Assignment 1

1. **The slides explain the Zero Trust Security Model, which is crucial for modern cybersecurity defense.**
    a. **Describe how a company handling financial data can implement Zero Trust principles in its network infrastructure.**

Ans:

- **Identity Sensitive Data and Assets** : Classify the data, applications, assets and services to determine the most critical and sensitive components that require protection.
- **Secure Devices**: All devices connecting to the network should be checked for security (e.g., updated software, no malware).
- **Network Segmentation**: The network should be divided into smaller segments, isolating critical financial systems from less sensitive areas. This ensures that even if one part of the network is compromised, attackers can't move freely across the entire system.

    b. **Consider specific challenges like managing remote employees and integrating cloud services. Discuss how micro-segmentation and strict access control mechanisms could be applied.**

Ans:

Remote employees accessing sensitive data from various locations pose security risks. To address this, secure VPNs or zero-trust network access (ZTNA) can be used, ensuring workers are authenticated and verified before accessing internal resources. **Micro-segmentation** further ensures they only access the specific network parts required for their roles.Micro-segmentation in cloud environments isolates sensitive financial data, and strict access controls based on user roles require continuous authentication. Micro-segmentation also divides the network into smaller zones, reducing the attack surface by limiting lateral movement. Strict access controls, like role-based access control (RBAC), are implemented to ensure users only access the data and systems relevant to their job, reducing the risk of unauthorized access.

    c. **What role does continuous monitoring play in a Zero Trust environment, and how can it mitigate potential insider threats?**

Ans:

- **Detecting Insider Threats**: Continuous monitoring tracks user actions in real-time. If an employee suddenly starts accessing large amounts of sensitive financial data or systems they don’t normally use, these unusual behaviors will trigger alerts. For example, an accountant trying to access engineering systems would be flagged for investigation.
- **Behavioral Analytics**: Machine learning models can analyze user behavior to detect patterns that suggest insider threats, such as accessing systems outside of work hours or downloading unusually large volumes of data.
- **Continuous Auditing**: Monitoring tools provide audit logs that can be used to trace the source of data breaches and anomalies. This is crucial for quickly responding to and containing security incidents.

2. **Based on the ransomware attack scenario discussed in the lecture, create a detailed Incident Response Plan (IRP) for a healthcare organization storing sensitive patient Records.**
    a. **Outline the steps that the organization should follow in response to a ransomware attack, from preparation to lessons learned.**

Incident Response Plan - A documented, structured approach for handling security breaches, cyber threats, and incidents to minimize their impact and recover from them as quickly as possible.

The Essential steps to prevent the ransomware attack can be:

- Regular Backup
- Security software and Anti-virus
- Network Segmentation
- Patch Management

Methods that a company should follow in response to a ransomware attack:

- **Preparation** - A Company has a IRP that includes-
    - Employee Training
    - Phising emails
    - Regular Data backup
    - Upto date Anti-virus software
- **Identification** - If an employee notices any kind of breaches or any important files or information is being affected as the attacker uses many ways like demanding the ransom. The employee should immediatly inform the Higher authorities.
- **Containment** - This is the method of disconnecting the network as they are not spreading across the network. These includes disconnecting the VPNs, isolating the internal network, preventing the remote employees to connect into the compromised network, safegaurding their network.
- **Eradication** - this is the time where the employees try to terminate the connection and try to resolve the problem. These include antivirus tools to remove the ransomware from the infected machines and check the system have any vulnerabilities that were exploited by the attackers.
- **Recovery** - This includes the recovery that will delete the affected files and retrieve the files from the backup. But we should ensure that the retrieved files have not been affected or it doesnot contain the virus. We should ensure the backup and recovery , enhance the email security, conduct regular training and awareness programs for the employees.
- **Lessons Learned** - Company should ensure and remedial action for how the attack happend, how they overcome the situation and also be prepared for the future. Company should have to make sure that they have regular meetups and so on
- **Reporting** - This is the important part of the scenario, which includes the proper and valid documentation of the incident happened and how they overcome that situation, how the breached extended, this report is used for validation for the future reference.

b. **What are the legal implications of failing to properly contain and report such incidents under regulations like HIPAA?**

Failing to report such incident under the regulations like HIPPA includes -

- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care been taken to abide by HIPAA Rules,Minimum fine of $100 per violation up to $50,000
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules),Minimum fine of $1,000 per violation up to $50,000
- **Tier 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation, Minimum fine of $10,000 per violation up to $50,000.
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days,Minimum fine of $50,000 per violation.

