KAMPALA INTERNATIONAL UNIVERSITY

SCHOOL OF MATHEMATICS AND COMPUTING

STUDY GUIDE FOR CERTIFICATE OF COMPUTER SCIENCE

NCIT213 FUNDAMENTALS OF COMPUTER ETHICS

INSTRUCTIONAL DESIGNER:

MS.NAMUGABO LYDIA *(BIT-KIU, MIS –KIU)*

Tel. 0783539607, lydiaphelix@gmail.com

Study unit 3: Forms of computer software attacks

Introduction

This unit introduces students to the forms of computer software attacks, steps to be taken to mitigate cyber threats.

Learning Outcomes of Study Unit 3

Upon completion of this study unit, you should be able to.

1. Explain what we mean by software attacks
2. Explain the different forms of software attacks.
3. Explain the method of mitigating cyber risks.
4. To know the following:

- Viruses
- Worms
- Trojan horses
- Denial of service
- Brute force

Software Attacks

These are programs written deliberately to vandalize someone's computer or to use that computer in an unauthorized way. There are many forms of malicious software; sometimes the media refers to all malicious software as viruses. This is not correct and it's important to understand the distinction between the various types as it has some bearing on how you react to the attack.

Different forms of computer software attacks

1. **Trojan horses**

Trojan horses are classified based on how they breach systems and damage they cause.

The seven main types of Trojan horses are as follows:

i. Remote Access Trojans

ii. Data Sending Trojans

iii. Destructive Trojans

iv. Proxy Trojans

v. FTP Trojans

vi. Security Software Disabler Trojans

vii. DoS Attack Trojans

2. **Worms**

A computer worm is a self-contained program that is able to spread functional copies of itself or its segments to other computer systems. Worms use components of an operating system that are automatic and invisible to the user. The worms are detected only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

3. **Viruses**

Virus is a program or piece of code that is loaded onto a computer without the knowledge of the user and runs against the user's wishes. Viruses can transmit themselves by attaching to a file or email or on a CD or on an external memory.

Viruses are classified into three parts

File infectors – File infector viruses attach themselves to program files, such as .COM or .EXE files. File infector viruses also infects any program for which execution is requested, such as .SYS, .OVL, .PRG, and .MNU files. These viruses loaded when the program is loaded.

System or boot-record infectors – These viruses infect executable code in system areas on a disk. These viruses attach to the DOS boot sector on diskettes or the Master Boot Record on hard disks. The scenario of boot record infectors is when the operating system is running and files on the diskette can be read without triggering the boot disk virus. However, if the diskette is left in the drive, and then the computer is turned off or restarted, then the computer will first search in A drive when it boots. It will then load the diskette with its boot disk virus, loads it, and makes it temporarily impossible to use the hard disk.

Macro viruses – These are the most common viruses, and they do the least damage. Macro viruses infect Microsoft Word application and typically insert unwanted words or phrases.

4. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Have you ever found yourself waiting impatiently for the online release of a product, one that you're eagerly waiting to purchase? You keep refreshing the page, waiting for that moment when the product will go live. Then, as you press F5 for the last time, the page shows an error: "Service Unavailable." The server must be overloaded!

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can't really overload a server with a single other server or a PC anymore. In the past years it hasn't been that common if anything, then by flaws in the protocol.

Spyware

Spyware is a type of malware that is installed on systems and collects small amount of information at a time about the users without their knowledge. Spyware is Internet terminology for advertising supported software such as Adware. All adwares are not spywares. There are also products that display advertising but do not install any tracking mechanism on the system. Spyware programs can collect various types of personal information such as Internet surfing habits and Websites that have been visited. It can also interfere with user's control on the system such as installing additional software and redirecting Web browser activity. Updated antispyware is used to protect spywares from attacking the system.

5. **Brute force**

   Brute force attack consists of an attacker submitting many password or pass phrases with hope of eventually guessing correctly. The attacker checks all passwords and passes phrases until the correct one is found.

STEPS TO MITIGATE CYBER (INTERNET) THREATS/RISKS

i. **Secure buy-in from senior leadership.** This is a must! Balance security budget vs. amount of risk your company executives are willing to assume.

ii. **Continuous employee education,** plus necessity to strengthen policy on PW protection.

iii. **Monitor network traffic for suspicious activity** – can you "see" in & outbound encrypted messages?

iv. **Upgrade and patch software immediately and promptly.** This must be done frequently as patches are released by the software vendor.

v. **Implement robust Endpoint security** to protect your business from zero-day malware & user mistakes.

vi. **Upgrade Authentication inside and out** – including mobility & IoT policies.

vii. **Harden external facing web applications.**

viii. **Know where sensitive data resides,** and then develop data protection strategy to include encryption monitoring.

ix. **Develop and implement** real-time monitoring strategy and analysis of log files and wire data.

