Incident Response Management

Dr Mukti Padhya

Assistant Professor

SCSDF, NFSU

CTMSDFIS S1 P3: Incident Response Management

- Subject Details
  - Teaching Scheme
    - Theory Credits : 3
    - Practical Credits : 1
  - Evaluatuion Scheme
    - Internal Exams
      - TA1/ TA2 (25 Marks Each)
      - MId Sem Exam : 50 Marks
    - End Sem Exam : 100 Marks
    - Practical End Sem Exam : 100 Marks

What is Incident Management?

- **CYBER SECURITY EVENT**
  - A cyber security change that may have an impact on organisational operations (including mission, capabilities, or reputation).

- **CYBER SECURITY INCIDENT**
  - A single or a series of unwanted or unexpected cyber se_x0002_curity events that are likely to compromise organisational operations.

- **CYBER SECURITY INCIDENT MANAGEMENT**
  - Processes for preparing, detecting, reporting, assessing, responding to, dealing with and learning from cyber security incidents.

Information Security : Terminology

- "Information security" is a state of well-being for information and infrastructure in which the possibilities of information and services theft, tampering, and disruption are low or tolerable

Assurance that the information is accessible only to those **authorized to have access**

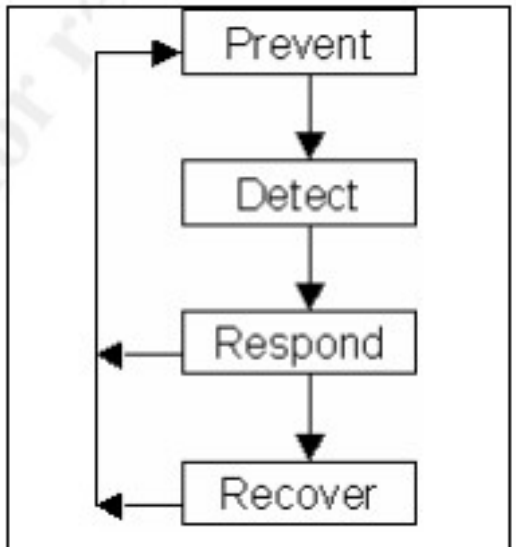
Trustworthiness of data or resources in terms of preventing improper and unauthorized changes

Assurance that the systems are **accessible when required** by the authorized users

Characteristic of a document, communication, or **dataset that ensures that it is genuine**

Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Computer Security



Preventative Operations

Preventative operations are all the activities performed to prevent the compromise of the confidentiality, integrity and availability of all the information that is processed, stored, and transmitted using a computer.

Prevention activities range from creating an information security policy to conducting user training sessions to implementing technical solutions such as access controls or firewalls.

Detection Operations:

Detection activities range from compliance inspections to whistle-blowers to implementing technical solutions such as Intrusion Detection Systems or Integrity Assurance Software.

Response operations

Response activities range from unplugging the network cable to blocking an IP address at the firewall.

Recovery operations

Recovery operations range from initiating the Business Continuity or Disaster Recovery Plan to conducting user awareness sessions to implementing technical solutions such as disk mirroring or automated backups.

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates from the notion that the target system stores or processes something valuable; this signals that the system may be under threat of an attack
- Attackers try various tools and attack techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Motives Behind Information Security Attacks

- Disrupting business continuity
- Information theft and data manipulation
- Creating fear and chaos by disrupting critical infrastructures
- Financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge
- Demanding ransom

Impact of Information Security Attacks

Information security attacks are a **major security concern** for any organization as they can severely impact an organization's assets, resources, financial records, and other confidential data

