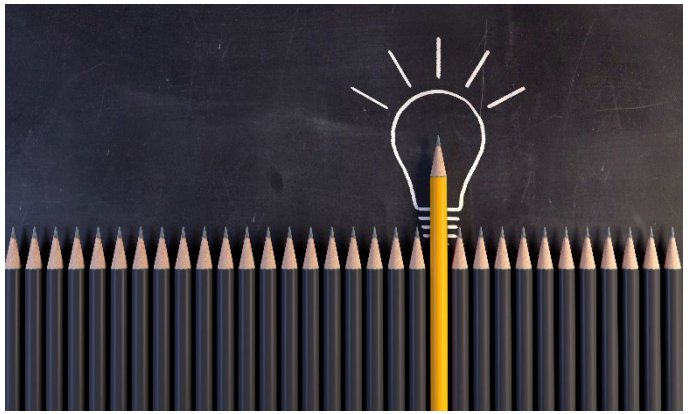
03-Threats, Vulnerabilities, and Risk Management

Learning Objectives

- Define vulnerabilities.
- Identify the common sources of vulnerabilities.
- Define vulnerability scanning.
- Demonstrate understanding of threats.
- Describe risk and risk management techniques.



Vulnerabilities

- A vulnerability is a weakness, or a hole in the system that makes the system exposed to the possibility of being attacked or harmed.
- An exploit takes advantage of a vulnerability to cause unintended behavior.
- For example, software bugs are flaws that cause unintentional damage.
  - They are inevitable in a complex system.
  - Attackers and malware often exploit software bugs to gain unauthorized access or cause damage.
  - Most software vendors provide patches (software updates) to fix these bugs and close any vulnerabilities throughout the planned lifecycle of their software.

Sources of Vulnerabilities 1/3

Information systems may have vulnerabilities due to platforms, wrong configurations, third parties, patches, or zero-day vulnerabilities.

- Platforms: a computer platform is a system that consists of the hardware device and an OS that runs software. Platforms can be categorized into:
  - Legacy Platforms: some enterprises still use an old platform with an old OS that cannot be updated anymore. With no security updates to the OS, these platforms are the most vulnerable.
  - On-Premises Platforms: on-premises platforms were considered the secure model of computing since everything is in the company's location. However, the continuous need for expansion and new technologies always emerging made these platforms harder to protect.
  - Cloud Platforms: many organizations are moving to cloud platforms nowadays for their computing resources. However, since cloud resources are complex and accessible from virtually anywhere, they introduce new vulnerabilities often due to misconfiguration.

Sources of Vulnerabilities 2/3

- Configurations: with modern hardware and software introducing new features, vulnerabilities often come as a result of weak configurations and security settings such as:
  - Default settings (vendors usually set the defaults to provide ease of use, not for security).
  - Open ports and service.
  - Unsecured root accounts.
  - Open permissions (users access files that should be restricted).
  - Unsecure protocols.
  - Weak encryption.
  - Mistakes and errors.
- Third Parties: outsourced services such as code development and data storage often grant access to a third party which could introduce vulnerabilities to the organization's system as a result of improper system integration.

Sources of Vulnerabilities 3/3

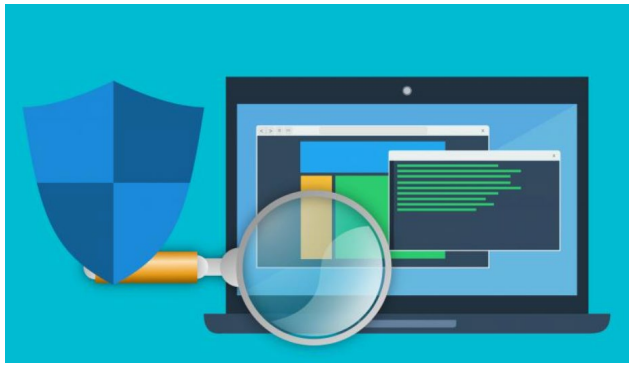
- Patches: as important as patches are, they can create vulnerabilities as a result of:
  - Difficulty patching software embedded in the hardware (firmware).
  - Few patches for application software. Some vendors don't automate patches, others don't provide patches at all.
  - Delays in patching OSs: because new patches may introduce new problems, some organizations take time to test the patch before applying it.
- Zero Day: vulnerabilities that have not been patched yet. The vulnerability could be known to the vendor, but its patch is not complete, or even not known at all.

