**PROJECT 11**

**Secure Architecture Report and Recommendations**

***By Titobiloluwa (Tito) Ilori***

**EXECUTIVE SUMMARY**

This report highlights the current security landscape of a mid-sized e-commerce company, identifying vulnerabilities and compliance concerns. The primary goal of the security architecture is to fortify data protection, regulatory adherence, and customer trust. Recommendations encompass network segmentation, data encryption, access controls, cloud security, and continuous improvement measures. By prioritizing these actions, the organization aims to establish a resilient security posture aligned with industry standards and future growth requirements. [Here is the link to the video presentation.](https://drive.google.com/file/d/18x_wZmQIfe2KYyp2rTwrMopkkjvJDL6M/view?usp=drive_link)

**1 INTRODUCTION**

The purpose of this report is to provide comprehensive cybersecurity recommendations for a mid-sized e-commerce company. The scope includes an analysis of the company's existing security infrastructure, vulnerabilities, and risk factors across various domains such as network, data, endpoint, IAM, cloud, incident response, and physical security. The report outlines a phased approach for implementing security measures, prioritizing compliance, and cybersecurity requirements.

Limitations in the assessment include the absence of specific company data, the budget set aside to improve security posture, real-time threat intelligence, and the evolving nature of cybersecurity threats, which necessitate ongoing adjustments and updates to the recommendations.

**2 CURRENT SECURITY LANDSCAPE**

In this medium-scale company security architecture case study, there are several vulnerabilities and risks that need to be addressed to enhance the security posture of the network. There are the eleven (11) identified vulnerabilities that have been categorized below:

| **#** |  | **Vulnerabilities** | **Risks** |
| --- | --- | --- | --- |
| **1** | **Flat Network Architecture** | All devices on the same network segment pose a significant risk. If one device is compromised, it can potentially compromise the entire network. | Increased exposure to lateral movement and the potential for widespread damage in case of a breach.1 |
| **2** | **Employee Workstations** | Outdated and unpatched antivirus software on employee workstations. | Vulnerable endpoints may serve as entry points for malware or attacks.2 |
| **3** | **Wireless Network** | Simple or default username and password combinations for Wi-Fi encryption. | Weaker Wi-Fi security can lead to unauthorized access, eavesdropping, or man-in-the-middle attacks.3 |
| **4** | **Access Controls** | Relying mainly on simple username and password combinations for access control. | Weak access controls increase the risk of unauthorized access and privilege escalation.4 |
| **5** | **Network Monitoring and Security Devices** | Lack of effective network monitoring and intrusion detection. | The company is unaware of potential security incidents or ongoing attacks, which can result in delayed response to threats.5 |
| **6** | **Router and Firewall** | While routers and firewalls are in place, their specific configurations and update status are not mentioned. | Misconfigurations or outdated firmware can potentially expose the network to vulnerabilities and attacks.7 |
| **7** | **Database Server** | Combining the web and database server on the same hardware. | A compromise of the web server may lead to unauthorized access to sensitive customer data on the database server.6 |
| **8** | **Internet Connection** | Reliance on a single broadband connection from a local ISP. | Network downtime and disruption of business operations in case of a connection failure. |
| **9** | **Payment Gateway on Web Server** | Hosting the payment gateway on the web server. | Compromising the web server may expose payment transaction data, potentially leading to financial losses and regulatory non-compliance. |
| **10** | **Internal Network** | Lack of strong access controls and reliance on simple username and password combinations. | Insider threats and unauthorized access to critical internal resources.4 |
| **11** | **Web Server** | Hosting both internal business records and the e-commerce website on the same server. | A security breach may result in the exposure of sensitive business records and customer data. |

**3 SECURITY ARCHITECTURE GOALS**

The security architecture recommendations in this document are influenced by key business requirements, compliance considerations, and future growth plans:

**Business Requirements:** The foremost requirement is to protect sensitive customer data, ensuring trust and maintaining the reputation of the e-commerce business. Operational continuity and the ability to support high volumes of online transactions are also critical. Additionally, the need for secure collaboration and remote work capabilities, especially in today's remote work environment, underscores the importance of endpoint and cloud security.

**Compliance Considerations:** Adherence to industry-specific compliance standards, such as PCI-DSS for payment data and GDPR for data privacy, is mandatory. Non-compliance can result in severe financial penalties and reputational damage. Meeting these standards through robust access controls, encryption, and incident response planning is paramount.

**Future Growth Plans:** Anticipating future growth, these recommendations prioritize scalability. This includes secure cloud adoption and capacity planning to accommodate increasing data and customer demands without compromising security. The ability to adapt to evolving cybersecurity threats and regulatory changes is essential to support long-term business expansion.

**4 SECURITY ARCHITECTURE RECOMMENDATIONS**

Here are detailed and specific recommendations using controls enumerated in the NIST Cybersecurity Standard and Compliance Framework (NIST 800-53)8 for various security domains listed below.

