The 7 Layers of Cyber Security & Vulnerabilities

Module 8

Module 8 Agenda

- Finish Module 7 Activity 2
- The 7 Layers of Cyber Security
- Malware
- Vulnerabilities

Module 7 Activity 2

- Each team, take about 10 to 20 minutes to finish up Module 7 Activity 2

The 7 Layers of Cyber Security

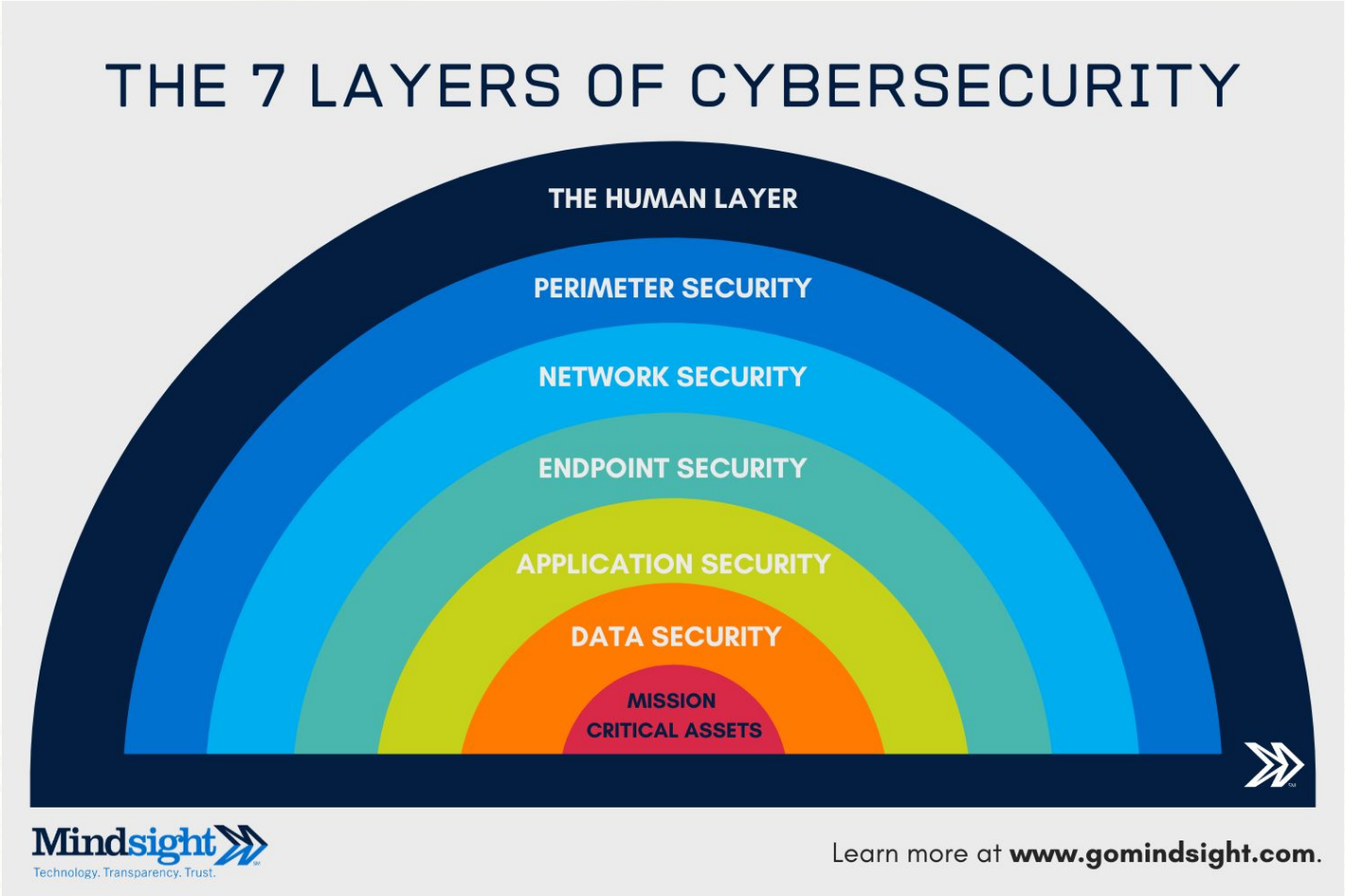
The 7 Layers of Cyber Security

1. **Mission Critical Assets**
   - This is the data that is being protected. Any asset an organization cannot function without (computers, software and data).
2. **Data Security**
   - Protecting your systems at this level would entail establishing reliable backups to save data, encryption of your data, and other policies such as Two-Factor Authentication (usernames & passwords).
3. **Application Security**
   - The testing and adding of application features to prevent and patch vulnerabilities.
   - Routine updating of applications and software to not leave any system open to an old exploit.
4. **Endpoint Security**
   - Protects the connection between the network and its devices
   - We can implement endpoint security through the use of antivirus software, web content filtering, and application controls.

