BSc-III (IRN) 3/10/24

Computer security incidents:

- It refers to events like unauthorised access, use, modification or destruction of data. Malicious activities leads to financial or data loss of individual or organization.

Types of Comp. security incidents:

1. Malware attack - (virus, worm, trojan, spyware)
2. phishing - (trick user, download unknown s/w)
3. Denial of service - overloads N/W & services and & DDOS prevent legitimate user.
4. Insider threat - insider employee misuse information
5. unauthorised Access - gain access to system & intrusion without permission
6. Data breaches - exposure of personal or financial data.
7. Configuration Errors - Misconfiguration in H/W & s/w.

Key Concepts of Info security:

1. Confidentiality (only available to valid user) data
2. Integrity (data remain accurate)
3. Availability (resource available for valid user)
4. Authentication (verify user identity)
5. Authorization (authorised user)

Incident Management (steps)

1. Incident identification
2. " categorization
3. " prioritization
4. " Response → mitigation
5. " Closure

Purpose of Incident Management :

1. Minimize operational damage (to business, downtime)
2. Mitigate damage (data integrity, financial loss)
3. Enhance security (system & overall security)
4. Ensure Compliance (Legal, Regulatory)
5. Effective decision Making (about security measures)
6. Preserve reputation & trust (with safety & transparency)
7. Better accountability (every stage of response)

Need / goal of Incident Response :

1. Ensure rapid recovery (affected system, services)
2. Identify root cause (How it occured)
3. Maintain Compliance (Legal)
4. Effective Communication & coordination
5. Preserve evidence & support investigation

Incident Response Plan:

It includes procedures & processes to effectively respond to manage security incidents. Plan includes:

1. preparation (use policies, tools & training)
2. identification (detect & classify incident)
3. Containment (short/long term strategies for prevention of damage)
4. Eradication (eliminate root cause of incident)
5. Recovery (check if system is back to normal)
6. Lesson Learned (document findings, identify areas of improvement)

Signs of Computer incident: (eg).

- unexpected traffic patterns
- unusual data transfer
- system performance degradation
- unfamiliar processes
- Multiple failed login attempts
- New user account
- Unexpected file modification
- " Antivirus Alert
- IDS/IPS Alert
- Multiple account Lockout
- phishing email.

Incident categories:

1. security incidents (data breach, phishing attacks)
2. H/w failure (component, system failure)
3. S/w issues (Application errors, compatibility issues)
4. User related incidents (User error, Access issues)
5. N/w problems (Connectivity, N/w security)
6. Compliance & Regulatory (policy violation
7. Third party incidents (Vendor, supply chain)

Incident prioritization

It is a process to determine order in which incidents should be addressed, based on urgency & impact. Matrix is given as follows.

Impact	Urgency	priority level	Description
High	High	Critical	Require immediate attention
High	Medium	High	address soon as possible
Medium	High	Medium	schedule for timely resolution
Medium	Medium	Low	Manage with regular workload
Low	Low	Minor	Address when convinient.

Estimating cost of an incident:

Incident Response:

It is systematic approach to Manage & address cyber security incidents to minimize impact and recover from attacks. steps involved in IR includes:

1. preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned.

Best practices in IR:

1. create clear IR plan
2. establish communication protocol
3. Use Advance detection systems
4. Conduct regular training & drill
5. Document everything.

Incident Handling:

It refers to structured process of Managing and resolving security incidents that could disrupt the operation of an organization. steps in incident Handling:

1. preparation
2. identification
3. Containment
4. Eradication
5. Recovery
6. post incident Analysis

Estimating Cost of an Incident:

Cost estimation in the context of cyber security involves direct & indirect factors. total cost vary based on nature & severity of the incident. Key cost components include.

Direct Cost-

- detection & response Cost-
- Legal & Regulatory "
- Remediation & Regulatory "
- public relation & Communication Cost-

Indirect Cost:

- Reputational damage
- productivity loss
- Loss of Intellectual property
- opportunity Cost-

Long Term Cost:

- Future investment in security
- Customer leaving org / Marketing cost-

Example:

Calculate total cost of data breach, caused due to incident at- 'persistant' Hyderabad in year 2023.

total incident cost = (Detection & response) + (downtime cost) + (lost business revenue) + Legal regulatory (cost) + Remediation cost + Reputational damage

Total cost of data breach can be calculated as follows.

Cost Component	Description	Estimated cost (Rs)
1. Detection & Response	Personal visit to the incident site	20,000.00
2. Downtime cost (8 hrs)	System/NPU was down	2 00000.00
3. Lost business Revenue	No of no development, No function.	500000.00
4. Reputational cost	Damaged reputation of Company	1,50,000
5. Legal & Regulatory cost	Expenses towards Lawyer/court-matter	2 50,000.00
6 post incident Remedy	preventive Measure taken by each dept / Unit	2 00000.00
		Total (Rs) ....

Incident Reporting:

- It is process of documenting & communicating details about the incident in prescribed format
- goal of reporting:
  - effective communication
  - proper response & resolution
  - Maintain record for analysis & compliance.

Incident reporting organization

1. CERT (Comp. Emergency Response team)
2. ISACs (Info. sharing & Analysis centre) for financial, Healthcare & Automotive.
3. government Agencies.
   - IC_3 - Internet crime Complaint Centre
   - CISA - Cyber security & Infrastructure security Agency.

Incident Response Team / Team Members. (Roles & Responsibility)

1. Incident Response Manager (Communicate, report)
2. security Analyst (Monitor Alert, provide solution)
3. Threat Intelligence Analyst (Research, provide soln)
4. Forensic investigator (Collect evidence) Disease identify
5. Syslem Admin / N/W Engineer (Isolate / restore system)
6. Legal & Compliance officer (Ensure compliance)
7. public relation specialist (Manage communication with media)
8. Disaster recovery specialist (develop recovery plan)
9. Incident Response Coordinator (Keep track of actions)
10. External Advisor. (provide expert advice)