Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Cybercrime: A threat to Network Security

Anusha Raman
Department of Computer Science, St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, India

Abstract **-**This research paper discusses the issue of cybercrime in detail, including the types, methods and effects of cybercrimes on a network. The study explores network security critically reviewing the effect and role of network security in reducing attacks in information systems that are connected to the internet. The efficiency of information security of any kind of security that exists and is used in information systems. Since hackers and other offenders in the virtual world are trying to get the most reliable secret information at minimal cost through viruses and other forms of malicious soft-wares, then the problem of information security - the desire to confuse the attacker: In other words, the Internet is a large computer network, or a chain of computers that are connected together. This connectivity allows individuals to connect to countless other computers to gather and transmit information, messages, and data.

Keywords**:** *Security, Network Security, Computer, Privacy, Cyber Crimes.*

I. INTRODUCTION

The advent of computers and the expansion of the Internet made likely the accomplishment of large improvement in research, surgery, expertise, and communication. Unfortunately, computers and the Internet have furthermore supplied a new natural environment for crime. As Janet Reno, U.S. advocate general throughout the Clinton management, put it, "While the Internet and other data technologies are conveying tremendous advantages to humanity, they furthermore supply new possibilities for lawless individual behavior"

Cybercrime is roughly characterized as committing a misdeed through the use of a computer or the Internet. The Internet has been characterized as "collectively the myriad of computer and telecommunications amenities, encompassing gear and functioning programs, which comprise the interconnected worldwide mesh of systems that provide work the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to broadcast data of all types by cable or radio". The purpose of the study is to determine the impact of cybercrimes on network security and to determine at what level network security is able to reduce cyber-crimes.

II. AIMS AND OBJECTIVES

- To determine the impact of cybercrime on networks.
- To determine the advent of cyber-crime.
- To determine the pros and corn of network security.
- To determine how network security reduces the treat of cyber-crimes.

III. MATERIALS AND METHODS

The measurements of choice for literature were relevancy to research topic and year of publishing. Both public and individual libraries, as well as online libraries, were chaffered to approach the data. Some of online databases that were accessed are SAGE, Questa, emerald, proudest and so on. Data collection establishments, for example, Gallup and AC Nielsen carry on researches on a repeated basis homing in on a wide lay of subjects. A library is an assemblage of services, resources and sources.

It is organized for the functioning of and is maintained by a public body, an organization, or even an individual. In the formal sense, a library is a collection of books. The term can mean the aggregation, the construction that homes such an assemblage, or both. Public and committed accumulations and services of process may be designated for use by individuals who prefer not to or cannot spend to purchase a huge collection, who require significant material that no person can fairly be anticipated to bear, or who demand professional help with his/her probe.

IV. DATA ANALYSIS

Understanding the nature and function of cyber-crimes and network security; the qualitative descriptive mechanism is the most ideal means of collecting and analyzing data due to the flexibility, adaptiveness, and immediacy of the topic. This brings inherent biases, but another characteristic of such research is to identify and monitor these biases, thus including their influence on data collection and analysis rather than trying to eliminate them. Finally, data analysis in an interpretive qualitative research design is an inductive process. Data are richly descriptive and contribute significantly to this research.

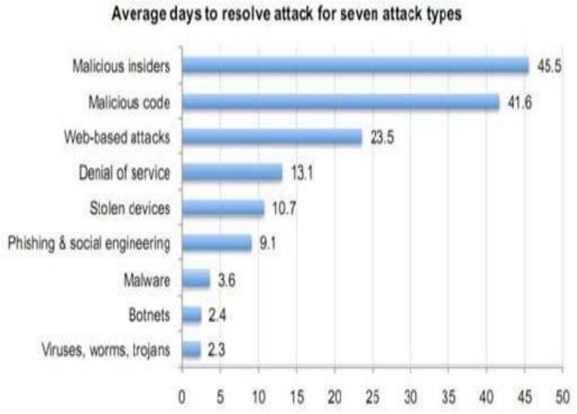
V. CONSIDERATION OF QUALITATIVE RESEARCH

Qualitative research measures consider a universal law in the hope of developing a static reality; on the other hand, qualitative research is an assumption of what the reality is a dynamic exploration. To solve the current problems of the market, it is important for retailers to adopt a more strategic approach to decision making, taking into account the great importance of intellectual property management, it does not say what is found in the process of universality, therefore, promotion and tolerance is often cited as a study of these types.