3. The lecture highlights the importance of security audits to ensure compliance with GDPR and other regulations.

a. **Using the example of a financial services firm, describe how a security audit should be conducted, including the key areas that must be assessed (e.g., patch management, access control, and encryption).**

Steps for the security audit includes -

- Preparation
- Assesment
- Review of their products
- Compliance check
- Report and Recommendations
- Follow - up

Security Audit - A Brief Summary

➔ **Preparation -**

- ◆ The auditors review the current security policies of the company, procedures and the compliance requirements with the industry standards like Payement card industry data security standards (PCI DSS).

➔ **Compliance Check -**

- ◆ The auditors check the companies practices aligned with the relevant legal and regulatory requirements, focusing on the data protection, privacy and financial regulations.

➔ **Report and Recommendations -**

- A report is being submitted regarding the company's current cybersecurity frameworks. This report includes specific recommendations for addressing the identified vulnerabilities such as enhancing encryption methods, updating the incident response stratergies.

➔ **Follow_up -**

- A company develops an action plan based on the audit's findings and works on implementing the recommendations.
- A follow up review is scheduled to access the effectiveness of implemented changes.

Patch Management - A Brief Summary

Steps in Patch Management:

1. Vulnerability Identification
2. Patch Availability
3. Risk Assessment
4. Patch Testing
5. Patch Development
6. Verification and Monitoring
7. Documentation and Reporting

Patch Management:

➢ **Vulnerability Identification -**

- The company's security team is alerted or informed to the vulnerability through a security bulletin or vulnerability database

➢ **Patch Availability -**

- The software developers who developed the web server application release a patch to address the vulnerabilities.
- This patch is announced on their official website, email alerts and by other means to the user.

➢ **Risk Assessment -**

- The company's security team assess the severity of the vulnerability, which will consider the fact such as the potential for data loss and unauthorized access.

➢ **Patch Testing -**

- The patch is tested on a safe environment before spreading wide as it does not interfere with the operation of web server application and the other interconnected devices. These can be done in an isolated environment.

➢ **Patch Deployment -**

- Once the testing is done, then it is deployed on the company network to all instance of the vulnerable web server applications. This is done manually using the patch management software.

b. Propose remediation steps for any discovered vulnerabilities while ensuring compliance with GDPR and similar regulations.

After a vulnerability is reported during the security review, it is necessary to coordinate and implement the remedy with precision in the security of the firm as well as with the requirements like the GDPR.

Patch and Update Management:

- **Vulnerability**: Old software or systems with pending patches or basic known flaws.

Remediation Steps:

- Patching Routine: Make it a routine to install security patches on various systems.
- Patching Tools: Tools that automate the patching process and all critical patches are met promptly.
- Routine Testing: It is important to test the appropriate patches so as to avoid disrupting the main service due to problematic patches.

GDPR Considerations: As directed by the CNI, patches will always be applied to the systems that handle personal data so that these systems are not accessed without authorization. It is also true that these patches support the terrors of the GDPR.

Enhancing Access Control-

- Vulnerability: Weak identity and strong control over management or too much access.

Remediation Steps:

- Access Control — Least Privilege: Employees are not professionals without needing them enabling access. Access Control Ace: Sensitive data is better managed by only allowing those with job critical roles to access it using Role-based access control mechanism.
- Multi-Layered Mechanism: Increased number of accesses, particularly for sensitive data, use Multi layer mechanisms.
- Access Control Review: Periodic access reviews may be useful in expanding access limits for end users where unnecessary rights have been removed.

4. In the lecture, both DAC and RBAC were discussed.

a. Compare and contrast the two mechanisms in the context of securing an online banking system.

Discretionary Access Control (DAC) -

- DAC is based on the idea in which the access right, privileges and the mechanisms for giving user such privileges.
- These privilege includes users to access some data such as to read ,or to write.
- A user who creates data object such as a table or a view automatically gets the privilege on that object
- These can be implemented using Sturctured Query Language (SQL) through the use of GRANT and REVOKE.
- DAC is often simpler, and generally more granular. Also, in the DAC model the data owner can decide who has access (if he has that permission on the data) and add or remove people from the list.

Role Based Access Control (RBAC)

- Apart from the DAC, RBAC is slight different as they give each user some specific privilege with roles.User are assigned to appropriate roles.
- Roles can then be granted to user and other roles.
- The main benefit of RBAC over DAC, is ease of management - in principle you have a very few roles, centrally administered, no matter how many users, and its just a question of granting each user the correct role; as opposed to DAC, where for each new user (or change in user, or deletion, etc), you have to go around to all the resources she needs access to and add them to the list.

b. Provide a real-world example where RBAC would enhance security and compliance. Consider the hierarchical nature of user roles.

