LIGHTHOUSE LAB

CYBERSECURITY

SECURE ARCHITECTURE REPORT & RECOMMENDATIONS

OLADAPO OLUWAYALE

Content **Page**

Executive Summary 3

Introduction 3

Current Security Landscape 3

Security Architecture Goals 4

Secure Architecture Recommendations 5

Implementation Strategy 6

Conclusion 7

Executive Summary

This report presents an overview of the current security landscape for a mid-sized e-commerce company, evaluates existing vulnerabilities in its infrastructure, and provides comprehensive recommendations for improving the company's security posture. Based on the NIST Cybersecurity Framework, the report suggests mitigation strategies across various domains such as network security, data protection, endpoint security, and incident response. A phased action plan with prioritized tasks is outlined, taking into account the company's resources and budget. The report aims to enhance the company’s cybersecurity posture, ensuring the protection of customer data, secure financial transactions, and overall business continuity.

Introduction

This report is designed to guide the e-commerce company in securing its digital infrastructure and protecting sensitive business data. The scope of the report includes a detailed assessment of the company’s current security landscape, identification of vulnerabilities, and recommendations for improvement. While the report focuses primarily on IT and network security, it is understood that other organizational processes (e.g., employee training, compliance) may also play crucial roles in an overall security strategy, but these are outside the immediate scope of this report.

Current Security Landscape

Existing Security Architecture: The company utilizes a flat network architecture with a shared web and database server. Key vulnerabilities identified include:

1. Lack of Network Segmentation: The web server and database server share the same hardware, increasing the risk of an attack on one system affecting both.
2. Weak Access Control: Many systems, such as employee workstations and internal network services, rely on simple password authentication, which makes them vulnerable to brute force and credential-stuffing attacks.
3. Unencrypted Data Storage: Customer data, including personal information and payment details, is stored without proper encryption, putting it at risk in case of a breach.
4. Inadequate Endpoint Protection: Employee devices run outdated antivirus software and lack regular patching, exposing the organization to known vulnerabilities.

5. Limited Monitoring: The company lacks sufficient intrusion detection and network monitoring tools, leaving it blind to potential threats or breaches.

Vulnerabilities and Risks:

- Data loss or theft due to poor encryption.
- Unauthorized access to sensitive systems due to weak access controls.
- Malware infections or ransomware attacks on outdated endpoints.
- Inability to detect and respond to security incidents in a timely manner.

Security Architecture Goals

Business Requirements:

- Ensure that all customer data (personal, payment, and order history) is protected and complies with data protection regulations (e.g., GDPR, PCI DSS).
- Safeguard the company's intellectual property and internal business operations from cyber threats.
- Maintain a secure e-commerce platform for customers to conduct transactions safely.

Compliance Considerations: The company must comply with legal and regulatory requirements, such as:

- Payment Card Industry Data Security Standard (PCI DSS) for payment processing.
- General Data Protection Regulation (GDPR) for customer data protection.
- Local data protection laws based on the company's operational region.

Future Growth Plans: As the company grows, it must scale its security measures to address an increasing volume of transactions, customer data, and employee devices. This will require a more robust security architecture capable of supporting a larger infrastructure.

Security Architecture Recommendations

1. **Network Security**:
   - Recommendation: Segment the network into multiple zones (e.g., DMZ for public-facing services like the website, internal network for employee devices, and isolated database server). Properly implemented Demilitarized Zones1 (DMZs) and firewalls can prevent a malicious actor's attempts to access high-value assets by shielding the network from unauthorized access. (CISA Feb 3, 2025)
   - Implementation: Deploy VLANs, firewalls with access control lists (ACLs), and network monitoring tools to detect intrusions.
2. **Data Security**:
   - Recommendation: Implement strong encryption both for data in transit (using HTTPS) and at rest (for sensitive customer data). Encrypting data ensures messages can only be read by recipients with the appropriate decryption key. (Fortinet, Feb 3, 2025)
   - Implementation: Use TLS for all web traffic and AES-256 for encrypting customer information in the database.
3. **Endpoint Security**:
   - Recommendation: Ensure that all employee devices are equipped with up-to-date antivirus software and are regularly patched.
   - Implementation: Implement endpoint detection and response (EDR) solutions to monitor and protect all endpoints continuously. (Lighthouse Labs, Feb 3, 2025.)
4. **Identity and Access Management (IAM)**:
   - Recommendation: Implement multi-factor authentication (MFA) and role-based access control (RBAC) across all critical systems. RBAC basically restricts network access based on a person's role within an organization. The roles in RBAC refer to the levels of access that employees have to the network. (Lighthouse Labs, Feb 3, 2025)

