company to aid in system restoration and damage mitigation. Moving forward, to prevent incident similar in nature to this on ABC Inc. will implement a comprehensive set of information

assurance (IA) policies and procedures. These security measures entail advanced email filtering and phishing detection, stronger malware protection, enhanced network segmentation and access controls, frequent programs for cybersecurity awareness and training, an optimized incident response plan, data backup and recover processes that are secure, and strict access management policies. The goal of security measures is to make ABC Inc.'s cybersecurity defenses stronger and protect the company's proprietary information and critical operations.

Background

ABC Inc. is a manufacturing-based company with approximately 1000 employees. ABC Inc.' network is divided into two main segments to ensure that their operations are as secure and efficient as possible. These two segments are the IT segment (Financial and Administration Operations) and the OT segment (Engineering and Manufacturing Processes). The IT segment handles receivable and payable accounts and oversees the company's money traffic. For inside and outside company communications, which supports tasks such as vendor interactions and customer relations employees utilized email addresses that are personalized. The OT segment deals with the main engineering and manufacturing processes. These tasks include quality control, machinery operations, and management of the product line. Also, the OT segment maintains production efficiency and quality by using specially designed equipment and programmable logic controllers (PLCs). A shared infrastructure connects IT and OT segments this infrastructure utilizes a specialized enterprise resource planning (ERP) system. This enterprise resource planning (ERP) system merges several functions of the company, data traffic support, inventory management, production scheduling, and resource planning. The ERP systems also facilitates decision-making and strategic planning and makes sure that financial reports are accurate. ABC Inc.'s usage of personalized emails enhances internal and external

communications by making it more secure and professional while also maintaining the protection of sensitive information. The division of the core functions into two segments and the ERP system aid in operation optimization, security improvement, and the efficient integration of financial, administrative, and manufacturing processes.

Summary of the Incident

It was reported that the breach occurred due to an ABC Inc. administrative support employee receiving a phishing email that held an Excel spreadsheet with malicious contents. When the administrative support employee opened the email attachment, within four minutes of opening the attachment Zloader malware was deployed in the system which harvested various logins and passwords. Over the next three weeks the financial and administration systems ended up being locked down because of Ryuk ransomware that was activated due to the deployment of the Zloader malware. The sector that was severely impacted was the IT segment which is responsible for receivable and payable accounts. The sector of ABC Inc. that remained unaffected which was the OT segment which covered manufacturing and engineering. In-house technical support's first response aimed for infrastructure restoration, but the decision made by higher management was to incorporate external cybersecurity expertise to develop a resolution quicker and more thorough. All of the system's compromised files were removed by this team of external cybersecurity experts allowing to company to resume normal operations.

Breach consequences

The breach that occurred at ABC Inc. caused several issues which includes disruption of operations, financial effects, damage to their reputation, and technical impact. ABC Inc.'s day-to-day operations were severely disrupted because to the company not being able to pay vendors or

send bills to their customers for over 3 weeks. Due to the company not being able to carry out these financial transactions the cash influx may have been exhausted and revenue may have been lost. Also, there was an added issue to the finances when ABC Inc. was required to hire the help of external cybersecurity experts. ABC Inc's customers and vendors started to question it he company was able to maintain their data security and operation reliability causing a significant amount of reputation damage to ABC Inc. Lastly, ABC Inc.'s IT segment was breached which required a thorough cleanup and recovery due to over 40 of the computers in the segment being compromised with Ryuk ransomware.

Vulnerability Analysis

When this breach at ABC Inc. occurred it displayed various vulnerabilities that were in their operational systems. One of the first vulnerabilities that were highlighted was the inadequacy of ABC Inc.'s email security. A sufficient email security system would have not allowed that phishing email which contained the Zloader malware to reach the administrative support employee. What this vulnerability entails is the company's email security system needs to enhance their email filtering capabilities and the mechanics for which they detect phishing. Secondly, the measures in which the networks were isolated and segmented were not strong enough. Because even though the OT segment was unaffected this breach was able to spread throughout the IT segment. Third, the methods ABC Inc. used for detection and response to malware in the system were insufficient. As the malware that was initially implemented was able to go undetected for up to three weeks during which they harvested the credentials of over 40 computers and then installing Ryuk ransomware. Lastly, user awareness and training clearly need to be enhanced and enforced. The administrative support employee was blatantly unaware of the risks that would come with opening the phishing email that appeared in their inbox. Thus,

emphasizing how crucial it is for all the employees to participate in routine cybersecurity training.