Implement rigorous application development testing and code reviews.

x. **Perform annual penetration assessments** and vulnerability assessments.

xi. **Prepare for the worst case scenario.** Develop emergency incident response (IR) plans.

STEPS TO ASSESS AND MITIGATE CYBER SECURITY RISKS

Step #1: Identify and document asset vulnerabilities

Your first step should be a risk assessment to understand what makes your business attractive to cyber criminals (customer data is likely to be your biggest commodity at risk) and where your main vulnerabilities lie.

Start with some basic questions, such as 'what information do we collect?', 'how do we store it?', and 'who has access to it?' You should then examine how you currently protect your data, and how you secure your computers, network, email and other tools.

For example, consider whether you have a formal written policy for social media usage on any device (including employees' personal ones) that connects to your company network. Do you provide internet safety training for your workforce? Do you wipe all old machines of data before disposal? Do you require multi-factor authentication (more than one way of confirming a user's claimed identity) to access your network

Step #2: Identify and document internal and external threats

Do your research and familiarize yourself with the main types of cyber crime and how they're perpetrated – the tactics, techniques and procedures used to target organizations. And don't focus exclusively outwards. While the word 'hacker' may conjure up visions of a malevolent teenager in a bedroom in some remote corner of the world, or a shadowy presence on the Dark Web, you should acknowledge the potential for a disgruntled or heavily indebted employee to steal intellectual property or commit cyber-enabled economic fraud.

Step #3: Assess your vulnerabilities

There are a growing number of tools (many of which are free) that you can use to scan your network and determine what services you are running, to determine whether your software versions are up to date, and to look for known vulnerabilities. There are also tools that will allow your IT administrator to run pre-defined exploits against your own systems and use brute-force attacks against your end users. You may wish to go one step further and appoint an outside security specialist to gauge your company's resilience through penetration testing, in much the same way as vehicle manufacturers use 'tame' burglars to break into cars.

Step #4: Identify potential business impacts and likelihoods

Carry out a business impact analysis to determine the effects or consequences – financial, operational, and reputational – of a cyber attack on your business and who would be affected. If you have a business continuity plan or resilience plan, you should already have a clear picture of the costs linked to IT failures or business interruption. If not, a specialist can guide you through this process, and ready-to-use questionnaires are available to help you collect information from various parts of your business.

Step #5: Identify and prioritize your risk responses

Once you understand the potential impact of a cyber attack on your business, you can start to prioritize how you will resolve any immediate flaws in your security. If you make any changes to your system security, test them to ensure you have not only closed the holes but that the changes haven't negatively impacted any of your other systems. Since people can be your greatest security liability, ensure rules and best practices are documented in policies, and undertake a regular program of staff education on the risks that come from today's interconnected ways of doing business.

Review questions:

1. Discuss the impact of the software attacks leant in the lesson.
2. Explain the methods of mitigating the threats caused by the software attacks.

References and Additional Reading Materials

1. Bynum, T. W., (2000). The Foundation of Computer Ethics. ACM SIGCAS Computers and Society
2. Floridi, L. (1999). Information Ethics: On the Theoretical Foundations of Computer Ethics (PDF). Ethics and Information Technology.
3. Floridi, L. and Sanders, J. W. (2002). "Computer Ethics: Mapping the Foundationalism Debate" (PDF). Ethics and Information Technology.
4. Haag, Stephen; Cummings, Maeve; McCubbrey, Donald J.(2003). Management Information Systems: For the Information Age (4th ed.). New York: McGraw-Hill. ISBN 978-0-07-281947-2.
5. Johnson, D. G. (2001). Computer Ethics. 3rd edn: Upper Saddle River, NJ:Prentice Hall.
6. Martin, C. D. Weltz, E. Y. (June 1999). From awareness to action: Integrating Ethics and Social Responsibility into the Computer Science Curriculum. ACM SIGCAS Computers and Society.
7. MacKinnon, B. (2011). Ethics: Theory and Contemporary Issues. 7th edn. Belmont, CA: Wadsworth.
8. Quinn, M. J. (2011). Ethics for the Information Age. 4th edn. Boston, MA:
9. Addison-Wesley. Moor, J. H. (1985). What is Computer Ethics? In Bynum, Terrell Ward Computers & Ethics. http://rccs.southernct.edu/what-iscomputer-ethics/#what-is-computer-ethics: Blackwell.
10. Mowshowitz, A. (March 1981). On approaches to the study of social issues in computing. Communications of the ACM.
11. Stamatellos, G. (2007). Computer Ethics: A Global Perspective. Jones and Bartlett. Tavani, H. T. (2004). Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology.
12. Hoboken, NJ: JohnWiley and Sons. American Philosophical Association's Newsletter on Philosophy and Computers: