Secure Architecture Report and Recommendations

Scott Maclean
Dec 2024

Table of Contents

Executive Summary

This report presents the findings of a security assessment conducted on a mid-sized e-commerce company. The assessment, guided by the NIST Cybersecurity Framework, reveals critical vulnerabilities in the company's current infrastructure, primarily stemming from a flat network architecture, weak access controls, inadequate monitoring, and a single point of failure in their central server setup. These weaknesses expose the company to significant risks, including data breaches, service disruptions, and financial losses. This report outlines an actionable plan based on NIST guidelines to address these vulnerabilities. The plan prioritizes tasks based on risk and feasibility, providing a clear roadmap for the company to enhance its security posture. Immediate actions include network segmentation, strengthening access controls, and implementing basic monitoring. The ultimate goal is to protect sensitive data, ensure business continuity, and build a resilient security architecture that can adapt to the evolving threat landscape.

INTRODUCTION

This report details the findings of a security architecture assessment conducted for a mid-sized e-commerce company. The purpose of this report is to provide a clear understanding of the company's current security posture, identify vulnerabilities and weaknesses, and recommend improvements to strengthen their overall security. The assessment was conducted using the NIST Cybersecurity Framework as a guide, focusing on the "Identify" phase to establish a baseline understanding of the company's assets, risks, and existing security measures.

Scope: The assessment covered the company's network infrastructure, web server, database server, payment gateway, employee workstations, and wireless network.

Limitations: The assessment was based on the information provided by the company and a review of their network topology diagram. A more in-depth assessment, including penetration testing and vulnerability scanning, would provide further insights but was outside the scope of this initial evaluation.

Current Security Landscape

The company's current security landscape presents several significant vulnerabilities that require immediate attention. The flat network architecture, coupled with weak access controls and a lack of network segmentation, creates an environment where a single compromised device could potentially expose the entire network to attackers. The central server, hosting the web server, database, payment gateway, and certificate server, represents a single point of failure and a highly attractive target for malicious actors. Outdated endpoint security solutions on employee workstations and inadequate network monitoring further increase the risk of successful attacks.

Key Vulnerabilities and Risks:

Flat Network: Lack of network segmentation allows attackers to move laterally across the network easily.

Single Point of Failure: The central server hosting multiple critical services presents a significant risk if compromised.

Weak Access Controls: Default or simple passwords, and a lack of multi-factor authentication (MFA), increase the risk of unauthorized access.

Outdated Endpoint Security: Employee workstations are vulnerable to malware and exploits due to outdated and unpatched security software.

Insufficient Monitoring: The absence of network monitoring and intrusion detection systems hinders the ability to detect and respond to security incidents effectively.

Lack of Data Encryption: Unclear if sensitive data at rest and in transit is adequately encrypted.

Inadequate Backup and Recovery: Backup procedures are undefined or not tested regularly, leading to potential data loss.

Lack of Security Awareness Training: Employees may be susceptible to social engineering attacks due to a lack of awareness.

Overview of the Existing Architecture/Topology

The company currently utilizes a flat network architecture. Key components include:

- Internet Connection: Broadband connection from a local ISP.
- Router: Manages traffic flow and connects to the ISP.
- Firewall: Filters incoming and outgoing traffic based on predefined rules.
- Central Server: Hosts the e-commerce website, database, payment gateway, and certificate server.
- Internal Network: A single network segment connecting all devices, including employee workstations, printers, and other resources.
- Employee Workstations: Desktop computers or laptops used by employees, protected by outdated endpoint security solutions.
- Wireless Network: Wi-Fi network for employee and guest access, secured with simple username and password authentication.
- Network Monitoring: No effective network monitoring or intrusion detection system is in place.

Weaknesses of this topology:

- Lack of segmentation exposes the entire network to threats if one part is compromised.
- The central server is a single point of failure.
- Weak access controls and outdated security software increase vulnerability.
- Inability to effectively monitor network traffic for malicious activity.

Security Architecture Goals

The recommended security architecture aims to achieve the following goals:

Protect Customer Data: Safeguard sensitive customer information, including personal details and payment data, from unauthorized access, use, or disclosure.

Ensure Business Continuity: Minimize downtime and maintain business operations in the event of a security incident or disaster.

Compliance: Meet relevant industry standards and regulatory requirements (e.g., PCI DSS for payment card data security).

Scalability: Support future growth and adapt to evolving security threats.

Improved Security Posture: Enhance the overall security posture of the company to reduce the risk of successful cyberattacks.