Question

- A company has an accounting software that can only be run on Windows 7. Knowing that Microsoft ended the life cycle of Windows 7 in 2020 (i.e., no more software updates), this system could be classified in which category of vulnerabilities?
  - Misconfiguration vulnerabilities.
  - Third-party vulnerabilities.
  - Zero-day vulnerabilities.
  - Legacy platform vulnerabilities.
  - Delayed operating system vulnerabilities.

Vulnerability Scanning

- A vulnerability scan is a frequent and ongoing process that continuously identifies vulnerabilities and monitors cybersecurity progress.
- The goal of a vulnerability scan is to detect vulnerabilities in the organization's system and create a mitigation strategy.
- Vulnerability scans can be conducted to assess vulnerabilities in one or a combination of the following:
  - Applications, such as the organization's web app.
  - Networks.
  - Databases and their configurations.
  - Hosts, such as critical servers and devices.
- The Mitre Common Vulnerabilities and Exposures (CVE) identifies vulnerabilities in operating systems and application software.
  - Their updated list of vulnerabilities can be used to feed vulnerability scanning software.



Types of Vulnerability Scanning

- Several types of scans exist, two major types are:
  - Credentialed vs. Non-credentialed Scans:
    - In a credentialed scan, valid authentication credentials, such as usernames and passwords, are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials.
    - A non-credentialed scan provides no such authentication information.
  - Intrusive vs. Nonintrusive Scans:
    - An intrusive scan attempts to employ any vulnerabilities that it finds, much like a threat actor would. These are more accurate but can impair the target system.
    - A nonintrusive scan does not attempt to exploit the vulnerability but only records it.
- Vulnerability scanning tools may produce a large list of discovered vulnerabilities. Security personnel must assess and prioritize which ones are critical and need to be addressed based on:
  - Importance: some vulnerabilities are of low importance to a company, but critical to another.
  - Accuracy: some vulnerabilities detected can be false positive.

Question

- A vulnerability scanning tool is configured to scan for vulnerabilities without attempting to exploit any found vulnerability. What type of vulnerability scan is this?
  - Non-intrusive scan.
  - Intrusive scan.
  - Non-credentialed scan.
  - Credentialed scan.
  - Black-box scan.

Threats

- A threat is something that has the potential to cause harm.
- It's a possible danger that could compromise the CIA or security posture of a system.
- Could be malicious (intentional) or accidental.
- Could be external or internal.
- Often is specific to certain environments:
  - a virus might be problematic on a Windows system but has no effect on a Linux system.

Risks

- Risk is the likelihood that something bad will happen.
- For an environment to have a risk, there must be a vulnerability and a threat that could exploit it.

  Example:

  - Light a fire near a wood structure
    - Threat: Fire.
    - Vulnerability: wood structure.
    - You definitely have a risk.
  - If the structure is made of concrete
    - No credible risk since the threat (fire) doesn't have a vulnerability to exploit.
- Risks must be managed to avoid/reduce potential harm.

Impact

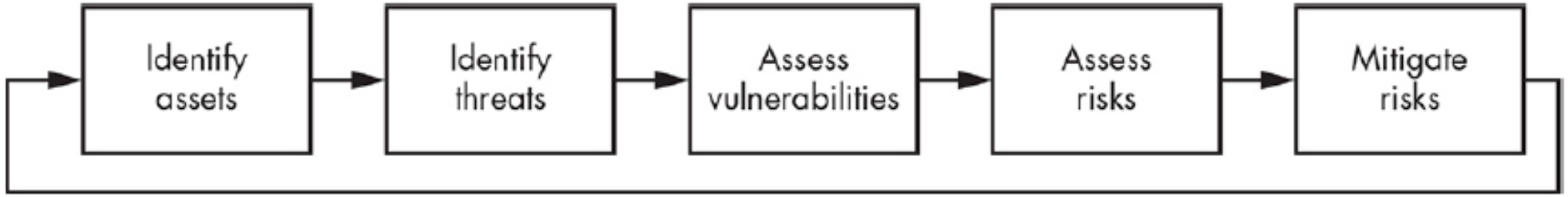
- Some organizations, such as the US National Security Agency (NSA), add a factor to the threat/vulnerability/risk equation called impact.
- Impact takes into account the value of the asset being threatened and uses it to calculate risk.