Scenario: Online Banking System

In an online banking system, various users (e.g., customers, bank tellers, managers, administrators) need access to different parts of the system, but only to the extent necessary for their roles. Here's how RBAC enhances security and compliance by organizing these users into roles:

1. **Customer Role**:
    - **Permissions**: Can only view their own account balance, transaction history, and perform actions like transferring funds or paying bills.
    - **Security Enhancement**: Limits customers to accessing only their personal data, reducing the risk of accidental or malicious access to other customers' sensitive information.
    - **Compliance**: Ensures data privacy, aligning with GDPR and banking regulations that protect customer information.

2. Bank Teller Role:

- **Permissions**: Can access customer account information to assist with transactions but cannot modify or delete account records.

- **Security Enhancement:** Prevents tellers from accessing or changing sensitive administrative settings or customer data beyond their job scope, reducing the risk of internal fraud.
- **Compliance**: Ensures compliance with financial regulations (e.g., PCI DSS) by enforcing separation of duties and limiting access to financial data.

3. Manager Role:

- **Permissions**: Can approve transactions over a certain threshold, view reports, and manage teller operations but cannot access system configurations.
- **Security Enhancement:** Managers can oversee operations but are restricted from technical system functions, reducing the risk of misuse or errors in system configuration.
- **Compliance**: Ensures proper oversight and audit trails for high-value transactions, meeting regulatory requirements for transaction monitoring and internal controls.

4. System Administrator Role:

- **Permissions**: Full access to system settings, configurations, and user management but no access to customer financial data.
- **Security Enhancement:** System administrators can maintain and secure the infrastructure but cannot tamper with financial data, which minimizes the risk of data breaches.
- **Compliance**: Segregates administrative functions from business functions, ensuring compliance with financial and data protection regulations like GDPR and SOX (Sarbanes-Oxley Act).

How RBAC Increase Security and Compliance:

- **Hierarchy**: By assigning permissions based on roles, RBAC ensures that only users with the appropriate level of authority can access sensitive functions, reducing the risk of unauthorized access.
- **Auditability**: RBAC ensures clear audit trails, showing who accessed or modified specific systems or data, which is crucial for meeting regulatory compliance.
- **Separation of Duties:** Enforces the principle of least privilege, ensuring that users only have access to the data and functions necessary for their role, which enhances both security and regulatory compliance. In this real-world scenario, RBAC provides structured, secure access control that Increase both security and compliance, crucial for an industry as regulated an

5. Database security is critical for maintaining data confidentiality and integrity, especially in systems that handle sensitive information like hospital patient records.

a. **Compare and contrast cell-level encryption and column-level encryption for securing sensitive data in a hospital's patient record system. Discuss how each method functions, their strengths, and weaknesses in terms of performance, security, and control over data access.**

Column - Level Encryption -

- The entire column is encrypted.
- The Social Security Number (SSN) column is completely encrypted.

Employee Table

employee_id	employee_name	salary	ssn
1	John Doe	50000	123-45-6789
2	Jane Smith	60000	987-65-4321
3	Bob Johnson	75000	456-78-9012

Column level encryption -

employee_id	employee_name	salary	SSN
1	John Doe	50000	ENCRYPTED_CONTENT
2	Jane Smith	60000	ENCRYPTED_CONTENT
3	Bob Johnson	75000	ENCRYPTED_CONTENT

Cell - Level Encryption -

- In cell level encryption only the specific cells or the data elements are encrypted.
- In the following example the salary for employee_id = 1 is encrypted.

employee_id	employee_name	salary	ssn
1	John Doe	ENCRYPTED_CONTENT	123-45-6789
2	Jane Smith	60000	987-65-4321
3	Bob Johnson	75000	456-78-9012

b. **Identify the practical challenges of implementing these encryption methods in a hospital's electronic health record (EHR) system or other healthcare data systems. Consider issues like performance degradation, key management, system complexity, and compliance with healthcare regulations such as HIPAA. Propose strategies to mitigate these challenges while ensuring both security and the system's operational efficiency.**

There are a number of practical considerations involved in the employment of encryption techniques in a hospital electronic health record (EHR) system which include

- performance concerns
- key management issues

- system complexity
- auditing or assessments in regard to the healthcare related laws such as HIPAA.