***4.1 Network Security***

4.1.1 Implement Network Segmentation: Isolate the e-commerce website and payment gateway in a separate DMZ segment (Firewall = allow only TCP port 443 into the DMZ) to protect them from the internal network using VLANs and firewalls. (NIST 800-53 Control: AC-4 (Information Flow Enforcement))

4.1.2 Intrusion Detection and Prevention: Deploy an IDS/IPS system to monitor and block malicious network traffic. Snort, OSSEC or Suricata open-source IDS/IPS or SIEM solutions can be used to detect and respond to threats in real-time. (NIST 800-53 Control: SI-4 (Information System Monitoring))

4.1.3 Firewall Configuration Review: Regularly review and update firewall rules to ensure they align with security policies and conduct quarterly firewall rule reviews to remove unnecessary rules and tighten security. (Relates to CM-4)

4.1.4 Web Application Firewall (WAF): Deploy a WAF (like ModSecurity or AWS WAF) to protect against web application attacks, such as SQL injection and cross-site scripting (XSS). (Relates to AC-3)

***4.2 Data Security:***

4.2.1 Data Classification and Encryption: Classify data based on sensitivity and use AES-256 encryption to protect customer data in the database and SSL/TLS for securing data in transit. (NIST 800-53 Control: SC-8 (Transmission Confidentiality and Integrity))

4.2.2 Access Controls: Use Azure AD for identity management and enforce MFA for accessing critical resources like the Database server and payment gateway. Implement Separation of Duties and Least privilege principles when accessing sensitive data or resources critical to the business. (NIST 800-53 Control: AC-2 (Account Management); NIST 800-53 Control: AC-3 (Access Enforcement))

4.2.3 Data Retention and Privacy: Define data retention periods and procedures for securely purging customer data that is no longer needed. PCI-DSS recommends a 5-year data retention period.

4.2.4: Secure Order Processing: Implement secure order processing procedures to protect against order fraud and data breaches.

***4.3 Endpoint Security:***

4.3.1 Patch Management: Update all Employee Workstations in the internal network and Microsoft WSUS (patch management system) should be used to automate Windows timely updates across all endpoints. (NIST 800-53 Control: CM-2 (Baseline Configuration); NIST 800-53 Control: CM-6 (Configuration Settings))

4.3.2 Endpoint Detection and Response (EDR): Consider EDR (CrowdStrike, Cisco or Carbon Black) solutions for advanced threat detection and incident response. (relates to NIST 800-53 SI-4)

***4.4 Identity and Access Management (IAM):***

4.4.1 Multi-Factor Authentication (MFA): Enforce MFA (Google or Microsoft Authenticator or DUO Security) for all users accessing critical systems and applications. (NIST 800-53 Control: AC-3 (Access Enforcement))

4.4.2 Privileged Access Management (PAM): Deploy CyberArk or Thycotic Secret Server for privileged account management to tightly control and monitor privileged access. (relates to NIST 800-53 AC-3 and AC-6)

***4.5 Cloud Security:***

4.5.1 Secure Payment Processing: Payment Card Industry Data Security Standard (PCI-DSS) compliance for secure credit card processing.

4.5.2 Cloud Governance and Policy: Create policies for resource tagging, encryption, and access control in AWS Identity and Access Management (IAM).

4.5.3 Cloud Security Monitoring: Use AWS CloudWatch and AWS GuardDuty for monitoring and threat detection in Amazon Web Services.

4.5.4 Secure API Usage: Securely manage and protect APIs used for payment processing and integration with external services.

***4.6 Incident Response:***

4.6.1 Incident Response Plan: Develop and document an incident response plan detailing roles and responsibilities, and procedures for identifying, reporting, and mitigating security incidents. (NIST 800-53 Control: IR-1 (Incident Response Policy and Procedures))

4.6.2 Incident Response Team: Establish a dedicated team with members who have expertise in forensics, malware analysis, and incident handling. (NIST 800-53 Control: IR-3 (Incident Response Team))

4.6.3 Incident Response for Data Breaches: Develop a step-by-step response plan for customer notification, legal compliance, and public relations in case of a data breach.

***4.7 Physical Security:***

4.7.1 Access Control Systems: Implement physical access controls like card readers and biometrics.

4.7.2 Surveillance and Monitoring: Deploy surveillance cameras at critical locations for monitoring. Use IP-based cameras with motion detection and remote viewing capabilities.

4.7.3 Visitor Management: Implement a visitor management system like LobbyGuard or Proxyclick to track and control visitor access.

**5 IMPLEMENTATION STRATEGY**

Here, there is a proposition of a phased approach that allows the organization to gradually strengthen its security posture while considering resource constraints and timelines. Continuous monitoring and adaptation are crucial for sustaining a strong security posture over time.

**Phase 1: Establishing Fundamentals (1-6 months)**

* *Objective*: Lay the foundation for robust security practices.

