ISM6124.300S2 ADVANCED SYSTEMS ANALYSIS AND DESIGN

TRR: Test Readiness Review

TOPIC - System Analysis and Design for Data Security

Team Fantastic Four

Nikhil Reddy Kotwal

Simran Agichani

Yeshwanth Kumar Lekkala

Neha Sapare

**1.0 Software Test Plan**

* 1. **Facility Testing**

Facility testing for security breaches and data loss involves assessing the security measures in place to protect physical assets and data within a facility. This type of testing is important to ensure that an organization is adequately protecting its assets and data, and to identify potential vulnerabilities and weaknesses in the security infrastructure. Some examples could be:

1. To test the network and infrastructure security measures in place, such as firewalls, intrusion detection and prevention systems, and VPNs. This will help to identify any weaknesses or vulnerabilities in the network and infrastructure security that could be exploited by attackers.
2. To test the data loss prevention measures in place, such as encryption, data backups, and data access controls. This will help to identify any weaknesses or vulnerabilities in the data loss prevention infrastructure that could lead to data loss or theft.
   1. **Personnel Testing**

In case of a security breach, a team of cybersecurity professionals will typically be responsible for conducting the security breach testing. The specific members of this team may vary depending on the organization, but some common roles may include:

1. Incident Response Team: This team is responsible for responding to security incidents, including investigating, and containing the breach.
2. Security Engineers: These professionals are responsible for designing and implementing security measures to prevent future breaches and may be involved in the testing and evaluation of security measures during and after a breach.
3. Forensic Analysts: These professionals are responsible for analyzing digital evidence related to the breach, such as logs, network traffic, and system images.
   1. **Method Testing**
4. Information security analysts are responsible for analyzing and identifying potential security risks and vulnerabilities within the organization's systems.
5. Network and system administrators are responsible for configuring, maintaining, and monitoring the organization's systems and networks to ensure that they are secure and functioning properly.
6. Data loss prevention specialists are responsible for implementing and testing data loss prevention measures, such as data backups, encryption, and access controls.
   1. **Equipment Testing:**

Equipment testing in the context of security breaches and data loss involves testing the hardware and software systems that are used to protect an organization's data and assets.

1. Firewall testing: This involves testing the organization's firewall systems to ensure that they are configured properly and are blocking unauthorized traffic.
2. Intrusion detection system testing: This involves testing the organization's intrusion detection systems to ensure that they are properly configured and are detecting and alerting on potential security threats.
3. Antivirus and anti-malware testing: This involve testing the organization's antivirus and anti-malware software to ensure that it is up-to-date and is detecting and removing known threats.
4. Backup and recovery testing: This involves testing the organization's backup and recovery systems to ensure that they are functioning properly, and that data can be restored in the event of a data loss or security breach.
5. Network segmentation testing: This involves testing the organization's network segmentation systems to ensure that they are properly configured and are isolating sensitive systems and data from the rest of the network.
6. Encryption testing: This involves testing the organization's encryption systems to ensure that they are properly configured, and that sensitive data is encrypted both in transit and at rest.
   1. **Environment Testing:**

The environment should be representative of the production environment in which the systems and data normally operate. This allows the testing team to replicate the conditions of the security breach and data loss in a controlled environment and to evaluate the effectiveness of the organization's security measures.

For example, if a data breach involved a web application, the testing environment might include a replica of the web application, a replica of the database containing the sensitive data, and the network infrastructure used to support the web application. The testing team would then attempt to identify the cause of the breach and assess the effectiveness of the organization's security controls in detecting and preventing the breach.

Similarly, if a security breach involved a server or other network infrastructure, the testing environment might include a replica of the affected systems, as well as any associated networking equipment and security controls. The testing team would then attempt to identify any vulnerabilities or weaknesses in the systems and network infrastructure that could have been exploited by the attacker.

**1.6 Location Testing**

The location used to test security breaches and data loss depends on the specific systems and data affected by the breach, as well as the resources available to the testing team. In some cases, testing may be conducted on-premises, in a controlled environment that replicates the conditions of the breach. In other cases, testing may be conducted remotely, using cloud-based resources or other off-site infrastructure.

