Conducting a Risk Assessment Using NIST SP 800-30

Scenario:

I am tasked with conducting a risk assessment for an e-commerce business at the Tier 3 level (information system level). This risk assessment evaluates the potential risks to the e-commerce business's IT infrastructure, focusing on a server with a powerful CPU, 128GB of memory, using the latest Linux operating system, and a MySQL database. The infrastructure uses IPv4 networking and SSL/TLS encryption for secure communication. Recommendations for mitigating identified risks are also provided.

The Risk Assessment Process:

There are four main stages of the risk assessment:

1. Prepare for the Assessment
2. Conduct the Assessment
3. Communicate Assessment Results
4. Maintain the Assessment

Prepare for the Assessment

Scope & Purpose:

The scope of this vulnerability assessment relates to the current security controls of the e-commerce business's server. The assessment will cover a period of three months, from September 2024 to November 2024. NIST SP 800-30 is used to guide the risk analysis of the information system. The database server is a centralized computer system that stores and manages large amounts of data. The server is used to store customer, campaign, and analytic data. It is critical to secure the system because of its regular use for business operations.

Assumptions:

1. **System Description and Context**:
    - The business relies on a Linux operating system with MySQL as the database management system.
    - The hardware configuration (CPU and 128GB of memory) is sufficient to handle current and anticipated workloads.
2. **Security Measures**:
    - SSL/TLS encrypted connections are properly implemented and provide adequate protection against data interception and tampering.
    - The network infrastructure is stable and uses IPv4 addressing.
3. **Interconnected Systems**:

    - All servers interacting with the system are trustworthy and follow best security practices.
4. **Software Updates**
5. **Business Operations**
6. **Risk Assessment Framework**

Constraints:

1. **Scope of Assessment**:
    - Limited to the described configuration (Linux OS, MySQL, IPv4 network).
    - Excludes considerations for IPv6 implementation, cloud infrastructure, or additional software/hardware not mentioned.
2. **Data Availability**:
    - Comprehensive logs, access controls, and configurations must be accessible to perform an accurate assessment.
    - The business must provide information about current operational policies and compliance requirements.
3. **Network Limitations**:
    - Assessment assumes the network operates on IPv4 and does not include the implications of transitioning to IPv6.
4. **Security Dependency**
5. **Evolving Threat Landscape**
6. **Time and Resource Availability**
7. **Third-Party Dependencies**:
    - Security of third-party servers interacting with the system is assumed but not guaranteed.

Sources of Information:

To create a risk assessment report for the e-commerce business using NIST SP 800-30, the following sources of information are needed as inputs:

1. System Description and Configuration
2. Organizational Context
3. Data Flow and Interactions
4. Threat Sources
5. Existing Security Controls
6. Regulatory and Compliance Requirements
7. Historical Data
8. Risk Assessment Framework
9. Stakeholder Input
10. External Information Sources

Identify Risk Model and Analytic Approach:

This assessment uses a qualitative risk model with three potential values (low, medium, or high) to assess likelihood and impact.

Conduct The Risk Assessment

System Description:

The assessed system is an e-commerce server with the following characteristics:

- **Hardware:** Powerful CPU processor, 128GB RAM
- **Operating System:** Latest version of Linux
- **Database:** MySQL Database Management System
- **Network:** Stable network connection using IPv4 addresses, interacts with other servers
- **Security Measures:** SSL/TLS encrypted connections

Risk Assessment Methodology:

This assessment follows the NIST SP 800-30 risk assessment process, which includes the following steps:

1. **Asset Identification:** Identifying valuable assets.
2. **Threat Identification:** Identifying potential threats to those assets.
3. **Vulnerability Identification:** Identifying weaknesses that could be exploited by threats.
4. **Risk Determination:** Assessing the likelihood and impact of potential risks.
5. **Risk Response:** Determining appropriate responses to identified risks.

1. Asset Identification

The key assets for this system include:

- **Customer Data:** Personally Identifiable Information (PII), payment information, order history.
- **E-commerce Application:** The software that drives the online store.
- **Database:** The repository for all business data.
- **Server Hardware:** The physical server hosting the system.
- **Network Infrastructure:** Network connections and related equipment.

2. Threat Identification

Potential threats to the system include:

- **Malware:** Viruses, ransomware, spyware.
- **Hacking:** Unauthorized access to the server or database.

- **Denial-of-Service (DoS) Attacks:** Overwhelming the server with traffic, making it unavailable.
- **Data Breaches:** Theft of sensitive customer data.
- **Insider Threats:** Malicious or unintentional actions by employees.
- **Software Vulnerabilities:** Exploits targeting weaknesses in the operating system, database, or e-commerce application.

3. Vulnerabilities

- Unpatched Linux OS or MySQL database software.
- Misconfigured SSL/TLS settings.
- Network exposure due to lack of advanced firewall configurations.
- Insufficient monitoring of server interactions.

Risk Matrix:

Threat	Vulnerability	Likelihood	Impact	Risk Score
Malware	No antivirus	Medium	High	High
Hacking	Weak passwords, lack of access controls	Medium	High	High
DDoS Attacks	Lack of intrusion detection/prevention systems	Medium	Medium	Medium
Data Breaches	SQL injection, weak encryption	Medium	High	High
Insider Threats	Lack of monitoring, and background checks	Low	High	Medium
Software Vulnerabilities	Outdated software	Medium	High	High

Risk Mitigation Recommendations:

1. **Patch Management:**
    - Regularly update the Linux OS and MySQL software.
    - Apply security patches promptly.

2. **Enhanced Access Controls:**
    - Implement role-based access controls (RBAC).
    - Limit user access to sensitive data based on the principle of least privilege.
    - Use multi-factor authentication (MFA) for privileged users.

3. **Network Security:**
    - Configure advanced firewalls and intrusion detection systems (IDS).
    - Regularly review and update network configurations.

4. **Data Security:**
    - Verify SSL/TLS configurations and renew certificates before expiration.
    - Encrypt sensitive data stored in the MySQL database.

5. **Backup and Recovery:**
    - Establish automated daily backups of database and application data.
    - Develop a disaster recovery plan and conduct periodic drills.

6. **Monitoring and Auditing:**
    - Deploy security information and event management (SIEM) tools.
    - Conduct regular security audits and penetration testing.

Communicate And Share Risk Assessment Results

This report will be shared with organizational decision-makers to support responses to the risks identified.

Maintain the Assessment

The organization should conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets. Recommended activities are listed below:

Maintenance Requirements:

Regular Activities
- Weekly security patches
- Monthly vulnerability assessments
- Quarterly penetration testing
- Bi-annual control reviews
- Annual risk assessment updates

Documentation
- Maintain incident logs

- Update security procedures
- Track control effectiveness
- Document system changes