Presentation / Discussion Outlines

Employee Training and Security Awareness

Employee training is essential to securing state networks from cyber-attacks. By ensuring employees are aware of criminals' attack strategies and teaching employees how to implement best practices, legislators can strengthen security across the entire system.

Speakers:

- Reginald Tompkins, Director, U.S. Public Sector Markets, Security Systems & Services Sales, IBM Corporation
  James Stanger, PhD, Chief Technology Evangelist - Computing Technology Industry Association (CompTIA

Terms

Reconnaissance
The activity of passively or actively obtaining information about an individual, organization, or department. Passive reconnaissance includes the activity of scanning networks

Denial of Service (DDOS) attack
Any activity designed to make a particular computer, network, or service to stop working (i.e., "crash"). When the computer or network falls victim to a DDOS attack, the services that this computer or network provides are no longer available. An example of a denial of service attack can include sending floods of network traffic to overwhelm a server. Another example of a denial of service attack can involve physically destroying a particular resources, or destroying infrastructure that enables access to that resource.

Distributed Denial of Service (DDOS) attack
The use of multiple computers to generate floods of traffic. As a result, a particular resource from a company or government can no longer provide resources. Sometimes, millions of compromised or unwitting systems can be enlisted to attack a particular computer, network, or company. Such attacks have been responsible for denying vital services for a period of hours, days or weeks. Examples include attacks against stock markets, government and corporate web sites, as well as military first-responder infrastructure.

Social Engineering
The use of deception to manipulate individuals into giving out sensitive information, or into a particular activity that defeats the security of an organization. A traditional "con man" is an example of someone who is a social engineer.

Pretexting
The use of a fabricated scenario that allows an attacker to trick the victim. This scenario often centers around creating a sense of a shared goal, and as a sense of urgency with the victim. This combination is often very powerful. A pretext is where an attacker manipulates a common bond, or goal, shared by the victim. For example, many times attackers are successful in convincing a victim that they need to act quickly in order to deliver a report or sensitive information to a person so that their boss will not get angry. All social engineering involves a convincing pretext.

Baiting
Where an attacker entices an individual with something of value. However, this item (e.g., a USB drive, a piece of software, money) is part of a larger social engineering scheme designed to defeat the security of the individual or organization.

Masquerading
Where an attacker is disguised as a legitimate individual or user. One example of masquerading is vendor impersonation. This is where an attacker obtains the uniforms and even the credentials of a known vendor, and then uses this disguise to enter into a facility. Once inside the facility, the attackers are able to steal information and/or install software and equipment to further infiltrate a target.

Phishing
The activity of sending a communication (usually e-mail) to a group of people with the intent of tricking people into clicking on a link. This e-mail appears to be legitimate. So does the link. However, the link goes to fake resources designed to defeat security. A "phishing" e-mail can use various pretenses, including a fake message from a friend who is in an emergency and needs money, or a message from a person's bank announcing a new security policy where you need to immediately enter a new password. These types of campaigns are common, and generate millions of dollars of revenue for hacker gangs around the world.

Spear phishing
Where the attacker targets a specific individual to trick through social engineering. Often involves sending falsified e-mails to a target. The attacker first profiles the intended victim to obtain personal information about the person's computing habits, as well as general interests. The attacker then creates a carefully-crafted e-mail using information about the person. Such e-mails can be very convincing, and can result in an end user revealing sensitive information, including user names, passwords, and other information, to an attacker.

Whaling
The activity of targeting high-profile end users, such as a company's CEO, a celebrity, or a government official, with the goal of obtaining personal information through social engineering. The goal is to obtain more information about that individual (reconnaissance), or to obtain user names, passwords, and other information with a purpose to defeat organizational security.

Waterhole attack
A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

A variant of this type of attack is where an attacker compromises a popular resource, such as a WiFi hot spot, with code designed to defeat the security measures of all visitors. For example, it is possible to create a rogue WiFi access point that captures all of the traffic of all visitors.

Rogue WiFi Access Point
Whenever you access a wireless (i.e., WiFi) network, you are accessing that network through an Access Point. This is a device designed to announce itself to your computer, and allow connections to additional networks, including the Internet. It is possible for attackers to create an access point that appears to be

legitimate (i.e., the access point at the local Starbucks), but in fact is designed to capture and analyze all traffic passing through it. Hackers can use rogue WiFi access points to capture passwords and sensitive information.

Rogue cell phone towers (interceptors, Stingray)
It is possible to configure radio transmitters to appear as if they were legitimate cell phone towers. Mobile phone users think that they are using their provider's tower (e.g., one created by Verizon or AT&T), but in fact are communicating through a rogue device. As a result, it is possible for attackers to analyze and read all voice and data that passes through the tower.

Shoulder surfing
The activity of looking over someone's shoulder to obtain someone else's user name and password. Can also be accomplished through the use of mirrors and long-distance optics (e.g., binoculars).

Ransomware
Software that is designed to encrypt all computer resources and make them no longer available to legitimate users. The legitimate users are then contacted by the attacker with a message to pay a certain amount of money so that they can get their files back. Many times, users who pay are never given back their information. Gangs and state actors are responsible for extortion schemes that generate well over $2 billion a year. Examples of ransomware include WannaCry, CryptoLocker, and Petya.

Tailgating
A social engineering technique where the attacker simply walks past a security measure by pretending to be part of a larger group, or simply walking in right behind an authorized user. Generally thwarted by allowing only one individual at a time through a security checkpoint, or by active, observant security guards.

War driving / walking
The activity of driving or walking around an area to discover open WiFi networks. This activity is an example of passive reconnaissance, because it involves identifying resources without first connecting to them or scanning them. Using a standard computer or mobile phone, an individual can use readily-available software to identify all WiFi networks in a particular area, with the goal to later actively scan and penetrate those networks to gain information or access sensitive resources (e.g., reports, papers, memos, voicemails).

Resources

- A Look at Employee Cybersecurity Habits in the Workplace: https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace
- Need for cybersecurity professionals: https://certification.comptia.org/it-career-news/post/view/2017/10/04/6-stats-that-prove-the-value-of-cybersecurity-pros
- Trends in cybersecurity: https://www.comptia.org/resources/international-trends-in-cybersecurity. This report includes the following details:
  - By 2021, cybercrimes will cost the worldwide economy up to $6 trillion
  - The majority of attacks involve social engineering / end user compromise

- Human error is playing an even larger role in business security breaches today compared to four years ago – the trend is getting worse
- Most organizations have end user security training, but social engineering remains the primary way intruders enter into systems