1. **Performance Degradation-**
    a. Lasting significant improvements comes at the cost of processing capabilities; encryption lacks operational efficiency within EHR systems, especially during data entry and retrieval that requires somewhat rapid functionality for efficient delivery of patient care.
    b. Employ fast but secure encryption algorithms (eg. AES-256) while encrypting only small data fields and items considered sensitive (e.g patient's full name) rather than the whole database. Use hardware-assisted encryption which saves on processing power by performing the encryption work already in certain hardware only.
2. **Key Management-**
    a. The security of the encryption keys is important since key loss or mishandling may lead to information loss or breach in security. In addition to this, key management and distribution in large healthcare institutions can be quite challenging.
    b. Establish a key rotation scheme where all keys are served from a central location by a key management server (KMS), thus serving to store, revoke and rotate keys. Provide secure storage for keys and their use through the use of hardware security modules. Implement Multi-factor Authentication and strict safeguards on Key Management Server (KMS) use.
3. **System Complexity-**
    a. Encrypting a component of an EHR system often brings about complications, more so in trying to connect with other industry components such as lab systems and external services.
    b. Implement the use of pre-defined encryption stack (for instance using TLS for moving data in transit) as well as communicating through standardized and securing enviros integration. Implement encryption abyads as a service model.

6. The lecture covered threat, vulnerability, and risk in cybersecurity.

a. Design a risk assessment framework for a cloud-based e-commerce platform that relies on user trust for processing payments and storing personal data.

Key Steps in Risk Assessment -

- **Identify Risks :** Recoganize the possible threats that include natural disastersm cyber attacks, system failures and so on.
- **Analyze Risks :** Determine the likelihood of each risk and the impact of that in our system.
- **Evaluvate Risks :** Prioritize risked based on the impact and combine them according to that.
- **Mitigate Risks :** Once we found if any risk can be happen, we must then develop strategies to reduce the risk or eliminate the high priority risks, these include implementing the security control, creating master plans etc.

- **Monitor and Review :** We must continuously track the progress and update the assessment as new threat emerge.

Risk Assesment Framework -

In order to build a risk assesment framework, we first develop a structured way to implement the key step of the risk Assessment. The include:

★ **Define the scope:**
  - We must have a idea about the users in a cloud based e-commerce platform
  - Ensure the confidentiality, integrity and availability of their personal information while maintaining the compliance regulations include GDPR,PCI DSS and so on.

★ **Risk Identification:**
  - Categorize the risk based on the criticality and sensitivity. Critical includes the payment gateway, personal data storage, authentication systems
  - Identifiy the potential source of threat , for eg if there is an unaythorized malicious software installed or nor and so on.
  - **Key Threat scenarios:**
    - **Data Breach**: Unauthorized access to personal and payment data.
    - **DDoS Attacks**: Disruption of service, affecting availability.
    - **Account Takeover**: Credential stuffing or brute-force attacks.
    - **Payment Fraud**: Exploitation of payment processing systems.
    - **Cloud Misconfigurations**: Insecure settings leading to data leaks or unauthorized access.

★ **Risk Assessment Criteria:**
  - **Likelihood**: Probability of the risk occurring.
    - **High**: Common occurrence (e.g., phishing).
    - **Medium**: Occasional (e.g., malware).
    - **Low**: Rare but possible (e.g., zero-day vulnerabilities).
  - **Impact**: Consequence of the risk if it occurs.
    - **High**: Major financial loss, severe data breach, reputational damage.
    - **Medium**: Moderate impact on service availability and customer experience.
    - **Low**: Minimal impact, isolated incidents.

  - **Risk Calculation Formula**:
    - Risk Score = Likelihood × Impact (Scale: 1-5, with 5 being highest).

★ **Risk Mitigation Statergies:**
  - If the score is between 12 and 25, then it is a High risk.
    - **Implement strong encryption** for both data in transit and at rest (e.g., TLS, AES-256).
    - **Enable multi-factor authentication (MFA)** for user accounts and administrators.
    - **Regular vulnerability assessments** and **penetration testing**.

