Security Architecture Report and Recommendations

By Heather Fincati

April 15, 2024

Image generated using gemini

Executive Summary

This report outlines security architecture recommendations to address vulnerabilities identified within the mid-sized e-commerce company's network. This company's impressive online growth, from a small startup to its current size, has also made it a more attractive target for cyberattacks The recommendations leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework Small Business Quick Start Guide [1] and prioritize actions based on risk and feasibility. This assessment aims to identify and address any weaknesses in the company's cybersecurity infrastructure. Implementing these measures will significantly enhance the company's security posture and protect critical assets like customer data and financial information. Here's an overview of the key areas covered in this report to help you understand the findings.

Introduction

This report details the results of a security assessment conducted to identify and address weaknesses in the e-commerce company's network security architecture. The assessment leveraged the Identify Function of the NIST Cybersecurity Framework [1], highlighting key areas for improvement.

Current Security Landscape

The organization currently faces challenges in coordinating and automating response actions during security incidents.The current security architecture utilizes a flat network with limited access controls, weak authentication methods, and outdated security software. This exposes the company to various threats, including unauthorized access, data breaches, and malware attacks.

Security Architecture Goals

The primary goals of the recommended security architecture are:

- Enhance data security and privacy for customers, complying with relevant regulations like the General Data Protection Regulation (GDPR) [2].
- Strengthen overall network security posture.
- Improve incident detection and response capabilities.
- Ensure compliance with relevant industry regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) [3].
- Support future growth and scalability of the business.

Security Architecture Recommendations

4.1 Application Security

Implement multi-factor authentication (MFA) for user logins to the e-commerce website and internal systems. MFA adds an extra layer of security beyond just usernames and passwords, making it more difficult for unauthorized users to gain access.
Enforce role-based access control (RBAC) to restrict user access based on their roles and responsibilities. RBAC minimizes the risk of privilege escalation by granting users only the permissions they need to perform their jobs.
Conduct regular vulnerability assessments for the e-commerce platform and payment gateway. Identifying and patching vulnerabilities in a timely manner is crucial to preventing attackers from exploiting them [1].

4.2 Data Security

Encrypt customer data at rest and in transit using industry-standard encryption algorithms like AES-256. Encryption renders data unreadable to anyone who doesn't possess the decryption key.
Implement a separate server dedicated to storing customer data, isolated from the web application server. This reduces the attack surface and potential damage if a breach occurs on the web server.
Develop and enforce data retention and disposal policies. These policies ensure data is retained only for as long as necessary and disposed of securely when no longer needed.

4.3 Device Security

Deploy a centrally managed endpoint security solution with anti-malware, intrusion detection/prevention, and firewall functionalities. This comprehensive approach provides multi-layered protection against various threats.
Enforce strong password policies with minimum password length complexity requirements and regular password changes. Strong passwords make brute-force attacks significantly more difficult.
Implement endpoint encryption for sensitive data stored on employee devices. Encryption protects data even if a device is lost or stolen.

4.4 Network Security

Segment the network to isolate public-facing services (e-commerce website, payment gateway) from internal resources. Network segmentation limits the potential impact of a breach on a single segment.
Upgrade the existing firewall to an advanced firewall with application-level inspection functionalities. This provides deeper inspection of network traffic to identify and block malicious activity.

Implement an Intrusion Detection/Prevention System (IDS/IPS) to monitor network traffic for suspicious activity. IDS/IPS systems can detect and prevent attacks in real-time.

4.5 Identity and Access Management (IAM)

Implement multi-factor authentication for access to the internal network and resources. As mentioned earlier, MFA adds an extra layer of security beyond passwords.
Enforce strong password policies for wireless network access points. Strong passwords make it more difficult for unauthorized users to connect to the network.
Conduct regular user access reviews to ensure continued validity of access privileges. This helps prevent unauthorized access by removing access for users who no longer require it.

4.6 Detection and Response

Implement a Security Information and Event Management (SIEM) system to centralize log collection and analysis from various security tools. A SIEM system provides a holistic view of security events across the network, helping to identify and respond to threats more effectively.
Develop an incident response plan outlining procedures for identifying, containing, and recovering from security incidents. A well-defined incident response plan ensures a coordinated and efficient response to security breaches. Conduct regular security awareness training for employees to educate them on cybersecurity best practices.

Implementation Strategy

A phased approach is recommended for implementing the security recommendations, prioritizing high-risk vulnerabilities and considering the company's resources and budget constraints.

Phase 1 (High Priority - 3 Months)

Implement multi-factor authentication for critical systems (e-commerce website, internal network).
Upgrade endpoint security software on employee devices.
Segment the network to isolate public-facing services from internal resources.
Develop and implement an incident response plan.
Conduct security awareness training for employees.

Phase 2 (Medium Priority - 6 Months)

Implement role-based access control for internal systems.
Implement data encryption for customer data at rest and in transit.
Upgrade the firewall to an advanced model with application-level inspection.

Deploy an Intrusion Detection/Prevention System (IDS/IPS).

Phase 3 (Low Priority - Ongoing)

Conduct regular vulnerability assessments of applications and network infrastructure.
Review and update user access privileges based on roles and responsibilities.
Implement endpoint encryption for sensitive data on employee devices.

Conclusion

Implementing the recommended security architecture will significantly improve the e-commerce company's security posture and mitigate potential threats. The phased approach ensures a practical and resource-conscious implementation, prioritizing critical security measures. Continuous monitoring, vulnerability management, and user education are crucial for maintaining a strong security posture.

References

1. National Institute of Standards and Technology (NIST). Cybersecurity Framework 2.0: Small Business Quick-Start Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
2. General Data Protection Regulation (GDPR). https://gdpr-info.eu/
3. Payment Card Industry Data Security Standard (PCI DSS). https://www.pcisecuritystandards.org/