Chapter 41- IFPO - CPO

Cybersecurity for Professional Security Officers

Purpose

Professional security officers spend a large amount of time on computers linked to the internet. It is imperative that security personnel are familiar with the threats that are online and to which they could become an unwitting victim.

The Death of Michael Hastings

- Was a reporter for Rolling Stone magazine.
- Was planning an expose on John Brennan, former head of the CIA.
- Was killed in a car crash in Los Angeles on June 18, 2013.
- It is felt that his “connected-car” was hacked, causing him to have no control over the operation of the vehicle.
- Connected cars can be hacked in a number of ways; however, the most common are:
  1. A malicious program allowing the attacker to remotely control the car could be implanted through the OBDII port under the dash of the car.
  2. Through the car stereo: A CD can be programmed to not only play the music listed on its label but also to download a command/control program, allowing the attacker full remote control of the car.
  3. Through the “connected car” function, which allows the user to call for help in an emergency, use real-time GPS maps, update with up-to-the- minute traffic conditions, and which can also allow the manufacturer to remotely install software updates to the car.

Cyberterrorism

- Cyberterrorism is the application of terroristic methods to damage and destroy information technology equipment, and the information it processes for the furtherance of the terrorist organization’s purposes, and in so doing, to damage the target organization’s ability to serve its mission.
- Is focused on targeting employees who spend a lot of time on a workstation. Employees who are most targeted include business managers, and employees who have hours of access to a company’s computer, and little work to do on it.
- All bad outcomes begin with a mouse click.
- Trade secrets are stolen, strategic plans are compromised, important sales proposals are handed over to the competition for a price, military weapon system designs are stolen by foreign powers, money is transferred out of the company bank account using faked authorized credentials, manufacturing processes are damaged—rendering the product output useless, reputations are destroyed, massive amounts of money are lost, and jobs are lost.

Cyberterrorism Methods

- IT systems are most commonly corrupted in one of two ways:
  1. Malware (malicious software
  2. by an Intrusion (a threat actor intentionally making entry into the system).
- One of the most common ways that both of these actions occur is through an innocent user “accidentally inviting” the offending software of the intruder into the system.
- In both cases, a simple URL click (clicking on a link in an email or clicking on a link in a webpage) can initiate the action.
- A “zero-day” attack is an attack method that has never been used before, and so many common protective measures have no defenses for this type of attack. Thus, the attack gets through until it is discovered by the protection company, and they modify their hardware or software to prevent the new attack method.

“Zero-Day” Attack

- In most cases, one of two things happens:

1. If it was a malware infection, the software “phones home” to a command/control server to get instructions. Typically, the instructions are to download ransomware onto the system (more on that in a moment).
2. If it was an intrusion attempt, the URL link will download a little bit of code that allows the intruder to gain access to the system, using the users’ own access permissions. It also alerts the intruder that he/ she now has permission to enter the system.

Ransomware

- One of the most common attacks is a ransomware attack.
- Ransomware is software that does two things to the organization’s entire computer network:
  1. It encrypts all of the organization’s data. The data becomes completely useless files. The attacker uses a key to do this. And the key can unscramble the data, returning it to its original state.
  2. The attacker says that they will give the organization the key for a large amount of money (the ransom).

Crypto-Mining

- Relates to cryptocurrencies, such as Bitcoin.
- Cryptocurrencies require an endless supply of prime numbers to operate on.
- Prime numbers can get very large. And there are computer programs that search for ever-larger prime numbers.
- The process of looking for prime numbers for cryptocurrencies is called crypto-mining.
- And it uses vast amounts of processing power and electricity.

Identifying Bad URL’s

- Cautious people learn how to recognize a bad URL in an email. And they learn how to recognize a bad URL on a website:
  - A misspelled email address: For example, “From: DonaldTrumf@whitehouse.com”
  - A bad URL in a website may look like: www. whitehouse.com (it should be www. whitehouse.gov)
  - A suspicious email that you didn’t expect; from someone you don’t know; asking you to open the important attachment: “Your UPS delivery is coming tomorrow morning. Click on the attachment to see the details.”
- If it’s too good to be true then it probably isn’t true.