1. On-premises testing may be necessary in cases where the systems and data affected by the breach cannot be easily replicated in a cloud environment.
2. Cloud-based testing may be more convenient and cost-effective in some cases, especially if the affected systems and data can be easily replicated in a cloud environment.

|  |  |
| --- | --- |
| **Name** | **High-level Testing Assignments** |
| Neha | Analyze and write software test plan. |
| Simran | Test case writing and execution for features ID: 1-4. |
| Nikhil | Test case writing and execution for features ID: 5 |
| Yeshwanth | Executing test cases and documentation. |

|  |  |
| --- | --- |
| **Test Case Field** | **Details** |
| Test Case ID: Access Control | 1: Successful login   * 1. User authentication with password   2. User authentication with OTP   3. Captcha to check if a robot or not. |
| Purpose | Tests that the user can log in with a proper username and password. |
| Initiation Criteria | All cookies cleared and user must be logged out.  User must have his registered phone with them for dynamic OTP. |
| Execution Steps | 1. Navigate to Web site. 2. Enter a valid username. 3. Enter a valid password. 4. Click on generate OTP button. 5. Enter the OTP received on phone. 6. Click enter button. |
| Expected Results | User is logged in to company portal. |

|  |  |
| --- | --- |
| **Test Case Field** | **Details** |
| Test Case ID: Monitoring and logging | 2: Successful detection   * 1. Generate an alert on login attempted after a certain no. of times.   2. Create logs of user activity |
| Purpose | Tests for any access breach or unauthorized user access |
| Initiation Criteria | All cookies cleared, start afresh to count the no. of login attempts. |
| Execution Steps | 1. Enter a valid username and password once.   1. If wrong enter again until success. 2. System to detect unusual activity and generate alert. 3. Validate via email or reset password. 4. Generate logs every time user gets logged in. |
| Expected Results | User activity is recorded. |

|  |  |
| --- | --- |
| **Test Case Field** | **Details** |
| Test Case ID:  Regular backups and updates | 3: Prevent data loss  3.1 Create and schedule jobs for backups at specific dates outside business hours.  3.2 Check and update softwares |
| Purpose | Tests for any available updates for all tools used and have backups to prevent data loss. |
| Initiation Criteria | System must be up and running with undisrupted connection. |
| Execution Steps | 1. Check for any available software or tool update.  2. Update or schedule to update after business hours.  3. Prepare and set up space for backups.  4. Check for any missing data or files.  5.Create backup jobs that run on scheduled hours. |
| Expected Results | Data backups and software updates completed timely. |

|  |  |
| --- | --- |
| **Test Case Field** | **Details** |
| Test Case ID:  Employee Training | 4: Awareness.  4.1 Provide access to online courses regarding secure practices.  4.2 Organize sessions. |
| Purpose | Verify that every member of each team is aware of the security policies. |
| Initiation Criteria | Check availability of each employee before arranging a session. |
| Execution Steps | 1. Provide access to online courses for secure systems.  2. Collect report after completion of courses by each employee.  3. Arrange in-person sessions to create awareness on data security, backups, and recovery.  4. Conduct mandatory assessments yearly. |
| Expected Results | Each employee is aware of the secure practices followed in the organization. |

|  |  |
| --- | --- |
| **Test Case Field** | **Details** |
| Test Case ID: Firewall | 5.Establish Security Policies  5.1 Deploy network security.  5.2 architect firewall zones and Ip addresses |
| Purpose | To protect the data from preventing Hackers to enter into our database by creating a firewall |
| Initiation Criteria | platform base, feature set, performance, manageability, price, and support. |
| Execution Steps | 1. Secure your firewall. 2. Architect your firewall zones and IP addresses. 3. Configure access control lists. 4. Configure your other firewall services and logging. 5. Test your firewall configuration. |
| Expected Results | Required Firewall has been setup for the protection of our data. |