VI. DISCUSSION AND ANALYSIS

After analyzing the results of the study through qualitative analysis it can be said that computers and the Internet are now a familiar part of our lives. You may not see them often, but they are involved in some way in most of our daily activities in the business, educational institutions, and government. Without the support of any of these tools, we would be able to handle the overwhelming amount of information that seems to characterize our society. But the problem of security limits.

The threats to the network security are not just for organizations, but can be observed all over the world in different countries and the degree to which each of them are exposed to threats. The statistics to which can be seen in the table illustrated below



VII. ATTACKS ON INFORMATION: WHAT ARE THE THREATS?

Not forgetting that the latter are always a combination of tools that have to do with technology and human resources (policies, training). Attacks can serve several purposes including fraud, extortion, data theft, revenge or simply the challenge of penetrating a system. This can be done by internal employees who abuse their access permissions, or by external attackers to remotely access or intercept network traffic.

At this stage of development of the “information society” and computer technology, hackers is no longer new. Some date back to emergence of digital networks, a good few years ago. No doubt as access to electronic communication networks became more widespread, also went by multiplying the number of those entering "illegally" to them, for different purposes. The Pirates of the cyber age considered as a sort of modern Robin Hood and demand a free and unrestricted access to electronic media. Another common attack on a computer system is the creation and distribution of malicious computer code, called “viruses”. Computer viruses are computer programs written specifically to damage other computer systems. Sometimes these malicious programs are contained within another program, known as a “Trojan horse”. The approximate time to resolve some categories of attacks on networks can see in the following table: Tiny It comes configured with a medium security level, suitable for normal Internet browsing. The network works fine without having to set special rules. Facilitates IP registration information. Sygate Firewall Interface comes configured with a high level of security. Win Route Pro It is a proxy server. Its source addresses filtering and destination of both incoming and outgoing. You can select levels of protection and block access to Internet after a certain time. At Guard Allows you to define rules for everything, is fast and gives you a control of what is happening. Blocks unwanted advertising has a log of date, time, URL, IP, bytes sent and received and time of all Web connections. Freedom it is very easy to install, pass ports invisible so you can surf the Internet anonymously.

VIII. RESULT

Computer geniuses, usually in their twenties, are thrown challenges to break one or another security program, capture the passwords to remote computers and use their accounts to travel the cyberspace, enter data networks, airline reservation systems, banking, or any other "cave" more or less dangerous. Managers of all systems have tools to control that "all is well", if the processes are normal or if there is suspicious activity, a user is using to access roads which is not authorized. Furthermore, the network is becoming the ideal place for criminals and terrorists to carry out their actions and activities. Hence, cybercrime and cyber terrorism have become two of the most serious threats seem to haunt Western societies. Moreover, the impact of the crimes on the victims and their measures to cope up with such crimes in the future will also be a part of the paper. This paper will also discuss the how network security is critically important in preventing the recurrence of these types of cyber-attacks in the future.

CONCLUSION

In conclusion, it can be said that attacks on machines connected to the Internet have increased by 260% since 1994, with an estimated loss of 1,290 million dollars annually in the U.S. In the era of information, ideas, data and files on your network are probably more valuable than your entire company. Think about your customer lists and records of shareholders, trading and marketing materials, marketing strategies and product design, the loss of which could mean the significant loss for your firm. With advances in technology, no one is safe from an attack by "hackers. Currently it is relatively easy to gain control of a machine on the Internet that has not been adequately protected. Companies invest a significant portion of their money in protecting their information, since the loss of irreplaceable data is a real threat to their business. The technology boom in the development of networks, digital communications and virtual world whose ultimate expression is the Internet.

References

[1] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

[2] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.

[3] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

[4] Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

[5] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.

[6] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-NetworkSabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.

[7] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012