Curtis Crawford

2024-10-12

Lighthouse Labs

Secure Architecture Report and Recommendations

Contents

[Executive Summary 1](#_Toc179702808)

[1: Introduction 1](#_Toc179702809)

[2: State of the Security Market. 2](#_Toc179702810)

[3: Security Architecture Objectives 3](#_Toc179702811)

[4: Security Architecture Recommendations 3](#_Toc179702812)

[5. Implementation Plan 5](#_Toc179702813)

[6: Conclusion 5](#_Toc179702814)

[References & Citations 6](#_Toc179702815)

# Executive Summary

**The current security model of the company, which has a flat network layer, poor endpoint security, and unwieldy access controls, is dangerous. The purpose of the security architecture was to secure vital business information, stay in compliance with the standards, and set the company up for future expansion. Some key tips are: network segmentation, improved access control, regular patch management and better monitoring. These security enhancements will also be adoptable in phases that will cause the least amount of impact on the business operations.**

# 1: Introduction

**This report will provide mitigation methods to resolve vulnerabilities discovered in a security architecture assessment on a mid-sized online store. In this report, we look at how to strengthen the cybersecurity of the business by tackling inefficiencies in the network design, access management, endpoint security and incident response abilities. The report finds potential risks, provides solutions to mitigate them, and makes sure the company can protect itself against cyber-attacks and maintain compliance with industry standards.**

**It focuses on assessing the network environment, server environment, endpoint security and access control for the company and suggesting practical recommendations. Time constraints prevented a full review of physical security or employee education.**

# 2: State of the Security Market.

**The current security model is exposing multiple threats to the following vulnerabilities:**

**Flat Network: All devices (web server, payment gateway, employee devices) are shared on the same segment network that makes it vulnerable to cyber attacks.**

**Old Endpoint Security: Staff devices aren’t regularly updated and anti-virus applications are out-of-date, making endpoints vulnerable to malware.**

**Poor Access Security: They just have plain username and password combinations and don’t support MFA, so it is not hard to gain access.**

**No Network Monitoring: It has no IDS or network monitoring to detect and attack threats at the moment of need.**

**One Server With Multiple Services: The web server, payment gateway and database server are all centralized on one server that becomes a major source of failure and can make an impact more likely when there is a breach.**

# 3: Security Architecture Objectives

**The objectives of the proposed security architecture are to:**

**Restoring Vital Business Resources: Safeguard the online storefront, payment gateway, and customer list from hackers.**

**Maintain Regulation Compliance: Security measures that are compliant with compliance with regulatory requirements like the Payment Card Industry Data Security Standard (PCI DSS) for secure payments.**

**Assist with Future Growth: Offer a scalable architecture that will support the company’s future growth in traffic and customer records.**

**Limit Business Interference: Offer solutions that can be implemented with minimum disruption to business as usual while increasing security of the company.**

# 4: Security Architecture Recommendations

**Security in your network, The Network Security:**

**Network Segmentation: Use VLANs to partition the network into separate units (e.g., public in a DMZ, internal network, database server). Use firewalls to regulate traffic between segments.**

**Firewall & Security Updates: Enforce firewall policies to sift through traffic and block unauthorized access to internal resources.**

**Intrusion Detection System (IDS): Install an IDS and watch for network intrusions to find and prevent breaches.**

**Privacy / Security: The Protection of your Data**

**Database Encryption: Encrypt customer data within the database and keep sensitive data safe if you are hacked.**

**Backup and Recovery: Plan a solid data backup system such as weekly backup of the customer database to an offsite location or protected cloud provider.**

**Endpoint Security –**

**Patch Management: Maintain a patch management schedule for all the employee devices, servers, and software.**

**Endpoint Protection: Upgrade antivirus and anti-malware solutions for every employee device, and invest in EDR products to prevent attacks.**

**IAM (Iam ) Identity and Access Management**

**MFA: Set MFA on all users’ logins especially those related to key systems like the payment gateway and the database.**

**Role Based Access Control (RBAC): RBAC allows you to control access based on employees’ position in the company so they are only allowed to access resources for the tasks they perform.**

**Cloud Security Solution:**

**- Encryption of Cloud Storage: Secure the whole cloud data and do not allow any access. Always review cloud service setups to make sure it’s security compliant.**

**Logging and monitoring: Logging and monitoring for all of the cloud services to monitor access and security threats.**

**Incident Response Services for you – Learn more about incident response.**

**Incident Response Plan: Create an official incident response plan, which will cover your protocols in case of a security breach or loss of data.**

**Security Information and Event Management (SIEM): Install a SIEM that collects logs from various locations (firewalls, servers, endpoints) and warns the security team on possible breaches real-time.**

**- Physical Security.**

**Secure Server Rooms: Create physical access control for all areas of IT infrastructure where privileged staff cannot get to sensitive hardware.**

**Monitors: Invest in security cameras and access control systems to log physical entry to the server room.**

# 5. Implementation Plan

**A phased approach is recommended to implement the security in a way that allows for as little disruption to business as possible:**

