Future of Cybersecurity

Section III

SELF PACED | ON-DEMAND | INSTRUCTOR-LED | COLLABARATE | SHARE

Vivaan-lms

A new way of learning

p:972-591-8515 | WWW.VIVAANLMS.COM

Contents

CHAPTER 1: THE FUTURE OF CYBER SECURITY

A NEW KIND OF WARFARE

A newer development in international conflicts is cyberwarfare which is when representatives of one nation hack into another nation's computer networks in order to cause damage or disruption.

One country may launch a cyberattack on another country for a number of reasons such as to spy on each other, or even to break into a secure network and steal important documents or military secrets. It's believed that powerful countries are always spying on each other. A larger threat comes from the possibility of using a cyberattack for the purposes of sabotage. It would be very bad if a foreign country were able to damage the computers that control our country's power or water supplies or our telecommunication or transportation systems.

As cybersecurity grows more common, cybersecurity experts are becoming an increasingly important part of national defense. Within just the first few months of 2016, there were four major cyberattacks on government organizations in the United States. Included in these attacks were NASA, the IRS, and the FBI. Cybersecurity experts have the important job of securing our nation's computer networks today. They also work hard to defend these networks from future cyberattacks.

Cybersecurity experts also study the defenses of the networks used by other countries. Countries such as China, Russia, and North Korea use a network of hackers to launch cyberattacks, which means that having a strong defense may be the only way to truly protect our country's data.

THE FUTURE OF CYBER SECURITY

As we rely more and more on the digital world to store important information, we also have to accept the fact that our data is at risk. Hackers and other cybercriminals may be extremely intelligent. Many are able to respond to new security countermeasures almost as soon as they're in place. They are able to take advance of zero-day vulnerabilities and perform a cyberattack. In fact, it almost seems as though cybercriminals are capable of turning all of our digital devices against us.

The need for intelligent and hardworking people in cybersecurity field will continue to grow. By increasing spending on cybersecurity efforts and making sure cybersecurity becomes something that is taught to children in school, we can make sure that our personal data is as safe and secure as possible.

Sometimes it seems as though hackers and other cybercriminals are unstoppable. However, in reality, they're just intelligent individuals who are devoted to breaking the law. If you are a cybersecurity expert who is equally intelligent and devoted, you will rise to the challenge of stopping them.

No system can be completely secure. Any countermeasure that a cybersecurity expert designs will eventually be cracked. That's why cybersecurity experts must constantly work on building safer systems and writing stronger codes. One of the easiest ways to make sure a system remains secure is to be sure the software is up-to-date. Cybersecurity also relies on ongoing user education. Teaching people how to safely operate computer systems and avoid obvious security risks will make a cybersecurity experts job much easier.

CHAPTER 2: GLOSSARY OF TERMS

Academic: Connected with a school, especially a college or university.

Access: The ability to use or enter something.

Activist: Someone who acts strongly in support of or against an issue.

Air Gap: In cyber security terms, an air gap is a physical separation between the network and critical systems.

Antimalware (anti-malware): A type of software program designed to prevent, detect and remove malicious software, called malware, on IT systems, as well as individual computing devices.

ARPANET: Advanced Research Projects Agency Network (*ARPANET*) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

Assets Identification: A critical process where organizations keep a track of their fixed or movable assets.

Asset Tags: For asset identification, the most common method used is asset tags. Asset tags or asset labels are used to identify physical assets.

Corporate Network: A group of computers and network devices that are connected together in the same area, which are all owned by the same company

Cybersecurity: A branch of computer science that deals with protecting information systems from damage or theft.

Disruption: The act of throwing something into disorder or interrupting it.

Download: To copy data from one computer to another, often over the Internet.

End-to-end encryption (E2EE): A step up from just standard encryption and is a system of communication that ensures that only the communicating users can read the messages and no other third parties can interfere, read, or decipher data or messages being communicated or stored.

Exploitable: Capable of being used for someone's advantage or profit.

Federal Communications Commission (FCC): An independent agency of the United States government created by statute (47 U.S.C. § 151 and 47 U.S.C. § 154) to regulate interstate communications by radio, television, wire, satellite, and cable.

Firewalls: The most common form of network security and can be software or hardware based. Firewalls are used to filter or block data being sent between two or more computer networks.

Hardware: The physical parts of a computer system, such as wires, hard drives, keyboards, and monitors.

IETF (Internet Engineering Task Force): The mission of this team is to make the Internet work better by creating standards for the Internet. This team consists of a large open international community of network designers, vendors, operators, researchers, and engineers that aim to make the dynamically changing environment of the Internet and its entire architecture run as smoothly as possible.

Infect: To transmit or copy a virus from one computer to another.

Internship: A job done in order to gain experience in a career. Internships can be paid and unpaid.

Intrusion detection system (IDS): A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

Leakware or doxware: A less common variant of ransomware where the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. However, this tactic is usually only used a threat as finding and extracting information is tricky for attackers so encryption ransomware is the most common form.

Mobile Device: A mobile device is a general term used for a handheld device/ smartphone/ computer.

Network: A system of computers and databases that are all connected.

Network security: Refers to preventing information access to files and directories in a computer network against hacking, misuse, and unauthorized changes to the system.

People Patching: Similar to updating hardware or operating systems, you need to consistently update employees with the latest security vulnerabilities and train them on how to recognize and avoid them.

Sabotage: Any act or process performed with the intent to damage or harm a business, government, or nation.

Security Vulnerability: A weakness in a product or system that attackers capitalize on and further compromise the system's integrity, confidentiality and availability.

Server: A computer or group of computers used by organizations for storing, processing, and distributing large amounts of data.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Software: Programs that run on computers and perform certain functions.

Tamper: To alter for an improper purpose or in an improper way.