Secure Architecture Report

Executive Summary

The mid size e-commerce company is looking to expand and requires added security measures to ensure the safety of their customers and their own network. Due to the rapid growth of the company, the basic security measures that are already in place need to be re-evaluated and restructured to suit the current needs of the company. The current security measures of the company include a network topology that is connected to a single network segment with no hierarchy for management (flat network structure), inadequate network monitoring, inadequate endpoint security, and inadequate network monitoring.

Introduction

The purpose of this document is to establish updated security measures, an evaluation of current assets, and establish updated monitoring methods, in accordance with the NIST framework (National Institute of Standards and Technology). In updating the current framework, its security measures, and monitoring methods, this document will provide a step by step evaluation and recommendation structure to enhance the current security measures and to patch possible vulnerabilities.

Scope of the Report

The scope of the report will include a detailed analysis of the current security landscape taking into account the risks and vulnerabilities of the network and the companies systems. The action plan will include a structured timeline for implementation, parties responsible for the acceptance of the risks included with updated security measures if any. Finally, Along with the action plan will be the implementation of the NIST framework (National Institute of Standards and Technology) in accordance with the action plan to ensure effective security precautions for the company's assets.

Assessment Limitations

There are a number of variables to consider when undergoing a security architecture evaluation. Resource and budget allocations based on prioritized assets may need to be taken further security measures are taken, this document will provide resource and budget friendly solutions. Another limitation would be employee awareness. Educating employees on the current threat landscape and industry best practices, as well as adhering to security policies are dependent on the employees. These measures are the responsibilities of the employees as well as the security team to ensure employees are using and adapting the recommended security measures and policies. The other limitation is that this document does not adapt to the external threat landscape which changes rapidly over time, but rather provides insight on the internal security architecture, and provides best practices in accordance with the NIST framework for a more secure network to protect the valuable assets of the company.

Vulnerability and Risk Assessment

Investigating the network topology it can be noted that there are a variety of vulnerabilities that can open the network up to possible threats as follows:

- **Lack of network segmentation**: Network segmentation is used for network administrators to better control the flow of network traffic and to improve the network's performance and security.

- **Single Server Hosting:** Hosting multiple services on a single server, which can lead to attackers using a variety of attacks that would target the server, which will shut down all services connected to that server.

- **Weak Access Controls:** The network seems to rely on simple passwords which increases the risk of unauthorized access.

- **Sensitive Data Storage Location:** Sensitive data being stored next to the e-commerce website poses a great risk to the data.

- **Outdated Endpoint Security:** The outdated endpoint security allows for the exploitation of malware and any other breaches.

- **Weak Wifi Security:** This increases the risk of unauthorized network access and without the proper network monitoring, this decreases response times for mitigation responses.

Security Architecture Goals

The goals to secure the network and valuable assets of the company are as follows:

Customer Data: Ensuring customer data's confidentiality, integrity, and availability to maintain trust in the service

Business Continuity: Ensuring that preventative measures and mitigation processes are readily available and enacted in a timely manner to prevent threats that attack services, which would impact the company in many ways including financially.

Future Growth Plans: Allow an adaptable and manageable process to carry through operations when the company expands more in customer base, and requires more services.

Security Policies and Procedures: Documenting and updating policies for consistent compliance with best practices and regulations.

Risk Mitigation: Identifying and mitigating vulnerabilities to reduce the risk of security breaches.

Customer Trust: Implementing strong security measures to secure customer information.

Incident Response: Having proper monitoring methods to allow for an effective remediation and mitigation process in response to incidents.

Compliance with Security Regulations: Complying to proper security and legal regulations to ensure the company is within its legal obligations, and to avoid legal repercussions and penalties for not having the necessary regulations.

Access Control and Authentication: Implement strong access controls and multi-factor authentication to protect sensitive data.

Endpoint Security: Ensuring the security of employee workstations with up-to-date security solutions and patch management.

Network Security: Strengthening wireless network security, implementing network segmentation, and implementing effective monitoring systems.

Continuous Improvement: Adapting to evolving threats through regular reassessment of security measures and strategies.