   - Implementation: Use identity management solutions to enforce secure access protocols and ensure only authorized personnel can access sensitive data.

5. **Incident Response**:
   - Recommendation: Set up a comprehensive incident response plan with clear procedures for identifying, responding to, and recovering from security incidents. The goal is to effectively manage incidents to minimize damage to systems and data, reduce recovery time and cost, and control damage to brand reputation. (BlueVoyant, Feb 3, 2025)
   - Implementation: Integrate a Security Information and Event Management (SIEM) system for log collection, analysis, and alerting on security events.
6. **Cloud Security**:
   - Recommendation: Secure any cloud services by enabling encryption and proper access control mechanisms.
   - Implementation: Ensure cloud service providers follow the best security practices, and use encryption keys managed internally. Enhanced data protection with encryption at all transport layers, secure file shares and communications, continuous compliance risk management, and maintaining good data storage resource hygiene such as detecting misconfigured buckets and terminating orphan resources. (Check Point Software Technologies, Feb 3, 2025.)

Implementation Strategy

The implementation of security measures will follow a phased approach:

1. **Phase 1: Immediate Action (0-3 months)**:
   - Segmentation of the network (DMZ, internal network, isolated servers).
   - Deploy MFA for access to critical systems.
   - Begin encryption of customer data at rest and in transit.
   - Upgrade endpoint protection (antivirus software, patch management).

2. **Phase 2: Mid-term Action (3-6 months)**:
   - Introduce a comprehensive firewall solution with advanced traffic filtering.
   - Implement centralized logging and deploy SIEM for real-time monitoring.
   - Set up a comprehensive incident response plan and conduct mock incident response exercises.
3. **Phase 3: Long-term Action (6-12 months)**:
   - Fully implement RBAC across all systems.
   - Conduct regular penetration testing and vulnerability assessments to ensure the effectiveness of the implemented controls.
   - Monitor compliance with regulatory requirements (e.g., PCI DSS, GDPR).

Resources Required:

- Network security tools, endpoint protection software, and SIEM systems.
- Cloud encryption services and identity management solutions.
- Personnel for training and monitoring system performance.

Conclusion

The security vulnerabilities identified in this assessment pose significant risks to the company's operations, customer trust, and compliance status. By implementing the recommended security measures outlined in this report, the company can greatly enhance its cybersecurity posture, mitigate risks, and ensure the protection of sensitive data. The phased implementation strategy will allow for a balanced approach, aligning security enhancements with the company's resources and growth trajectory. Prioritizing these actions will help the company maintain the security of its e-commerce platform and safeguard against evolving cyber threats.

Link to the Presentation video

https://drive.google.com/file/d/1--w7S_XBx8FOkF1UmOkmO9vcXqlDR7Pm/view?usp=drive_link

Reference

Cybersecurity and Infrastructure Security Agency. (Feb 3, 2025). *Layering network security with segmentation* [Infographic]. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

Fortinet. (n.d.). *Data security*. Fortinet. https://www.fortinet.com/resources/cyberglossary/data-security

Lighthouse Labs. (n.d.). *Week 10, Day 1 activity*. Lighthouse Labs. https://web.compass.lighthouselabs.ca/p/cyber/days/w10d1/activities/3261

Lighthouse Labs. (n.d.). *Week 10, Day 2 activity*. Lighthouse Labs. https://web.compass.lighthouselabs.ca/p/cyber/days/w10d2/activities/3264

BlueVoyant. (n.d.). *What is incident response? Process, frameworks, and tools*. BlueVoyant. https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools

Check Point Software Technologies. (n.d.). *What is cloud security?* Check Point Software Technologies. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/