Proposal of Information Assurance policies and procedures

A comprehensive set of information assurance policies and procedures is proposed to ABC Inc.'s cybersecurity defenses and prevent security breaches in the future. First, to strengthen email security, advancements will be made to systems that perform email filtering and phishing detection. This will be utilized to stop any seemingly malicious emails before the emails are able to reach the employees. Also, to defend against vulnerabilities in the system that are know there will be regular updates and patches to email servers and clients. For real-time identification and mitigation of threats advanced detection and response tools will be implemented. In addition to the malware protection, to defend the system against recent threats there will be regular updates to the antivirus and anti-malware software.

When discussing network security there is a need to limit the amount of malware that may be spread between segments, so to limit that there will be enhancement made to the network segmentation and access controls. Also, to promptly identify and respond to suspicious activities in the network there will be an implementation of strict anomaly detection and network monitoring. Regular cybersecurity training and phishing simulations will be conducted to address user training and awareness, so employees can be educated on potential threats and have the ability to address these threats properly. The IT department also can take immediate action due to the establishment of a protocol for reporting suspicious emails and activities that is clear and concise.

To ensure company preparedness there will be development of an incident response plan that is routinely updates to adapt to the constantly evolving cyber security threats. This incident response plan will outline steps for addressing security incidents and it will also include regular company drills. To safeguard vital company information there will be implementation of secure and regular data backup and recovery procedures. And in if there is a security incident data needs to be capable of being promptly and effectively recovered, so to ensure this there will be periodical tests performed on the backup restoration processes. Finally, to enhance the security of company accounts and strengthen access management multi-factor authentication and strict password policies will be put in place. To make sure that only authorized personnel holds access to sensitive information there will be regular reviews of user access rights and permissions.

Plan for implementation

A structured implementation plan has been established to make sure the information assurance policies and procedures that were proposed will successfully be employed. The planned duration of this policy and procedure rollout is about 6 months. In month one, what will is occur is initial assessment will be carried out, extensive policy documentation will be finalized, and implementation of advanced email filtering, phishing detection, and malware detection tools. During the second and third months, the attention will shift to enhancement of access management and the segmentation of the networks. Also, periodic phishing simulations and cybersecurity training will be launched for all of ABC Inc.'s employees. During the fourth month, an extensive incident response plan will be created and put into action, establishment of secure procedures for data backup, and examination of backup restoration processes. Lastly, in the fifth and sixth months of the implementation plan, there will be enforcement of multi-factor authentication and secure password policies. Also, during these months there will be reviewal,

and updates made to the user access rights and permissions. There will also be the addition of regular training and revisions to the incident response plan will be carried out.

For accountability assurance there has been clear establishment of the roles and responsibilities. The responsibility of the IT sector is to deploy email security measures, implement malware protection tools, and improve the network security. The IT team will also perform routine training sessions and simulations of phishing incidents. The OT team role is to aid the IT team to make sure the manufacturing processes are not interrupted by the access control measures and segmentation of the networks. They will also take part in the incident response drills that will occur periodically. There's also a team of external cybersecurity experts that will be employed to aid in the deployment of malware detection and advanced email filtering mechanisms. These external cybersecurity experts will also be tasked with enhancement of the indent response plan, providing specialized training, and carrying out phishing simulations. The responsibility of the Chief Information Assurance Officer (CIAO) is to manage the implementation of the process, making sure this process aligns with the objectives and regulatory requirements of ABC Inc. The HR department's role in the implementation process is to supervise the programs for user training and awareness. Finally, the responsibility of the finance department is to oversee the budget and the distribution of resources for cybersecurity efforts.

There will be diligent management of the budget and distribution of resources. ABC Inc.'s finances will be designated to the employment of external cybersecurity experts, obtaining security software and tools that are advanced, routine training, and tools used for phishing simulation. During the implementation phase the budget will also cover the IT and OT teams overtime and additional employment. To make sure the resources are utilized effectively and the

implementation timeline is complied with ABC Inc.'s spending will be meticulously monitored, so the required adjustments can be made.