Recommendations

The recommendations for security measures to be made for further network security are measures such as network segmentation, server separation, MFA (Multi-Factor Authentication), etc. The recommendations being made in relation to the vulnerabilities assessed and observed from the earlier vulnerability assessment. Server separation will allow for the monitoring of network traffic, turning different services off temporarily while others are running, and the mitigation of the risk of attacks with the intention of shutting down services. Enabling MFA on employee and customer accounts will help prevent unauthorized access to the network. Finally, network segmentation can be used to separate critical systems from less critical systems, to minimize lateral movement on the network. Lateral movement is a technique used by attackers to move through a network in search of sensitive data.

Regular endpoint security updates and patch management are important to the security of the employee workstations, to protect against threats such as malware attacks. In relation, ensuring that employees are trained in security awareness regularly, will mitigate the risks of vulnerabilities due to uninformed individuals not using strong security measures. Introducing advanced IDS/IPS (Intrusion detection and prevention systems), will allow network analysts to monitor network traffic, detect anomalies in the network, and prevent potential threats to the network. Documentation of security policies and procedures will align with best practices and regulations, to allow for the amendment of security policies and procedures based on the threat landscape. Strengthening wireless network security through encryption services such as WPA3 (Wi-fi Protected Access 3) to reduce unauthorized access to the services provided. Finally, undergoing regular security assessments and compliance monitoring, in order to continue improving security by identifying newer and more possible vulnerabilities to allow for effective and timely mitigations. Doing these inspections regularly will not only be proactively threat hunting, but would also be in compliance with legal security policies.

Implementation Strategy

The Implementation strategy is made with monetary and resource constraints in mind to accommodate for the possible constraints. The implementation strategy goes as follows:

Phase 1: Security Enhancements (Months 1 - 3)

Objective: To assess vulnerabilities and risks, and to implement improved security.

Key Actions: Wireless network improvements (ie, network segmentation), Dedicated server setup, strong access controls, basic intrusion detection implementation.

Timeline: The first month should be dedicated to setting up improved network architecture. The second month would be dedicated to setting up access controls and better account security through MFA. The third month would be dedicated to setting basic intrusion detection methods and monitoring systems.

Phase 2: Security Measure Improvements (Months 4 - 6)

Objective: The objective of this next phase is to implement enhanced network security, detection, and monitoring capabilities .

Key Actions: Advanced intrusion detection and prevention system (IDS/IPS), Implementing enhanced employee security training, and amendments or additions to security policies and procedures.

Timeline: The fourth month would be dedicated to more network improvements, such as network segmentation if that has not been implemented yet, if it has, network monitoring systems should be implemented as well. The fifth month should be dedicated to implementation of advanced IDS/IPS setup. The sixth month would be dedicated to the development of more improved security policies and procedures as they should be updated as more network advancements are implemented.

Phase 3: Continuous Improvements and Compliances (Months 7 - 12)

Objective: These next months are dedicated to any other improved methods of network and mechanisms, as well as ensuring there is compliance with legal and security regulations.

Key Actions: These actions will be carried on beyond the months as they are recommended for best practice to implement regular security, procedure, and policy assessments for regular updates. Carrying on education of employees awareness.

Timeline: This timeline is ongoing, as such each of these actions and implementations should be done in accordance with any governing laws of security assessment, or as needed by the company. Carrying out regular inspection and awareness training will help prevent easy unauthorized access.

Conclusion

To finalize this document, the assessments provided should bring to light the current vulnerabilities in the system described above. Awareness of these vulnerabilities and awareness of how to mitigate or take preventative measures to improve network security to elevate the trust in security measures taken when dealing with customer and employee sensitive data. The recommendations are some of the best and budget friendly ways of remediation, but there can be more security measures implemented that are not in the scope of this document. Finally, the action plan is another recommendation to implement a strategy to remedy the vulnerabilities presented throughout the document.

Work Cited

Cybersecurity framework. NIST. (2023, October 27). https://www.nist.gov/cyberframework

GeeksforGeeks. (2021, September 27). *What is network segmentation?*. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-network-segmentation/

What WPA3 is and how it differs from WPA2. NetSpot. (n.d.). https://www.netspotapp.com/blog/wifi-security/what-is-wpa3.html

Landsberger, D. (2023, October 6). *What is network segmentation and why does it matter?*. CompTIA. https://www.comptia.org/blog/security-awareness-training-network-segmentation

What is ids and IPS?: Juniper Networks Us. Juniper Networks. (n.d.). https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html