Financial Losses	Financial losses faced by the organization may be **direct or indirect**
Loss of Confidentiality and Integrity	Results in the **loss of trust in data or resources**; damage to the corporation's reputation; and the loss of goodwill, and business credibility
Damaged Customer Relationship	Impacts the organization's relationships with its customers, leading to the **loss of customers**, a **decrease in sales**, and a **drop in profits**
Loss of Business Reputation	**Hurts the business's reputation**, leading to loss of existing loyal customers as well as of the potential to attract new customers
Legal and Compliance Issues	Results in **negative publicity for the organization** and affects the business's performance
Operational Impacts	May **disable the organization** by disrupting the operations of an entire organizational network

Information Warfare

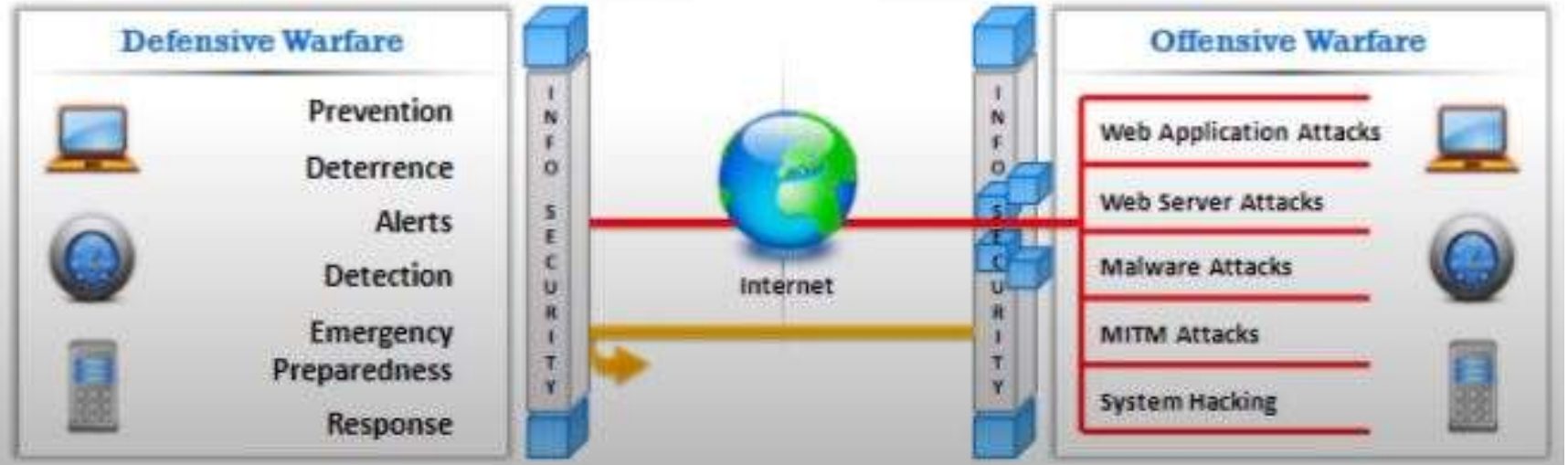
- The term "Information Warfare" or "InfoWar" refers to the **use of information and communication technologies (ICT)** as competitive advantages over an opponent

Defensive Information Warfare

Refers to all strategies and actions to **defend against attacks on ICT assets**

Offensive Information Warfare

Refers to information warfare that involves **attacks against ICT assets** of an opponent



Information Security Incidents

ECIH

- "An information security incident" is a network or host activity that impacts the security of information stored on network devices or systems with respect to confidentiality, integrity, and availability
- May be any **real or suspected adverse event** in relation to the security of computer systems or networks
- A **violation or imminent threat** that has the potential to impact computer security policies, acceptable use policies, or standard security practices

Types of Information Security Incidents

1 Malicious Code or Insider Threat Attacks	4 Email-based Abuse	7 Employee Sabotage and Abuse
2 Unauthorized Access	5 Espionage	8 Network and Resource Abuses
3 Unauthorized Usage of Services	6 Fraud and Theft	9 Resource Misconfiguration Abuses