Resource Requirements: (a) Dedicated security personnel or team. (b) Budget for security tools and services. (c) Time for employee training.

*Timelines*:

* Month 1-2: Formulate security policies and appoint an incident response team.
* Month 3: Perform a comprehensive security assessment.
* Month 4-6: Implement basic access controls, MFA, and firewall reviews.

**Phase 2: Data Protection and IAM (6-9 months)**

* *Objective*: Enhance data security and identity management.

Resource Requirements: (a) Encryption tools. (a) IAM solutions (e.g., PAM). (c) Employee training on data handling.

Timelines:

* Month 7-9: Implement data classification, encryption, access controls, and PAM.
* Ongoing: Educate employees on data protection practices.

**Phase 3: Network and Endpoint Security (9-12 months)**

* *Objective*: Strengthen network and endpoint security.

Resource Requirements: (a) Network security appliances (firewalls, IDS/IPS). (b) EDR solutions. (c) IT personnel for configuration and monitoring.

*Timelines*:

* Month 10-12: Implement network segmentation, IDS/IPS, and EDR solutions.
* Ongoing: Continuously review and update security configurations.

**Phase 4: Cloud and Incident Response (12-18 months)**

* *Objective*: Secure cloud resources and strengthen incident response.

Resource Requirements: (a) Cloud security tools (e.g., WAF, Cloud Monitoring). (b) Incident response plan development. (c) Cloud expertise or consultants if needed.

*Timelines*:

* Month 13-15: Implement cloud governance policies and security monitoring.
* Month 16-18: Develop and test an incident response plan for data breaches.

**Phase 5: Physical Security (18-24 months)**

* *Objective*: Bolster physical security measures.

Resource Requirements: (a) Physical security systems (access control, surveillance). (b) Budget for infrastructure upgrades.

*Timelines*:

* Month 19-21: Install access control and surveillance systems.
* Month 22-24: Implement visitor management procedures.

**Phase 6: Continuous Improvement (Ongoing)**

* Objective: Maintain and adapt security measures.

Resource Requirements: (a) Ongoing budget for security tools, updates, and training. (b) Regular security audits and assessments.

Timelines:

* Ongoing: Regularly review and adapt security measures based on evolving threats and compliance requirements.

**6 CONCLUSIONS**

The key findings underscore the critical need for the mid-sized e-commerce company to promptly implement the security architecture recommendations. Vulnerabilities in network, data, and physical security pose significant risks, demanding immediate action for regulatory compliance and customer trust. To meet the stringent requirements of compliance bodies such as PCI-DSS, HIPAA, and GDPR, it is imperative to strengthen data protection, access controls, and network security. Failure to do so not only jeopardize regulatory adherence but also exposes the company to legal and reputational consequences.

Furthermore, the phased approach outlined here ensures a systematic and manageable implementation of security measures, allowing the organization to address high-priority cybersecurity needs first. By proactively fortifying its security posture, the company not only aligns with compliance standards but also safeguards its reputation and sustains customer confidence in an era where data breaches and cyber threats are on the rise.

[Here is the link to the video presentation.](https://drive.google.com/file/d/18x_wZmQIfe2KYyp2rTwrMopkkjvJDL6M/view?usp=drive_link)

***REFERENCES***

1. What Is a Flat Network? Definition, Benefits, and How It Works | SUSNIGDHA TRIPATHY (February 21, 2023) - <https://www.enterprisenetworkingplanet.com/management/the-risks-and-rewards-of-flat-networks/>

2. The Dangers of Running Outdated and Unpatched Software | International Consulting Group (February 2, 2023) - <https://www.icgi.com/blogs/the-dangers-of-running-outdated-and-unpatched-software#:~:text=Your%20software%20no%20longer%20receives,them%20to%20compromise%20your%20system>.

3. Securing Wireless Networks | CISA (February 1, 2021) - <https://www.cisa.gov/news-events/news/securing-wireless-networks>

4. 11 Common Authentication Vulnerabilities You Need to Know | Andrew Magnusson (December 19, 2022) - <https://www.strongdm.com/blog/authentication-vulnerabilities>

5. Intrusion Detection | KirstenS, Wichers, Jkurucar, kingthorin - <https://owasp.org/www-community/controls/Intrusion_Detection#:~:text=Lack%20of%20intrusion%20detection%20allows,to%20identify%20some%20attack%20traffic>.

6. SHOULD YOUR WEBSITE DATABASE HAVE ITS OWN DEDICATED SERVER? | Luxsci.com (August 24, 2021) - <https://luxsci.com/blog/database-server-dedicated.html>

7. Firewall Configuration | Fortinet.com (2023) - <https://www.fortinet.com/resources/cyberglossary/firewall-configuration>

8. Security and Privacy Controls for Information Systems and Organizations | NIST Joint Task Force Working Group (September 2020) - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>