KIZITO SEBUTEMBA EZEKIEL 213012200 13/U/6970/EVE

AINEBYONA DONALD 216013098 16/U/2970/PS

KYOBWEINE BIKANGAGA PRISCA 216002579 16/U/6489/PS

KAHIGIRIZA PETER WARREN 216002577 16/U/5173/PS

February 8, 2018

MAKERERE UNIVERSITY

COLLEGE OF COMPUTING AND INFORMATION TECHNOLOGY

A CONCEPT PAPER ABOUT CYBER SECURITY

RESEARCH METHODOLOGY

BIT 2207

Introduction

Cyber security is defined as a protection technique of information systems. It can also be termed as information security. This is mainly protection from vices like theft, software malpractice, damage of hardware all this adding up to protecting raw data or information itself. This also prevents chaos and misdirection of services offered by say any given ICT based company.

Cyber security involves controlling tangible access on hardware, barring harm or any threats on a given network field as well as raw data or any similar kind of plagiarism. Furthermore, it does not have to be prone to any planned or accidental form of illegal access. All these kinds of uncertainties must undergo a legal frame of security procedures designed as per given type of cyber security.

Looking more into this field, many software systems designed of late amongst the various communities in the world have seen evolution of cyber security grow as it is now an essential priority. Such software systems include Xender, ShareIt and Bluetooth as these are one of those wireless networks that may be susceptible to cybercrime! Others that are
not wireless are smartphones which are a growing trend each new day that rises.

Cyber security is vulnerable to a large number of attacks; some amongst the many can be stated below.

Click jacking

This is a malicious technique through which the attacker tricks (fools) a user into clicking on say a button or rather a link of another webpage without the user necessarily having to click on that particular button intentionally. You realize that these malicious acts are done by use of transparent or opaque interfaces. During this process, the user is tricked into believing that they are entering authentic information such as passwords on a given webpage yet actually when the attacker is channeling this information to a specific invisible frame for personal or malicious gains.

0.0.1 Spoofing

This is another malicious technique in which user?s identity is stolen in the context that another person or program pretends to be the user by use of falsified data.

0.0.2 Eavesdropping

This is an act of illegally tapping a conversation amongst users over a given network without their conscious.

0.0.3 Privilege escalation

This defines a state in which an attacker privileged with a given level of restricted access that without any form of authorization is able to access or elevate the rights in order to access a given system.

0.0.4 Direct access attacks

Here the attacker gains tangible access to a computer. It?s at this point that they are able to compromise security say by downloading data from it, carry out malicious modification of the system such as installing software like worms and Trojans, key loggers, etc. This form of cyber security vulnerability usually surpasses any form of standard security measures in place.

Background
Over the years, the number of many and sophisticated cyber-attacks is steadily increasing. It so happens that this comes at a time where by our dependence on the Internet and other similar networks such as Wi-Fi and Bluetooth is also growing day by day. This is because there?s an enormous demand for both critical services and important information that can only be accessed over these platforms. It is stated by one of the anti-virus companies McAfee that 2011 is when a large number of cyber threats were discovered. It is said that an approximate of about 70 million different pieces of malware are circulated all over the earth. This is as a result of smartphones being the major intermediary through which these malwares are spread.

Furthermore, analysts report that at-least 70 percent of the mails spread around are Spam. Several systems such as e-commerce, e-banking, super intelligent transport networks such as airline and railway systems all are interconnected in one way or the other. You find that failure in the link amongst these different systems will lead to failure of the other. This therefore means that however convenient and efficient these systems may be running, they are vulnerable to cyber-attack and thus the need for cyber security is paramount.

What is around the world is that most of these systems running side by side are not believed to that way around the globe. There might not be a standard cyber protection policy but this would not matter much since some laws at hand harmonize with a legal frame work considered to deal with reference to cyber-attacks. However, this can be easier if the technical solutions put in place can be made stronger by complimenting them with security measures.

This is also evident in the current inter-correlation of networks in the world today.

Problem statement

The measures put in place to tackle the different types of cyber-attacks and cyber-crime is not strong enough to overcome the vulnerabilities incurred as of the present. This is because there is an increasingly noticeable level of cyber-attack techniques that are way more advanced than the security techniques at hand.

Objectives

Main Objectives

To develop a pro-active approach to improving security and managing cyber-attacks.

To issue alerts regarding significant cyber threats, vulnerabilities and any incident.

Specific Objectives.

To enable use of multiple platforms to promptly share information with other users.

To establish a definite and trusted information sharing environment amongst users.

Scope

The description of this project focuses on mainly the ability of any system at hand to be able to deny access of any unauthorized users of a given system software and be able to issue warnings to the credible users in case there is any. It will be mainly for computer related system.

Significance

Information security is very important in society especially in the ICT world. Methods such as verification ensure a secure and configuration of tangibles such laptops, workstation or even smartphones.

Cyber security also puts into measures of checks and balances on whether any given system within an organization having internal security software such as anti-virus or any protection software is functioning correctly.

Helps in assessments of any given current data backup as well as recovery policies in case any major cyber- attacks.

References

http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm
http://www.whitecase.com/publications/insight/cyber-risk- why-cyber-security-important https://www.dhs.gov/topic/cybersecurity
http://www.disaster-resource.com/index.php?option=com$_{c}ontentamp; view = articleamp; id = 1717 : the - importance - of - cyber - security - within - your - organization$