Category	Types
Service Interrupts	- Denial of Service - Mail Bomb - Ping Attacks - Multiple Request Attack - Root Compromise - Packet Floods - IRC Bots - Virus Infections
Computer Interference	- Port Scans - System Mapping - System Probe
Unauthorised Access	- Identity Theft - Unauthorised Release of Data - Theft or Modification of Data
Malicious Communication	- Threats - Hate Mail - Harassment Mail - IRC Abuse - Flaming directly to Individual
Copyright Violation	- MP3 - Warez: Sites - Video Copyright - Content Violation
Theft	- Physical Theft of Hardware and Peripherals - Theft of Software - ID Theft - Credit Card Theft - Password Theft

Events and Incident

What is an event

- An event is any observable occurrence in a system or network.
- Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- As far as our field is concerned, We will only address adverse events that are computer security related, not those caused by natural disaster or power failures.

What is Computer Security Incident

- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:
  - An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
  - Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  - An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
  - A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Cont.

- In the context of information technology, an incident is an event that disrupts operational processes.
- An incident may involve the failure of a feature or service that should have been delivered or some other type of operation failure.
- Security incidents are events that indicate that an organization's systems or data may have been compromised.

Cont.

- It is an act of violating explicit or implied security policy resulting in, unauthorized access, denial of service/disruption, and unauthorized use of a system for processing or storage of data or change to system software, hardware, firmware characteristics without the owner's knowledge.
- Incidents include minor disruptions, such as running out of disk space on a desktop machine, as well as major disruptions, such as data breaches involving the exposure of sensitive information.

Cont.

- Each organization must define what a computer security incident is for their site.
- Examples of general definitions for a computer security incident could be:
  - “Any real or suspected adverse event in relation to the security of computer systems of computer networks”
  - “The act of violating an explicit or implied security policy”

Types of Incidents

- DoS and DDoS
- MiTM attack
- Phishing or Pharming attack
- Drive-by attack
- Password attack
- SQL Injection
- Eavesdropping attack
- Malware attack
- Vulnerability Scanning

Types of Malware

- Viruses
- Spyware
- Adware
- Ransomware
- Keylogger
- Botnet

- Backdoor
- Downloader
- Launcher
- Rootkit
- Scareware
- Spamware

Viruses

- Created to relentlessly self-replicate
- it infects programs and files. The malicious activities may be targeted at destroying valuable data or causing unrepairable damages

Backdoor

- Malicious code that installs itself onto a computer to allow the attacker access.
- Backdoors usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.

Downloader

- Malicious code that exists only to download other malicious code.
- Downloaders are commonly installed by attackers when they first gain access to a system.
- The downloader program will download and install additional malicious code.

launcher

- Malicious program used to launch other malicious programs.
- Usually, launchers use nontraditional techniques to launch other malicious programs in order to ensure stealth or greater access to a system.

rootkit

- Malicious code designed to conceal the existence of other code.
- Rootkits are usually paired with other malware, such as a backdoor, to allow remote access to the attacker and make the code difficult for the victim to detect.

Spyware

- The software is created to spy on the victim.
- It is secretly implanted on the computing device by the hacker.
- The spyware gathers information and sends it to the hacker.

Adware

- The malicious program is devised to pop-up unwanted advertisements on the victim's computer without their permission.
- The pop-ups are uncontrollable and tend to behave erratically.

scareware

- Malware designed to frighten an infected user into buying something.
- It usually has a user interface that makes it look like an antivirus or other security program.
- It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their “software,” when in reality, the software it’s selling does nothing more than remove the scareware.

Spamware

- Malware that infects a user's machine and then uses that machine to send spam.
- This malware generates income for attackers by allowing them to sell spam-sending services.

Ransomware

- The ransom malware blocks the user from accessing the files or programs and the malware removal demands to pay the ransom through certain online payment methods.
- Once the amount is paid the user can resume using their system.

Key-Logger

- Tools designed to record every keystroke on the affected machine for later retrieval
- It stores the data regarding each and every key user presses on the keyboard.
- It is very commonly used method to get username and passwords from a legitimate user.

