Final Project

Information Assurance Cybersecurity

Ashley Barasebwa

Old Dominion University

9 December 2024

Table of Contents

Information Assurance Policies and Procedures for ABC Inc.

1 Summary

ABC Inc., a small manufacturing company, suffered a severe ransomware attack that compromised its internal network and disrupted financial and administrative operations for a few weeks. The breach originated from a phishing email received by an administrative support employee, containing a malicious Excel spreadsheet. Within 4 minutes of opening the file, a version of Zloader malware was installed, which harvested login credentials over a three-week period. This led to the deployment of Ryuk ransomware, encrypting files across 40 computers on the IT segment of the network. Also, the financial and administrative system was locked down with ransomware demands. Operations in the engineering and manufacturing programmable logic controllers (PLC) segment were unaffected, which allowed manufacturing processes to continue. External cybersecurity experts resolved the issue by removing malicious files from the ABC Inc. network and restored full company activities.

2 Background Section

ABC Inc. employs approximately 1,000 people and operates in the manufacturing sector. The company's success depends on its ability to maintain uninterrupted production and efficient financial operations. ABC's key commercial responsibilities include fulfilling customer orders, paying vendors, and managing intellectual property related to its manufacturing processes. The company's key and corporate alliances include partnerships with suppliers, customers, and industry stakeholders who depend on ABC's reliability. The company's network infrastructure is logically segmented into two parts, consisting of the administrative/financial segment, and then

the engineering/manufacturing segment. The administrative/financial segment can be associated with Information Technology (IT), while the engineering/manufacturing segment can be associated with Operational Technology (OT). The administrative segment can be characterized as the IT side, due to the handling of financial and administrative operations, including accounts receivable and payable. The manufacturing segment can be characterized as the OT side, due to overseeing engineering and manufacturing processes, including programmable logic controllers (PLCs).

Both the IT and OT segments share a common infrastructure connected by a custom enterprise resource planning (ERP) system. Employees have personalized email accounts for internal and external communication. While segmentation provides some level of protection, the shared infrastructure and reliance on email communications create vulnerabilities. Strengths that the network infrastructure has is a logical network segmentation that reduces the risk of a total system compromise. Another strength is that the OT segment remained operational during the attack, which mitigated the impact of the ransomware attack. Weaknesses in the network infrastructure consist of the lack of email filtering and employee training to avoid phishing attacks. Also, insufficient monitoring allowed malware to operate for three weeks. Lastly, shared infrastructure introduces risks if one segment is compromised.

3 The Consequences

The consequences of the breach had significant disruptions for the ABC Inc. company such as financial costs, data compromise, reputational damage, and operational disruption. Financial costs were a disruption due to the company not being able to bill its customers or pay its vendors for three weeks. Also, financial expenses included hiring external cybersecurity experts, restoring

compromised systems, and potential loss of business opportunities during downtime. Data compromise was an interruption due to the login credentials harvested by Zloader, which may have exposed sensitive financial and administrative data, increasing the risk of future breaches. The data compromise could have also exposed customer data, which could lead to lawsuits and legal actions taken against the ABC Inc. company. The reputation of ABC may have raised concerns among customers, suppliers, and partners about ABC's ability to secure its network and intellectual property. Operational disruption was a disturbance because financial and administrative operations were halted, preventing the company from billing customers and paying vendors for three weeks. This definitely damaged cash flow and strained relationships with partners and other organizations.

4 Security

To prevent future network breaches, ABC, Inc. should implement a comprehensive information assurance (IA) program focusing on preventive measures, monitoring, and employee training. A comprehensive information assurance program is necessary, as that is the only measure where we can ensure that data is stored in authorized and protected spaces in the network. Email security is important, due to an employee opening an attachment on an e-mail from a malicious entity. Advanced email filtering solutions to block phishing emails and malicious attachments are necessary. Also, Domain-based Message Authentication, Reporting, and Conformance (DMARC) should be implemented in our measures to reduce spoofing risks.

Employee training consists of regular cybersecurity awareness training for all employees, which emphasizes phishing recognition and reporting. The simulation of phishing attacks should also be used to assess and improve employee responses every 6 months. An incident response

plan is necessary, the plan should include the appropriate staff that will be available to respond to incidents, as well as the responsibilities and communication channels during a cyber incident. The incident response plan should be regularly tested through tabletop exercises and simulations. By implementing the recommended measures, ABC Inc. can significantly reduce the risk of future incidents, protect its proprietary information, and maintain trust with its stakeholders.

5 References

Dmarc. Org – domain message authentication reporting & conformance. (n.d.). Retrieved December 10, 2024, from https://dmarc.org/

InfoSec Institute. (2022, June 1). *ZLoader: What it is, how it works, and how to prevent it [Malware spotlight].* Retrieved December 10, 2024, from https://www.infosecinstitute.com/resources/malware-analysis/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/