Evaluation and monitoring

A vigorous monitoring and evaluation framework will be developed, so we can confirm that information assurance policies and procedures that were established are sufficient. The monitoring and evaluation framework will include all the organizations information assurance policies and procedures carrying out periodic audits and assessments. These audits and assessments that will regularly occur will evaluate the adherence and employment of the information assurance policies and procedures. The audits and assessments will provide suggestions on how to improve ABC Inc.'s cybersecurity defenses and detect any flaw and gaps.

Also, to identify where there is a need for improvement we will seek employees, external experts, and partner feedback. Because ABC Inc. collects this information, we as a company can sufficiently adapt IA policies and procedures to address new and cybersecurity threats. This is due to the feedback employees, stakeholders, and external experts providing us with information about threat landscape alterations, best practice advancements, and emerging risks.

Additionally, to measure how effective the information assurance policies and controls we implement are ABC Inc. can develop key performance indicators (KPIs) and metrics. The se key performance indicators (KPIs) may include detection rates of malware, return on investment (ROI), phishing awareness scores, response times to incidents, and many others. ABC Inc. can create informed decisions based upon data by gauging policy performance and metric tracking.

Conclusion

In summary, significant vulnerabilities ABC Inc.'s cybersecurity defenses were exposed during recent ransomware incident that occurred in the company's IT segment, such as operational disruptions, which led to financing and reputational damages. So, to strengthen ABC Inc.'s cybersecurity defenses prevent future company breaches, we have designed a thorough Information assurance policy and procedure proposal. This proposal includes advanced email security, powerful malware protection, improved network security, regulatory user training, a comprehensive incident response plan, a data backup and recovery plan that is secure, strict authorization and access management protocols.

It cannot be stressed enough the importance of regular monitoring and creating a strong and thorough set of information assurance policies. It is dire for employees to commit to these updated policies and procedures to maintain strong cyber defenses and adapt to the continuously evolving cyber threats. We are able to safeguard ABC Inc.'s day-to-day operations and protect not only operational but customer sensitive data if we cooperate and remain aware which will ensure ABC Inc.'s success and security.

Appendices

On day 1 the phishing email that contains malicious Excel spreadsheet attachment is received by an administrative support employee. 10 minutes later the administrative support employee activates the Zloader malware by opening the email. The now successful Zloader malware starts to harvest login credentials and passwords. Day 19, the Ryuk ransomware is deployed this ransomware encrypts the data of more that 40 computers that are held in the IT segment. This ransomware has now successfully disrupted financial and administrative operations. Day 24, mitigation methods are implemented by ABC Inc.'s internal technical support. Along with the in-house support mitigation efforts management decides to bring

cybersecurity experts from outside the company to aid in these efforts. Day 29, the ransomware and compromised files are completely removed from the system by the external cybersecurity team. Thus, allow all of ABC Inc.'s day-to-day operations to continue.

References

[1] Andrew Blyth and Gerald Kovacich, Information Assurance, Security in the Information Environment, Springer-Verlag Ltd, London, 2006.

[2] Cisco. (2024, March 15). How is OT different from it? OT vs. it. Cisco. https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html#:~:text=IT%20is%20the%20technology%20backbone,securing%20an%20organization's%20industrial%20operations.

[3] Greg Belding, Zloader: What it is, how it works and how to prevent it, https://resources.

infosecinstitute.com/topic/zloader-what-it-is-how-it-works-and-how-to-prevent-it-

malware-spotlight/, 2020.

[4] Implementation plan template and examples. (n.d.). https://www.implementationpractice.org/wp-content/uploads/2021/05/NIRN-CIP-Implementation-Plan-Template-and-Examples-fillable-v1.pdf

[5] John Klossner, Untitled, http://www.jklossner.com/humannature/

wktpnx3p7sqi73aj18g1fglmbswg92, 2006.

[6] Malwarebytes Staff, Ryuk ransomware, https://www.malwarebytes.com/ryuk-ransomware, 2021.

[7] Managing threats and business disruption risk. Resolver. (2023, September 15). https://www.resolver.com/blog/threats-business-disruption-risk/#:~:text=Any%20of%20these%20breakdowns%20can,and%20may%20cancel%20their%20contracts.

[8] Mark Twain, Following the equator: a journey around the world, Harper & Brothers, 1903.

[9] Robert a Heinlein, Time Enough for Love, G. P. Putnam's Sons, 1973.

[10] Sean Gallagher, Dr. Strangenet - or, how i stopped worrying and embraced the WFH IT apocalypse, https://arstechnica.com/features/2020/11/future-of-collaboration-03/, 2020.