        - **Use PCI-DSS compliant payment gateways** and adhere to regulatory requirements.
        - **Cloud Configuration Audits**: Regular checks for security misconfigurations (e.g., least privilege access).
    - If the score is between 6 and 11, then it is a Medium risk.
        - **DDoS Protection Services**: Use cloud-based mitigation tools to handle large-scale attacks.
        - **Automated Patch Management**: Ensure all systems and software are updated regularly.
        - **Access Controls and Logging**: Restrict user and administrator access to sensitive data, with logging enabled for audit trails.
    - If the score is between 1 and 5, then it is a Low risk.
        - **Awareness Training**: Educate staff on phishing and social engineering.
        - **Routine Backups**: Secure and periodic backups to ensure data availability.
        - **Incident Response Planning**: Create and update incident response and recovery plans regularly.
- ★ **Compilance and Regulatory controls:**
    - **GDPR**: Ensure data processing and storage meet GDPR requirements, including data subject rights, lawful processing, and data minimization.
    - **PCI-DSS**: For payment handling, adhere to PCI-DSS standards for encryption, logging, and system monitoring.
- ★ **Risk Acceptance and Transfer:**
    - **Risk Acceptance**: Some low-impact risks may be accepted if they pose little threat to business operations.
    - **Risk Transfer**: Use cyber insurance to cover high-impact risks like data breaches or payment fraud.
- ★ **Documentation and Reporting:**
    - **Maintain a Risk Register**: Track all identified risks, mitigation steps, and monitoring activities.
    - **Report to Stakeholders**: Provide regular risk assessment reports to key stakeholders, including technical teams, management, and legal advisors.
    - **Incident Reporting Procedures**: Define clear steps for reporting security incidents both internally and to regulatory bodies.

b. Discuss how the framework can be used to identify potential vulnerabilities and propose suitable mitigation strategies, including multi-factor authentication and intrusion detection systems.

- **Spotting Possible Weak Points**

A risk assessment framework helps to spot these weak points that might affect a cloud-based e-commerce platform:

- **Poor User Login Security**
    - Weak Spot*: Bad guys could break into accounts if the password rules are too lax or if there's no two-step login process.
    - Result: Someone who shouldn't could get in and steal data or commit fraud.

- **Break-ins or Sneaky Access**
    - Weak Spot: Hackers might use tricks like SQL injection or set up cloud tools to sneak into private customer info.
    - Result: This could make customers lose faith, cost money, and lead to fines.

- **Payment System Crashes**
    - Weak Spot: If you use one way to take payments, you're in trouble if it stops working.
    - Result: You could lose money and make customers unhappy.

- **Phishing Attack**
    - Vulnerability: Scammers might trick customers or workers into revealing their login details or money info through fake emails or websites.
    - Impact: This can lead to crooks making bogus purchases or taking control of accounts.

7. Penetration testing was described as a proactive cybersecurity measure in the lecture.

a. Outline a penetration testing plan for a government agency's critical infrastructure, covering phases like reconnaissance, scanning, and post-exploitation.

➔ **Planning and Preparation:**
- ◆ We must define the scope and targets as well as the objectives, understand the systems you will test which includes networks, databases, servers.

➔ **Reconnaissance**
- ◆ These includes the data or information gathering about the targeted system, these are collected without interacting directly with the target, they do this with publicly available data

➔ **Scanning:**
- ◆ Then we have to identify the opened ports and find the vulnerabilities, then have to perform the network scanning to find the opened ports and running services, we can use the **NMAP** tool for doing these.

➔ **Exploitation:**
- ◆ If we find any vulnerabilities, we must exploit the vulnerabilities to gain access. After identifying the weakness, we try to exploit them, we use the tool names Metasploit fo this, we will maily focus on getting the privilege for accessing the sensitive data

➔ **Post Exploitation:**
- ◆ After getting the access, we must the system and the data that can be manipulated, understanding the potential damage which include data theft, privilege escalation and

so on. We must have a clear knowledge of what we are doing as we have to make proper documentation.

➔ **Report and documentation:**

◆ We have to document all the vulnerabilities discovered and exploited, recommend patches and configuration to fix the issues

b. Consider the ethical and legal boundaries of penetration testing and how these factors should be managed during the engagement.

- **Legal Considerations:**
  - **Permission and Authorization**: Ensure the penetration testing team has explicit legal approval from the relevant government agency to conduct the test. Unauthorized testing is illegal and may result in prosecution for hacking.
  - **Compliance**: Adhere to applicable legal frameworks, such as GDPR or HIPAA, if the test involves handling sensitive personal data.
- **Ethical Boundaries:**
  - **Minimizing Harm**: Perform tests in a controlled manner to prevent any real damage to the system. Avoid actions that may disrupt services or compromise sensitive information.
  - **Data Protection**: Ensure that no sensitive information is exposed or misused during the test. Securely handle and dispose of all collected data unless it is required post-testing.
- **Transparency:**
  - **Reporting**: Be clear about the methods used and the vulnerabilities identified. Provide the agency with a detailed explanation of how risks were discovered and exploited.
  - **Recommendations**: Offer practical solutions to address the issues found without causing alarm or confusion.

Submitted By
Nanda Krishnan V
Msc Computer Science with Cybersecurity.