Edward Gulmayo ITE 370

3IT-SYSDEV

I. POTENTIAL THREATS AND VULNERABILITIES

Potential Threats:

- Phishing and Social Engineering Attacks
- Distributed Denial-of-Service (DDoS) Attacks
- Credential Stuffing Attacks
- Malware (Trojan, Ransomware)
- Insider Threats
- Man-in-the-Middle (MITM) Attacks
- Supply Chain Attacks
- Data Breaches and Unauthorized Data Access
- API Security Weaknesses

Potential Vulnerabilities:

- Outdated Software and Systems
- Weak Authentication Mechanisms
- Unencrypted Communication
- Improper Session Management
- Lack of Regular Penetration Testing
- Poorly Secured APIs
- Risks from Third-Party Integrations

II. RISK MANAGEMENT

1. IDENTIFICATION

- Identified Assets: customer data, transaction data, authentication systems, online banking apps, internal systems, and third-party APIs.

- Identified Vulnerabilities: outdated systems, poor authentication, unsecured APIs, weak employee awareness, and unencrypted data.
- Identified Threats: data breaches, MITM attacks, SQL injection, insider threats, phishing, and API vulnerabilities.
- Identified Controls: multi-factor authentication, regular patch updates, API security, data encryption, staff training, firewalls, and incident response plan.

2. ASSESSMENT

Risk Scoring System:
- Likelihood: Probability of occurrence (1 = low, 5 = high)
- Impact: Severity of consequences (1 = low, 5 = high)
- Exposure: Potential damage to reputation, compliance, and customer trust (1 = low, 5 = high)

Risk	Likelihood	Impact	Exposure	Total Risk Score
Phishing	5	4	5	20
SQL Injection	4	5	5	20
Insider Threats	3	5	5	15
DDoS Attacks	3	4	4	12
MITM Attacks	3	5	4	12
Data Encryption Gaps	4	5	4	16

Insights from Assessment:
- Highest Risks: Phishing (20), SQL Injection (20)
- Moderate Risks: DDoS Attacks (12), MITM Attacks (12)
- Lower Risks: Insider Threats (8), Third-party Vendor Risks (9)

3. TREATMENT

- Phishing & Credential Stuffing:
  - Use multi-factor authentication (MFA) for all users.
  - Use AI-based phishing detection for emails.
  - Encourage customers to use strong passwords and password managers.
- SQL Injection & Web App Security:
  - Conduct regular vulnerability assessments and penetration testing.
  - Use web application firewalls (WAF) and secure coding practices.
- Data Encryption Gaps:
  - Ensure encryption of data at rest and in transit (AES-256).
  - Use SSL/TLS for secure communication.
- DDoS Attacks:
  - Set up DDoS protection services (e.g., Cloudflare).
  - Implement rate-limiting on critical pages.
- Insider Threats:
  - Use User Behavior Analytics (UBA) to monitor for suspicious activity.
  - Regularly review employee access to sensitive data.
- API Vulnerabilities:
  - Use API security best practices: authentication, rate-limiting, and regular testing.
  - Apply API gateways to monitor and enforce security policies.

4. COMMUNICATION

- Internal Communication: Keep employees informed of security policies and incident response plans through internal channels.
- External Communication: Notify customers of security measures and any incidents that affect them.

5. REIDENTIFICATION

- Collect intelligence on new threats and vulnerabilities.

- Update the risk register regularly and adjust controls accordingly.
- Communicate any updates to stakeholders and employees