Botnet

- The cybercriminal blocks a user actions and takes full control of the system.
- The hacker creates a network of malware-infected computers which functions as a bot.
- The botnet is used to transmit malware, send spam emails, and execute other malicious tasks.

Sign of an incident

Sign of an incident

- Signs of an incident fall into one of two categories: precursors and indicators.
  - A precursor is a sign that an incident may occur in the future.
  - An indicator is a sign that an incident may have occurred or may be occurring now.

Sign of an incident

- Most attacks do not have any identifiable or detectable precursors from the target's perspective.
- If precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack.

Sign of an incident

- Examples of precursors are:
  - Web server log entries that show the usage of a vulnerability scanner.
  - An announcement of a new exploit that targets a vulnerability of the organization’s mail server.
  - A threat from a group stating that the group will attack the organization.

Sign of an incident

- While precursors are relatively rare, indicators are all too common.
- Too many types of indicators exist to exhaustively list them, but some examples are listed below:
  - A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
  - Antivirus software alerts when it detects that a host is infected with malware.
  - A system administrator sees a filename with unusual characters.
  - A host records an auditing configuration change in its log.
  - An application logs multiple failed login attempts from an unfamiliar remote system.
  - An email administrator sees a large number of bounced emails with suspicious content.
  - A network administrator notices an unusual deviation from typical network traffic flows.

Incident Category

- Generally, Incidents are divided into three main categories:
  - High
  - Medium
  - Low

Incident Category - HIGH

- The severity of a security incident will be considered “high” if any of the following conditions exist:
  - Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire UNIT is affected)
  - Poses a potential large financial risk or legal liability to the Organization.
  - Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)

Incident Category - HIGH

- It adversely impacts an enterprise system or service critical to the operation of a major portion of the organization (for example, e-mail, customer information system, Financial information system, human resources information system, etc.).
- It poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
- It has Has a high probability of propagating to many other systems on premise and/or off premise and causing significant damage or disruption.
- High severity incidents require an immediate response and focused, dedicated attention by the CISO and other appropriate officials and IT security staff until resolved.

Incident Category - Medium

- The severity of a security incident will be considered “medium” if any of the following conditions exist:
  - Adversely impacts a moderate number of systems and/or people, such as an
  - individual department, unit, or building
  - Adversely impacts a non-critical enterprise system or service
  - Adversely impacts a departmental system or service, such as a departmental file server
  - Disrupts a building or departmental network
  - Has a moderate probability of propagating to other systems on premise and/or off premise and causing moderate damage or disruption

Incident Category - Medium

- Medium severity incidents require a quick response by appropriate personnel (usually from the affected unit) who have primary responsibility for handling the incident.

Incident Category - LOW

- Low severity incidents have the following characteristics:
  - Adversely impacts a very small number of systems or individuals
  - Disrupts a very small number of network devices or segments
  - Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate
- Since a single compromised system can “wake up” and negatively affect other systems at any time, appropriate personal (usually the technical support staff responsible for the system) must respond as quickly as possible, no later than the next business day.

Identify an Incident

- Event Management
  - Event Management provides qualified alerts when one or more Configuration Items (CI) have encountered a disruption in its normal functioning or may encounter disruption in its normal functioning. In practice, Event Management may lead to generation of a manual incident OR an automated incident creation.
- From Web Interface
  - Web interface is a very efficient method to identify incidents as it involves no human interface to log the ticket. Organization need to provide a intuitive interface to the end users to log incidents.

Identify an Incident

- Phone Calls
  - Phone calls is the most common way of reporting incidents. This is a labor intensive method to report incidents. However this method has its own merits as end-user incidents can be quickly resolved via First Call Resolution, thus improving customer satisfaction substantially.
- Email Interface
  - Emailing incident details to Service Desk is the easiest method to report an incident. However, in most cases, this mode of incident reporting is rigged with lot of inefficiencies.