**Phase 1 (0-3 months):**

**Segmentation and firewall updates of the network.**

**— Enable multi-factor authentication (MFA) — Add MFA and enable multi-factor authentication.**

**Apply endpoint defense and patching solutions.**

**Phase 2 (3-6 months):**

**Encrypt the database and implement backup cycles periodically.**

**Network and cloud monitoring with an IDS/SIEM.**

**Create an incident management plan.**

**Phase 3 (6-9 months):**

**Apply role-based access control (RBAC).**

**Upgrade physical security (if required)**

**Check and configure cloud security settings.**

**Hardware Prerequisites:**

**Group: IT Security, network engineers, cloud administrators.**

**Technologies: IDS, SIEM, MFA tools, encryption, cloud monitoring solutions.**

**Budget: Based on hardware upgrades, software licenses, and potential consulting.**

# 6: Conclusion

**There are severe risks to business and customer information due to the security holes that have been found in the company network. If they follow the recommended security policies, the company is less susceptible to cyber attacks, regulatory compliance and create a scalable, secure environment for further expansion. A gradual rollout will give the company the flexibility to expand its security presence without compromising business operations. Continuous monitoring, updates, and training will be key to keeping the security architecture working well.**

References & Citations  
 **NIST SP 800-125: Guide to Security for Full Virtualization Technologies**

* Citation: National Institute of Standards and Technology (NIST). (2011, January). Guide to Security for Full Virtualization Technologies (SP 800-125). https://doi.org/10.6028/NIST.SP.800-125
* Used in the context of discussing **server virtualization** as a mitigation strategy.

 **NIST SP 800-41: Guidelines on Firewalls and Firewall Policy**

* Citation: National Institute of Standards and Technology (NIST). (2009, September). Guidelines on Firewalls and Firewall Policy (SP 800-41). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>
* Referenced for recommendations on **firewall configuration** and **traffic filtering**.

 **MITRE ATT&CK Framework**

* Citation: MITRE. (n.d.). MITRE ATT&CK Framework. Retrieved October 13, 2024, from https://attack.mitre.org/
* Used as a source for **standard mitigations** and techniques related to network segmentation and traffic monitoring.

 **MITRE CVE (Common Vulnerabilities and Exposures)**

* Citation: MITRE. (n.d.). Common Vulnerabilities and Exposures (CVE). https://cve.mitre.org/
* Referenced in the context of discussing vulnerabilities in **outdated endpoint security** systems.

 **NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems**

* Citation: National Institute of Standards and Technology (NIST). (2011, August). Guide for Security-Focused Configuration Management of Information Systems (SP 800-128). https://doi.org/10.6028/NIST.SP.800-128
* Cited for recommendations related to **patch management** and configuration management processes.

 **NIST SP 800-207: Zero Trust Architecture**

* Citation: National Institute of Standards and Technology (NIST). (2020, August). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207
* Referenced when recommending the adoption of **role-based access control (RBAC)** and **multi-factor authentication (MFA)**.

 **PCI DSS: Payment Card Industry Data Security Standard**

* Citation: PCI Security Standards Council. (2022). PCI DSS v4.0: Requirements and Security Assessment Procedures. https://www.pcisecuritystandards.org/document\_library
* Used in the discussion on **payment gateway security** and ensuring compliance with industry standards.

 **NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations**

* Citation: National Institute of Standards and Technology (NIST). (2013, April). Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53). https://doi.org/10.6028/NIST.SP.800-53r4
* Referenced for best practices related to **network monitoring** and the implementation of an **Intrusion Detection System (IDS)**.

 **A Guide to Digital Forensics and Cybersecurity Tools**

* Citation: Forensics Colleges. (2022, May 19). A guide to digital forensics and cybersecurity tools. <https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>
* Cited for **endpoint detection and response (EDR)** solutions.

 **NIST NVD: National Vulnerability Database**

* Citation: National Institute of Standards and Technology (NIST). (n.d.). National Vulnerability Database (NVD). <https://nvd.nist.gov/>
* Used to reference **specific vulnerabilities** found in outdated software and hardware configurations.

 **ISO/IEC 27002:2013 - Information technology - Security techniques**

* Citation: International Organization for Standardization. (2013). ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls. https://www.iso.org/standard/54533.html
* Cited in the discussion of **access control policies** and overall **information security management** practices.

 **Incident Response Planning and Execution Guide**

* Citation: SANS Institute. (2023). Incident response planning and execution guide. https://www.sans.org/incident-response-guide/
* Used to support recommendations on developing an **Incident Response Plan (IRP)**.

 **Security Information and Event Management (SIEM) Best Practices**

* Citation: Threatpost. (2023, March 15). Security Information and Event Management: Best practices for deploying a SIEM solution. https://threatpost.com/siem-best-practices/178162/
* Referenced for **SIEM** system implementation and integration within the organization’s monitoring strategy.

 **Endpoint Protection: A Comprehensive Guide**

* Citation: Cybersecurity Insiders. (2022). Endpoint protection: A comprehensive guide. https://www.cybersecurity-insiders.com/endpoint-protection-guide/
* Cited for information on **endpoint security improvements** and **patch management solutions**.

 **The Importance of Database Encryption in E-Commerce**

* Citation: Data Security Magazine. (2023). The importance of database encryption in e-commerce. https://www.datasecuritymagazine.com/database-encryption-importance
* Used to support the recommendation for **database encryption** and securing customer information.