Example:

- You lose your USB drive:
  - If it contains the instructor's lecture slides, the impact is low, you can download them again from D2L.
  - If it contains your assignment, the impact is higher:
    - you may have to redo the assignment to submit it,
    - and make sure no one else submits your file as you may be at risk of academic dishonesty.

Risk Management

- Risk management refers to the steps taken to prevent/mitigate risks in an environment.

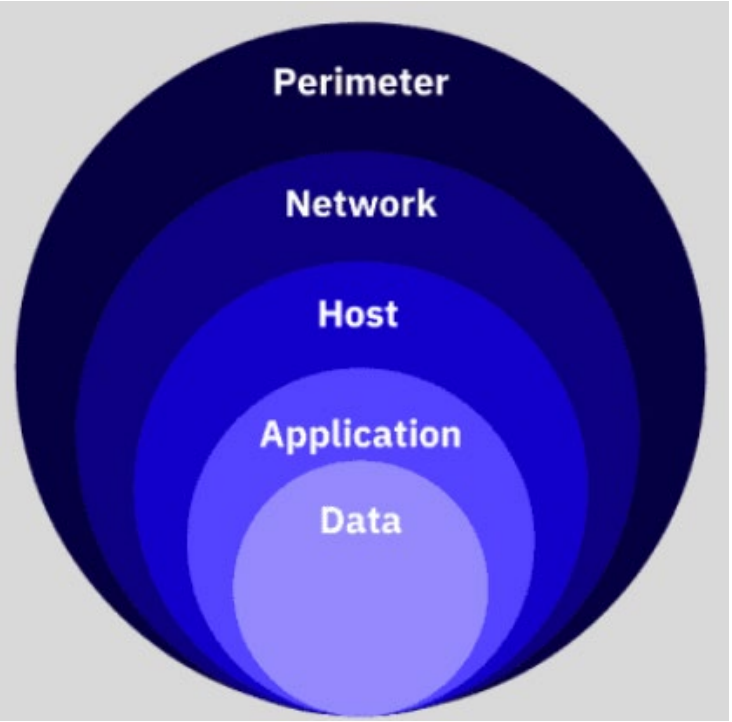


Risk Management

- Identify assets:
  - What is the most critical asset to protect? Is it hardware, software, data?
- Identify threats:
  - What threats could affect your assets and violate the CIA triad? Is it, power outage, virus, database breach, physical access?
- Assess vulnerabilities:
  - Any given asset may have thousands of threats, but only a small fraction of these will be relevant.
- Assess risks, if a vulnerability has no matching threat, there is no risk. Consider using the impact as well.
- Mitigate risks by taking measures (controls) to account for each threat:
  - Physical controls: fences, gates, cameras, fire suppression system, etc.
  - Logical controls: access control (privileges), data encryption, intrusion detection systems (IDS), etc.
  - Administrative controls: based on rules, laws, policies, procedures, guidelines, etc.
  - Train your team and educate the users. Humans tend to override controls, turning them into useless safeguards.

Defense in Depth

- Defense in depth is a strategy based on using multiple overlapping security mechanisms.
- Since nothing is 100% secure, defense in depth will allow keeping a successful resistance should one or more of the defensive measures fail.
- The goal is to place enough defensive measures between important assets and the attacker so that:
  - you'll notice that an attack is in progress, and
  - have enough time to prevent it.



The End

End of Slide Set