Name : Alok Bhawankar
Roll : 1032170126

ISM

Theory 1

Q1. what are attacks and threats to IS?

⇒ Threat is an object, person or other entity that presents on ongoing danger to an asset compromises of Intellectual property. An attack is an information security threat that involves an attempt to obtain alter, destroy, remove or reveal information access or permission.

Types of Viruses:

1. Deliberate Software Attack:
It occures when an individual or group design and deploy to attack a system.
These software components are designed to damage target system.

2. Virus - A computer virus consist of segments of code that perform malicious actions many times user unwittingly help virus get into the system opening infected mail or same other seemingly.

3. Worms - worms are malicious program that replicate itself constantly. They can replicate until they fill available resources.

4.

4 Trojan Horse - They are software program that hide true nature and reveal their behaviour activated

Types of Attacks

1. Malicious code - Includes execution of viruses worms, Trojan horse with intent to steal or destroy information. Software application like bots, Spyware, etc.

2. Spoofing - Technique used to gain unauthorized access to computers IP indicating message coms from trusted source.

3. Spam - Spam is unsolicited commercial email many organization.

4 Mail Bombing :- Type of Dos attack in which attacker routs large quantities of mails.

5 Social Engineering - Process of using social skills to convince people to reveal access credentials to attacker

6 Phishing - Attempt to gain persond or financial information.

7 Pharming - Redirection of web traffic to an privare information

Q2 What is Risk Management ? How to Identify Risk?

=> Risk Management is the process or identifying risk as represented by vulnerabilities to an organization, information, assets and infrastructure and taking steps to reduce an acceptable level.

* Identify Risk:
1. Plan and organize the Process
2. Asset Identification and Inventory
3. People procedures and data Identification
4. Hardware, Software or Network asset
5. Automated Asset Inventory tools

Risk Control strategies.

1) Defend -
- Application of Policy
- Education and training
- Application of Technology

2) Transfer - Attempts to shift risk to other assets

3) Mitigate - Attempts to reduce the impact caused by exploitation of vulnerability through plannings and preparation.

4. Accept - choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.

5. Terminate - Instead of using a safeguard to protect an asset or deploying zero safeguards and accepting risks.

Q3 Explain purpose of security policies? Also discuss on Enterprise ISP, Issue specific ISP system specific?

⇒ A security policy could be high level documents or set of documents that describe in detail the safety control to implement in order to protect the corporate.

- Enterprise Information security Policy
- Typically Addresses compliance in 2 areas:

1. General compliance to ensure meeting the requirement to establish a program.

2. The use of specified penalties

* Issue specific security policies.

Independent ISSP document specific issue.
Single comprehensive - covering all issues
modular ISSP - unit policy creation & administration

System specific security Policy:
It might describe the configuration and the operation of Network Firewall

Q4 What is purpose of security model? Write brief on Access control.

=> Purpose of management security model is of what an organization should do to provide a secure environment for itself.

1. Discretionary Access control (DAC)
DAC is type of access control system that assign access right based on rules specified by user.
DAC model takes it based on advantage of using access control list and capability tables

2. Role base Access control:
Also known as non-discretionary access control is used when system within the organization. RBAC assigns based on roles.

3. Mandatory Access control (MAC)
considered as the strictest of all levels. The system design and implementation mostly used by government.

MAC defined Integrity levels are system, High, medium, low, untrusted.

Q5 What are security management models? Write Note on models.

→ Security management model is meant to be a generic description of what an organization should do to provide secure environment for itself.

1. Bella - LaPadula
   - simple: no read up
   - * (star): no write down
   - Also called as multilevel model for enforcing access control in government & military application

2. Biba
   - developed to address concerns of integrity
   - In biba model user can only create content at or below their own integrity level.

3 Clark - wilson:
   It was created in 1987. Addresses all goals of Integrity. dictates that seperation of duties must be enforced subjects must access data through an application.

4. Graham Denn
- The Graham Dennie model is a computer ~~see~~ security model that shows how subsets mainly used in access control of distributed system.

5. Harriyan-Ruzzo-Ulman:
Based on idea of Finite set of procedure being available to edit access right of on object.

6. Bewr-Nash:
Also known as chinese was model. Used to design to provide controls that mitigate conflict of interest in commercial organizations