Ch.8 summary By @MHazazi

Standard Operating Procedures (SOPs) or standard operating protocols.

- SOPs is detailed explanations of how to perform a task.
- SOPs Objectives is to provide direction to improve communication, reduce training time, and improve work consistency.
- SOPs should be documented to protect the company from the pitfalls of institutional knowledge
- SOPs should be written as simple a style as possible for all to clearly understand the procedures
- SOPs should include all steps of a given procedure
- SOPs should not be overly detailed and should remain clear

- **Common SOP formats:**
  - simple step, hierarchical, flowchart, graphic
  - 2 factors determine what type of SOP to use:
    - how many decisions the user will need to make
    - how many steps are in the procedure

Many Decisions?	More Than Ten Steps?	Recommended SOP Format
No	No	Simple Step
No	Yes	Hierarchical or Graphic
Yes	No	Flowchart
Yes	Yes	Flowchart

- After a procedure, has been researched, documented, reviewed, and tested, it should be authorized by the process owner.
- The integrity of the SOP documents must be protected .
- Change management process must be defined so SOPs mirror the evolution of business processes
- All revisions of the SOP documents must be reviewed and approved by the process owner

Operational Change Control

- **Change control:** Internal procedure where only authorized changes are made to software, hardware, network access privileges, or business processes.

- Change control process:

1) **Starts with a Request for Change (RFC)**
   - Description of the proposed change
   - Justification why the change should be implemented
   - Impact of not implementing the change
   - Alternatives
   - Cost
   - Resource requirements and timeframe

   The change is then evaluated and if approved implemented

2) **Change control plan**
   - Developed after the change is approved
   - **Components**:
     - Security review to ensure no new vulnerabilities are introduced
     - Implementation instructions
     - Rollback and/or recovery options
     - Post implementation monitoring

3) **Change must be communicated to all relevant parties**
   - Two categories of messages
     - Messages about the change
     - Messages how the change will impact employees

4) **All actions should be documented throughout the implementation process**

Why Is Patching Handled Differently

- **Patch =** Software or code designed to fix a problem
- Security patching is the primary method of fixing security vulnerabilities
- Patches need to be applied quickly
- **Patch management:**
  - The process of scheduling, testing, approving, and applying security patches
  - Patching could be unpredictable and disruptive
  - User should be notified of potential downtime

Malware Protection

- **Malware =** malicious software
  - designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems and mobile devices.
  - bundled with other programs or self-replicated
  - Typically requires user interaction

- **Advanced persistent threats (APTs)** is when malware is designed to quietly, slowly spread to other hosts, gathering information over extended periods of time and eventually leading to exfiltration of sensitive data and other negative impacts

- **Malware categories:** based on infection and propagation characteristics

Virus	Piece of self-replicating code embedded within another program (host)
Worm	Self-contained program, Spreads through a computer network, Exploits security holes in network computers.
Trojans	- malicious code that masquerades as a legitimate benign application - open connections to a command and control server keylogger ,screen scraper
Bots	Backdoor Trojan responds to commands sent by a command-and-control program on another computer
Ransomware	Type of malware that takes a computer or its data hostage in an effort to extort money from victims . Lock screen ransomware , Encryption ransomware
Rootkits	A set of programs that provides privileged access to a computer
Spyware/adware	Program communicates over Internet connection without user's knowledge
Hybrid	code that combines characteristics of multiple categories

How Is Malware Controlled

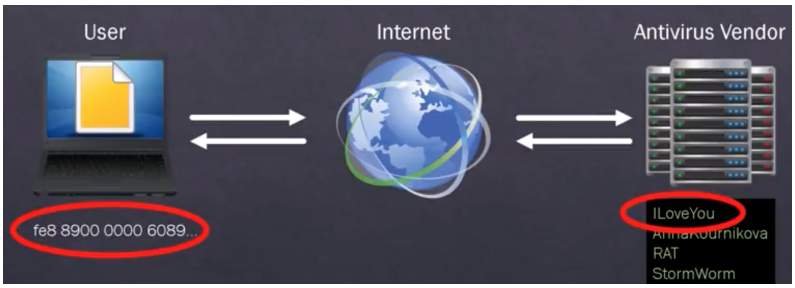
- **Defense in depth**

  implementing prevention, detection, response controls, in addition to security awareness camp
- **Prevention controls =** Stop an attack before it occurs
- **Detection controls**
  - Identify the presence of malware
  - Alert the user
  - Prevent the malware from carrying out its mission

What Is Antivirus Software?

