12.09.2024

Key objectives:

1. Confidentiality:

1.1 data confidentiality

1.2 Privacy

2. Integrity:

2.1 data integrity

2.2 system integrity

3. Availability

Goals: Prevention, detection, recovery

Security management process:

1. Identify security controls. NIDS (network intrusion detection system)

2. Implement security controls (previous incident wise) IDS(intrusion detection system), IPS(intrusion prevention system)

3. Monitoring security control (anti-virus notifications)

CIA Triad : Confidentiality, Integrity ,Availability

1. Vulnerabilities

2. Threats

3. Risk= likelihood \* impact , 1\*2

4. Attacks (physical, swe based , social eng, web app based , network based)

5. Security control (Prevention, detection, recovery)

DAD : Disclosure, Alteration, Denial

Data classification:

1. Personally identifiable information

2. Personal data

3. Sensitive personal info

4. Non-public personal info

Data security state: 1. At rest 2. In transit 3. In use

OSI security attack:

Attack, mechanism, service

Attacks :

Passive attacks : release of message contents and traffic analysis(sniffing)

Active attacks:

1. Masquerade

2. Denial of services

3. Modification 4. Replay

Commands:

Ifconfig

Passwd

Uname

Ip a