NIST Action Plan

The following action plan aligns with the NIST Cybersecurity Framework core functions: Identify, Protect, Detect, Respond, and Recover.

1. Identify:
Asset Inventory: Maintain a comprehensive inventory of all hardware and software assets, including servers, workstations, network devices, applications, and data repositories. (Priority: High)

Risk Assessment: Conduct regular risk assessments to identify, analyze, and prioritize threats and vulnerabilities specific to the company's environment and business operations. (Priority: High)

2. Protect:
Network Segmentation:
Implement VLANs to segment the network into isolated zones (e.g., web server, database server, payment gateway, employee workstations, guest Wi-Fi). (Priority: High)

Configure firewall rules to strictly control traffic flow between segments. (Priority: High)

Access Control:
Implement strong password policies (complexity, length, regular changes). (Priority: High)

Enforce multi-factor authentication (MFA) for all user accounts, especially privileged accounts and remote access. (Priority: High)

Adhere to the principle of least privilege, granting users only the minimum access required. (Priority: High)

Implement a centralized directory service (e.g., Active Directory) for user management. (Priority: Medium)

Data Security:
Implement full-disk encryption for servers and workstations. (Priority: Medium)

Encrypt sensitive data at rest within databases. (Priority: Medium)

Ensure all payment transactions are processed over HTTPS using strong TLS protocols. (Priority: High)

NIST Action Plan

Implement Data Loss Prevention (DLP) solutions to monitor and prevent data exfiltration. (Priority: Low)

Endpoint Security:
Deploy and maintain up-to-date endpoint protection (antivirus, anti-malware) on all devices. (Priority: High)

Implement a patch management process to ensure timely updates for all systems. (Priority: High)

Consider application whitelisting to restrict the execution of unauthorized software. (Priority: Low)

Separate the web, database, payment gateway, and certificate server into their own individual servers. (Priority: High)

3. Detect:
Intrusion Detection/Prevention System (IDS/IPS): Deploy an IDS/IPS to monitor network traffic and identify/block malicious activity. (Priority: Medium)

Security Information and Event Management (SIEM): Implement a SIEM system to aggregate and analyze security logs from various sources for centralized monitoring and threat detection. (Priority: Medium)

4. Respond:
Incident Response Plan: Develop a comprehensive incident response plan that defines procedures for handling security incidents. (Priority: Medium)

Incident Response Team Training: Conduct regular training and tabletop exercises to prepare the incident response team. (Priority: Low)

5. Recover:
Backup and Recovery: Establish a robust backup and recovery plan. Regularly test backups to ensure data can be restored effectively. Store backups securely offsite. (Priority: High)

Implementation Strategy

Prioritization of Tasks Based on Risk

The tasks have been prioritized based on their potential impact on reducing risk and their feasibility of implementation:

High: Immediate action required. These tasks address critical vulnerabilities and should be implemented as soon as possible.

Medium: Important tasks that should be addressed in the short to medium term.

Low: Tasks that can be implemented in the longer term or as resources permit.
Roadmap for the Company

Phase 1: Immediate Remediation (1-3 Months)
Focus: Addressing critical vulnerabilities and establishing a basic security foundation.

- Implement network segmentation.
- Enforce strong password policies and MFA.
- Deploy and update endpoint protection.
- Establish a backup and recovery plan.
- Separate servers.

Phase 2: Enhanced Protection (3-6 Months)
Focus: Building upon the foundation and implementing more advanced security controls.:

- Deploy IDS/IPS.
- Implement data encryption at rest and in transit.
- Develop an incident response plan.
- Implement a centralized directory service.

Phase 3: Continuous Improvement (6-12 Months and Ongoing)
Focus: Maturing the security program and adapting to the evolving threat landscape.

- Implement a SIEM system.
- Implement DLP solutions.
- Conduct regular security awareness training.
- Implement application whitelisting.
- Conduct regular vulnerability scanning and penetration testing.
- Conduct regular risk assessments.

Conclusion

The e-commerce company's current security posture presents significant risks to its operations and customer data. Implementing the recommendations outlined in this report is crucial to strengthen its security architecture, mitigate identified vulnerabilities, and protect against evolving cyber threats. The phased implementation strategy provides a manageable roadmap for achieving a more secure environment. By prioritizing security and investing in the necessary resources, the company can significantly reduce its risk exposure, safeguard its reputation, and ensure its long-term success. Continued vigilance, regular security assessments, and ongoing employee training are essential to maintaining a strong security posture in the face of an ever-changing threat landscape.