The 7 Layers of Cyber Security

5. **Network Security**
   - At this layer, we are concerned with the breadth of access a user has within a network. It would be dangerous to grant every employee root access.
   - We need to provide people with the minimum amount of “user privilege” possible for them to do their job and nothing more.
6. **Perimeter Security**
   - Prevents suspicious activity from entering the network by protecting the gateway with firewalls, data encryption, anti-virus software.
   - Monitors and secures devices that transmit data outside of the walls of your network.
7. **The Human Layer**
   - Being aware of human threats like spamming, phishing, and any other clever form of social engineering.

The 7 Layers of Cyber Security



Malware

Malware

Malware: **Mal**icious Soft**ware**. Malicious code scripts, files, or programs that aim to deceive, manipulate or spy on the target user without their knowledge.

- Malware comes in different forms, and not limited to
  - Worms, Trojan Horses, Viruses, Keyloggers, Scareware

Another way to define malware is to know that malware is any software that compromises confidentiality, integrity, and availability of your computers.

- **Confidentiality**: No unauthorized reading
- **Integrity**: No unauthorized writing
- **Availability**: System are accessible, ready to use

Malware

Malware Propagation Methods:

- **Worms**
  - Worms are able to self-replicate, without the need for human interaction.
- **Computer Viruses**
  - Requires a human to spread. Usually hidden and embedded within an application or other software.
- **Social Engineering**
  - Also referred to as “human hacking”, involves taking advantage of the human element to gain access to unauthorized systems.
- **Malicious Websites**
  - Sometimes trustworthy websites can contain dangerous content.
- **Trojan Horses**
  - A malicious function contained within a seemingly benign product.

Malware

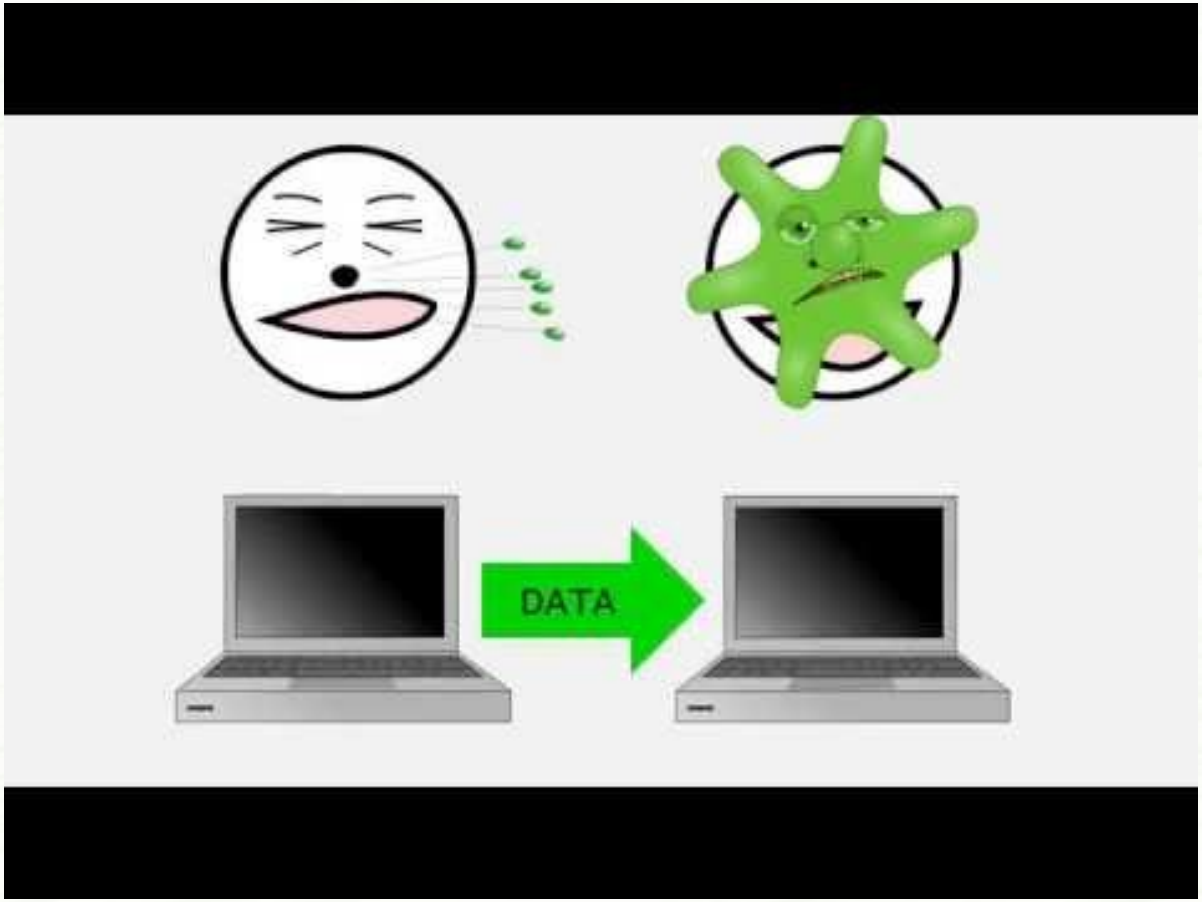
Malware Vessels:

