جامعة الملك سعود
King Saud University
1957
كلية علوم الحاسب والمعلومات

CSC 429: Computer Security

Course Project: Comprehensive Analysis of a Major Cybersecurity Incident

Group Member:

Abdulrahman Alateeq [redacted]
Mohammed Aljalajil
Abdulrahman Almayman

Question 1

A. Risk Assessment Approaches

1. **Baseline Approach:**
   This method uses standard guidelines to identify risks. It assumes common threats and provides basic recommendations. It is simple but may miss organization-specific risks.

2. **Informal Approach:**
   Relies on the experience and intuition of individuals rather than structured methods. It is flexible and quick but lacks consistency and may overlook critical risks.

3. **Detailed Risk Analysis:**
   A thorough and structured method that identifies, analyzes, and evaluates risks in depth. It offers detailed insights but is resource-intensive.

4. **Combined Approach:**
   Merges elements of all methods. For example, it may use baseline controls for common risks, detailed analysis for critical risks, and informal methods for unique situations. It is versatile but requires careful coordination.

B. Recommendation

The **Baseline Approach** is recommended for a mid-sized organization with a limited budget. This is because it is cost-effective and ensures common and significant threats are addressed within the financial constraints. Although it may not capture every specific risk, it provides a practical starting point for risk management.

Question 2

A. Asset Identification

1. **Customer Databases:**
   Store sensitive client information such as contact details and purchase histories. Protecting them maintains customer trust and ensures compliance with data protection laws.

2. **Email Systems:**
   Essential for communication within and outside the organization. Breaches can lead to phishing or unauthorized access to confidential information.

3. **Proprietary Project Management Application:**
   Critical for project management and operational efficiency. A compromise could disrupt

project timelines.

4. **Development Servers:**
   Host the codebase and tools for software development. Their security ensures the integrity and availability of the software.

B. Threat and Vulnerability Identification

1. **Data Breach:** A potential threat to customer databases, often caused by weak encryption. Hackers could exploit this vulnerability to access sensitive information, representing a man-made threat.

2. **Phishing Attack:** Email systems are susceptible to phishing, particularly if employees fall for deceptive emails. This threat arises from human vulnerability and is categorized as man-made (social engineering).

3. **System Downtime:**Development servers face risks from power outages or natural disasters. A lack of redundancy in the system increases this vulnerability, making it a natural threat.

C. Risk Assessment Matrix

Threat	Likelihood	Consequence	Risk Level	Existing Controls	Recommended Controls
Data Breach	High	Critical	High	Firewalls, Basic Encryption	Advanced Encryption, Security Audits
Phishing Attack	Medium	High	High	Security Awareness Training	Phishing Simulations
System Downtime	Low	Significant	Medium	Backups, UPS for Power	Server Redundancy

D. Risk Treatment

1. **Data Breach:** To mitigate this threat, reducing the likelihood is essential. Implementing advanced encryption and conducting regular security audits will help prevent breaches.

2. **Phishing Attack:** Reducing the likelihood is the recommended treatment. This can be achieved by providing employees with advanced training and conducting regular phishing simulations to improve their awareness and preparedness.

3. **System Downtime:** Reducing the consequences is the best course of action. Adding server redundancy ensures that operations can continue smoothly even during outages, minimizing disruption.

Question 3

A. Limitations and Adaptability of Risk Assessment Approaches

1. **Baseline Approach:** The baseline approach is limited in dealing with unforeseen threats because it relies on predefined controls and common risks. It does not adapt well to unique or emerging risks, such as new types of cyberattacks or technologies.

2. **Informal Approach:** While flexible and fast, the informal approach depends heavily on the analyst's knowledge and intuition. It may fail to consider new or complex threats that require specialized expertise or a structured analysis.

3. **Detailed Risk Analysis:** Although comprehensive, this method is time-consuming and resource intensive. It might not be agile enough to respond to rapidly evolving threats like zero-day vulnerabilities.

4. **Combined Approach:** The combined approach balances flexibility and thoroughness but still requires significant planning and resource allocation. While adaptable, it might not address unforeseen threats quickly without updated inputs and assessments.

B. Comparison: Tech Solutions vs. Silver Star Mines

Aspect	Tech Solutions	Silver Star Mines
Assets	Customer databases, email systems, proprietary applications, development servers.	SCADA systems, financial systems, procurement systems.
Threat Levels	Higher risks from human-driven threats like phishing attacks.	Lower likelihood, high-impact threats like system modifications.
Focus Areas	Data security and employee awareness.	Operational continuity and system reliability.

Implication:
Tailored risk assessments ensure resources are allocated to address the most relevant threats. Tech Solutions should prioritize securing digital assets and training staff, while Silver Star Mines must focus on maintaining operational systems under strict regulations.