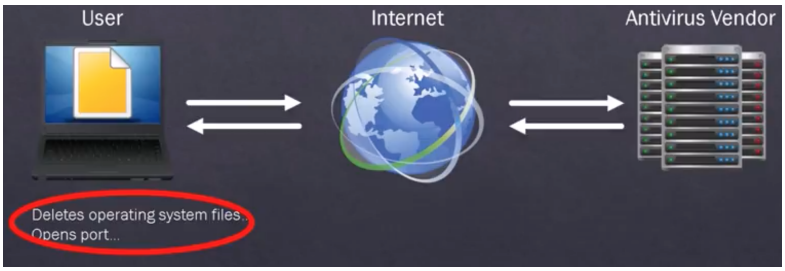
- Software used to detect, contain, and in some cases eliminate malicious software
- The core of AV software is known as the “engine.” It is the basic program.
- The program relies on virus definition files (known as DAT files) to identify malware.
- The definition files must be always updated by the software publisher & then distributed to user
- **AV are limited due to the following :**
  - the sheer volume of new malware
  - the phenomena of “single-instance” malware
  - the sophistication of blended threats
- **AV software employs two techniques:**

  1) **Signature based virus recognition**



  - Any created viruses will have signature (hash file).
  - Cybersecurity community, revels this kind of signature, by analyzing the virus once released.
  - These hashes are stored in databases which get updated regularly.
  - If you get any virus, your Antivirus App compare the hash code of that file with its database, if any partial match has found, this file will be quarantined or deleted.

2) **Behavior(Anomaly)based virus recognition**



- Any created viruses shall do specific action or process or behavior (delete files, opens port, delete OS files)
- If you get infected file, the Antivirus App inspect the file to see what does that file do!
- AV will compare the behavior to a list of known malicious behaviors stored in databases.
- If that infected file starts to delete files, opens a port, or delete a system file, it will be flagged out and quarantined or deleted.

Data Replication

- **Data Replication**

  Copying data to a second location that is available for immediate or near-time use.
- **Data backup**

  Copying and storing data that can be restored to its original location.
- **Failure to back up threatens data availability and data integrity**
  - Lost/corrupt data can also have a negative impact on the company:
    - Financially
    - Legally
    - PR-wise
- **The following aspects should be considered when the strategy is designed:**
  - Reliability
  - Speed
  - Simplicity
  - Ease of use
  - Security of the stored information
- Backed-up or replicated data should be stored at an off-site location in an environment secured from theft, the elements, and natural disasters
- Insure that information stored on the backup media is restorable in case of an incident
- Restores should also officially scheduled.

Securing Messaging

- E-mail is, by default, an insecure way to transmit information.
- Documents sent as e-mail attachments might contain more information like Metadata

  Metadata : Details about a file that describes or identifies it, such as title, author name,etc
- E-mail is an effective method of distributing malware (embaded,hyperlink)
- **Compromising the e-mail server**
  - **Relay abuse:** using the mail server to distribute spam and malware
  - **DOS attack :** against an e-mail is an attack against the availability of the service
  - **e-mail server should be set up to not allow an open relay of SMTP traffic.**
  - **Failure do to so implies two issues:**
    - The e-mail server will be used by unscrupulous spammers
    - The domain name used for e-mail purposes will be blacklisted

Activity Monitoring and Log Analysis

- **Log:** A record of the vents occurring within an organization's systems and networks
- Almost every device and application on the network can log activity
- Log management:
  - Configuring the log sources, including log generation, storage, and security
  - Performing analysis of log data
  - Initiating appropriate responses to identified events
  - Managing the long-term storage of log data
- **Syslog** = provides an open framework based on message type and severity
- Log analysis techniques:
  - Correlation = ties individual log entries together based on related information
  - Sequencing = examines activity based on patterns
  - Signature = compares log data to "known bad" activity
  - Trend analysis = identifies activity over time that in isolation might appear normal.

Service Provider Oversight

- Service providers include vendors, contractors, business partners and affiliates who store, process, transmit, or access company information on company information systems.
- Service providers internal controls should meet or exceed those of the contracting organization
- Due diligence is the process used to assess the adequacy of service providers
- SSAE16 audit reports are the most widely accepted due diligence documentation