Mark Ngugi

I132/g/1614/21

COURSE CODE: ICB 1401

COURSE TITLE: IT SECURITY ARCHITECTURE AND DESIGN

Securing TechNova Inc.

1. Emerging Threats and Their Impact (15 Marks)

a) Identified Cybersecurity Threats:

1. **Ransomware Attack:** Encrypted internal databases and disrupted operations.
2. **Supply Chain Attack:** Compromised third-party vendor software introduced vulnerabilities.
3. **Insider Threat:** A disgruntled employee leaked sensitive customer data.
4. **Advanced Persistent Threats (APTs):** Attempted to gain long-term access to sensitive financial records.
5. **IoT Vulnerabilities:** Payment terminals were exposed to unauthorized access.

b) Potential Impacts on TechNova:

- **Operational Impact:** Service disruptions and delayed recovery from ransomware attacks impede business operations.
- **Reputational Damage:** Customer trust can erode due to data breaches and operational failures.
- **Compliance Risks:** Violations of data protection regulations (e.g., GDPR, PCI DSS) may result in fines.
- **Financial Losses:** Direct costs of incident response, potential legal liabilities, and lost business opportunities.

2. Mitigation Strategies (20 Marks)

a) Strategies to Mitigate Each Threat:

1. **Ransomware Attacks:**
   - Implement robust backup systems with regular testing.
   - Deploy endpoint detection and response (EDR) solutions.
   - Establish clear disaster recovery protocols.
2. **Supply Chain Attacks:**
   - Conduct thorough vetting and continuous monitoring of third-party vendors.
   - Employ software composition analysis (SCA) tools to detect vulnerabilities.
   - Use secure coding practices and ensure contractual obligations for vendor security.
3. **Insider Threats:**
   - Implement user behavior analytics (UBA) to detect abnormal activities.
   - Enforce least privilege access.
   - Conduct regular employee background checks and exit interviews.
4. **APTs:**
   - Use intrusion detection and prevention systems (IDPS).
   - Employ multi-factor authentication (MFA) for sensitive systems.
   - Conduct continuous network monitoring with threat intelligence integration.
5. **IoT Vulnerabilities:**
   - Secure IoT devices with firmware updates and patches.
   - Segregate IoT networks from critical systems.
   - Implement device authentication and encryption.

b) Tools, Frameworks, and Practices:

- **Backup Tools:** Veeam, Acronis.
- **EDR Solutions:** CrowdStrike, SentinelOne.
- **Threat Intelligence Platforms:** MISP, Recorded Future.
- **Vulnerability Scanners:** Nessus, Qualys.
- **Encryption Tools:** BitLocker, VeraCrypt.

3. Protecting Organizational Data (10 Marks)

a) Best Practices for Protecting Data:

1. **Data Encryption:**
   - Encrypt data at rest and in transit using AES-256.
   - Employ transport layer security (TLS) for communication.
2. **Access Control:**
   - Implement role-based access control (RBAC).
   - Enforce MFA for all user accounts.
   - Regularly audit access permissions.
3. **Employee Training:**
   - Conduct regular cybersecurity awareness programs.
   - Simulate phishing attacks to educate employees.
   - Provide training on secure handling of sensitive data.

b) Specific Strategies for Data Encryption, Access Control, and Employee Training:

1. **Data Encryption:**
   - Use full-disk encryption for all storage devices.
   - Implement secure key management practices to ensure encryption keys are protected.
2. **Access Control:**
   - Utilize zero trust architecture to verify every access request.
   - Regularly rotate passwords and enforce strong password policies.
3. **Employee Training:**
   - Integrate cybersecurity modules into onboarding processes.
   - Use gamified training programs to make learning engaging.
   - Schedule periodic refresher courses to keep employees updated on the latest threats and defenses.

4. Risk Management and Incident Response (15 Marks)

a) Risk Management Framework:

1. **Identify Risks:** Conduct regular threat assessments and penetration testing.
2. **Analyze Risks:** Use risk matrices to prioritize vulnerabilities.

3. **Mitigate Risks:** Deploy appropriate security controls and contingency measures.
4. **Monitor and Review:** Continuously evaluate the effectiveness of implemented measures.

b) Incident Response Plan:

1. **Preparation:**
   - Develop and maintain an incident response playbook.
   - Conduct regular incident response drills.
2. **Detection and Analysis:**
   - Use SIEM tools (e.g., Splunk, LogRhythm) to identify anomalies.
   - Establish a 24/7 monitoring team.
3. **Containment:**
   - Isolate affected systems immediately.
   - Block malicious IP addresses and deactivate compromised accounts.
4. **Eradication and Recovery:**
   - Remove malware and patch vulnerabilities.
   - Restore systems from verified backups.
5. **Post-Incident Review:**
   - Document lessons learned and improve security measures.
   - Share incident findings with relevant stakeholders.