INTRODUCTION TO NETWORK SECURITY

Nischit Vaidya, CISSP

Instructor

INSTRUCTOR BIOGRAPHY

- Nischit Vaidya, CISSP, Security+
- President/CEO of Argotis, Inc. - Providing Cybersecurity services, solutions, training, and information technology support
- M.Sc in Information Assurance (Capitol College 2012)
- B.Sc in Information Assurance (UMUC 2009)
- 15+ years in the Information Technology Field
- 3+ years teaching information security at colleges throughout Maryland
- Currently supporting Department of Defense as an Information Systems Security Engineer (ISSE)

BEFORE WE BEGIN, LET'S TAKE A POP QUIZ

- What is the biggest threat to a network?

A. Virus

B. Employees

C. Lack of Training

D. Hackers

ANSWER

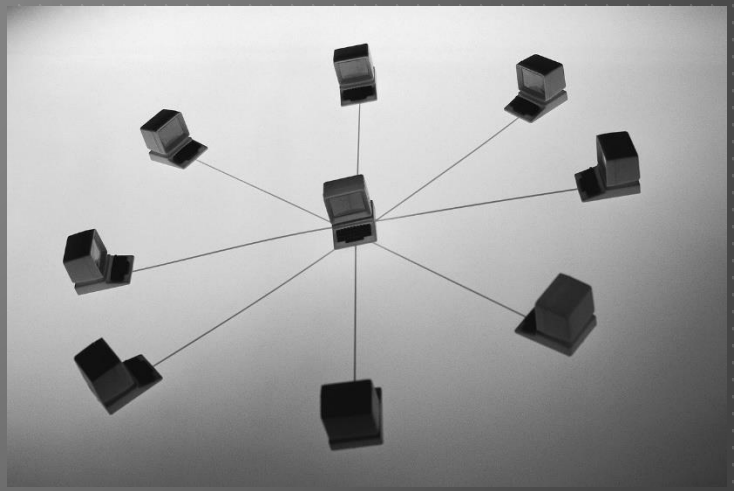
- ***B. Employees***
- Employees are the biggest threat to the network security..
- You may be asking yourself right now, "How is this possible? I'm an employee and I don't consider myself a threat!"
- We will answer this question for you during this lecture, including helping you understand the purpose of network security

LESSON OBJECTIVE

- Define and Discuss Network Security
- Define and Discuss the C.I.A triad
- Define and Discuss Defense-In-Depth
- Define and Discuss Risk, and insider threats
- Lesson Summary

DEFINING A NETWORK

- Before we define network security, we need to understand what a network is
- A network is an internetworking of computers to provide users with information from different locations.
- Internetworking means connecting computers from different locations together
- The Internet is an example of a network



DEFINING NETWORK SECURITY

- Network security is the protecting information that is stored on internetworked computers from threats
- More closely defined, network security is the practice of protecting internetworked computers from unauthorized access, misuse, and denial of service
- Examples of threats include computer virus and hackers

- Network Security involves ensuring the C.I.A of information is protected

DEFINING THE C.I.A TRIAD

- Three letters that all network security professionals live by (also known as tenants:
- C. I. A which stands for:
  - ***Confidentiality*** – Protecting information from unauthorized access and disclosure
  - ***Integrity*** – Maintaining and assuring the accuracy of the information that is accessed
  - ***Availability*** – The information is readily available when authorized users need to access it
- Finding a balance in protecting these three tenants equals a balanced network security process

DEFENSE IN DEPTH

- Defense in depth is what can help a network security professional ensure that the CIA of an information system is protected
- Defense-In-Depth (DiD) means applying a layered approach in providing a strong network security process
- A castle is an example of a Defense-In-Depth strategy
  - Moat, drawbridge, guards, before access into the castle

DEFENSE IN DEPTH

- In the computer world a defense-in-depth process is defined as having layers of security protecting the data
- A very basic structure would be the following:
  - Internet => Router => Firewall => Intrusion Detection System => Anti-virus => Data on the computer
- Firewall, Intrusion Detection System, Routers are all security devices that control the information that comes in and goes out of the network.
- Good DiD implementation would make it much harder for an attacker to penetrate a network

DEFINING RISK

- How would I know to implement a Defense-In-Depth security approach?
- This is accomplished by performing a risk assessment, which is the first step in implementing security
- Risk is defined as an action or activity that can lead to an intended or unintended harm and/or loss
- An information security professional uses a formula to ascertain risk prior to recommending a defense-in-depth solution
  - Risk = Threat (x) Vulnerability
  - Threat = the 'act' that elicit the negative response
  - Vulnerability = the 'weakness' that the threat can compromise or take advantage of
- There is more detail about risk assessments and management we will discuss later in the course

DISCUSSING RISK AND INSIDER THREAT

- We started our lecture with a quiz about employees being the biggest threat to a organization
- Employees have the most access to the organization's data including the inner working of their security structure
- Recall from our Risk slide about what a threat is, and employees pose the biggest threat due to their access
- Employees are known as insider threat

SUMMARY

- Information security involves many facets in order to ensure that our data is protected
- In this lesson we learned about insider threats such as employees, defined risk, learned about defense-in-depth, and learned the basic security principle of the CIA Triad.
- Are there any questions?