- Removable Media (USB flash-drives)
- Internet Downloads
- E-mail Attachments
- Corrupt Files
- An unsuspecting user

Modern cyber attacks will implement a variety of these methods and those mentioned on the previous slide to successfully infiltrate the target.

Malware

Video: Varieties of Malware by IowaCyber



https://www.youtube.com/watch?v=pFETP9CAJj4

Malware

Malware Triggers:

Triggers are the mechanism that activates the “core” or payload of malware. Examples of triggers include but are not limited to:

- Time
- System configuration settings
- Existence of certain files or folders
- Current software version
- A specific human user action
- Failure to comply with ransomware demands

Malware

Malware Payloads:

A **payload** could be considered malware's purpose. What is it setting out to accomplish? Examples include:

- Destruction of data
- Data encryption
- Spy on the target
- Bring down a website by keeping people from accessing it, through a denial of service attack
- Cause real-world harm, in the case of attacking hospitals
- Install a backdoor
- Zombify your computer

Vulnerabilities

Vulnerabilities

By using some of the propagation methods previously described, hackers can intrude and embed malware through vulnerabilities.

- **Vulnerabilities** are weaknesses within a computer system that compromise systems under attack. They can occur throughout the system's. . .
    - Design
    - Implementation
    - Configuration

Vulnerabilities

- **Design Vulnerability:** flaws in the design of the computer or software that bypass security.
- **Implementation Vulnerability:** errors within implemented software. (installed improperly)
- **Configuration Vulnerability:** user configures the system incorrectly or uses defaults. (not changing default password/using weak passwords)

Vulnerabilities

How to check for vulnerabilities?

Penetration testing (Pen test):

- Simulated cyber attack against a computer system to check for vulnerabilities (test run)
- Provides insight on weak parts of a system that need to be patched up
- Used to ensure that a system is secure and reliable
- Allows for vulnerabilities to be detected and fixed before the system is compromised by attackers

Vulnerabilities

Steps of a pen test (Optional video)

https://youtu.be/b7jW9X9UqiY

Vulnerabilities

- As we learned in the video, passive reconnaissance is the first active step of a pen test.
- **Passive reconnaissance** is the action of acquiring and analyzing as much publicly available information as possible without interacting in any way with the target.
  - This gives the attacker the opportunity to identify potentially vulnerable and misconfigured systems for physical attacks. Additionally, it could potentially provide sensitive information that might allow for impersonation, exploitation, or blackmail.

You will be practicing passive reconnaissance in Activity 1

To Do

- Have Module 7 Activity 1 Completed
- Complete Module 8 Activity 1
- Complete Module 8 Activity 2

End of Module 8!

What questions do you have?

Next Module Topic:

Web Vulnerabilities

Questions?

Contact IT-Adventures support staff!

email:
ita@iastate.edu

Your school's IP-Range can be found at:
http://www.it-adventures.org/ip-ranges/