© 2016 IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Study of Internet and Cyber Crime

Henry Kristian Siburian

Lecturer, STMIK Budidarma, Jl. Sisingamangaraja XII No.338, Siti Rejo I, Medan Kota, Kota Medan, Sumatera Utara

ABSTRACT

Development of network technology, especially Internet technology is now so large that almost any facilities for information requires an internet connection, the more available and easy communication allows the cyber-attacks against the objects connected to the Internet, to minimize cyber-attacks need to be overcome by providing defense in the form of network security, especially in the vital objects such as government agencies, hospitals and banks as well as many other objects also necessary secured, one of the way for protected network were using firewall.

Keyword: Cyber Crime, Cyber Defense, Security, Internet Connection, Cyber Attack

I. INTRODUCTION

Advancement of information and communication technology has changed a lot the way we communicate has changed the face of the world and simultaneously shift the understanding of some power or sovereignty of a country, the strength of a country previously relied on military force but is now beginning to mastery of information technology and communication [1], this is due at the time almost all activities ranging from personal activities until the government cannot be separated from the utilization, empowerment, and implementation of information and communication technologies [1].

The importance of Internet security almost have attention the entire world, especially in the business sector, government, education due to very many transactions processed in seconds, in addition to the sector there are still some people use the internet either adults or children, access to information for children children [2], requires special attention because could have accessed the site is a site that is not in accordance with their age, the ease of the internet has a positive as well as negative effects for some users, and of course we need a form of security in order to minimize the negative effects [2] [3].

To view the security system of the Internet need to know how the system works Internet, among others, is the connection between the computer and the protocol used [4]. Internet is a highway that can be used by everyone (public). To reach the destination server, packets of information to go through multiple systems (routers, gateways, hosts, or other communication devices) that are likely to be out of control. Each point through which has the potential to be cracked, intercepted and forged [3] [4].

Many ways security can be proposed, so an internet connection is used for the better, one of the techniques that can be used is cryptography in exchanging information in the internet [3] and this technique has been used by many companies, especially banks and also national or international level. Modern cryptography involves computers in operation, so has the complexity of the complex. Things that need to be considered in modern cryptography include privacy issues, the data integrity, authentication and non-repudiation [3], in addition to the use of cryptography could also use a special software that can be used as forms of communication security such as Zone Alarm Firewall, BitDefender Firewall and many others.

This article we will discuss the use of internet in the country of Indonesia and how the information security that has been applied in Indonesia as well as how the impact of the use of internet communication security for the community in general.

II. METHODS AND MATERIAL

THEORY

Internet is actually starting from the concept Galatic Network proposed by JCR Licklider of MIT who was the first director of the computer research program DARPA (Defense Advanced Research Project Agency) [5] in his book Series of Memos, in August 1962, which dreams of a global network of interconnected using the computer so that everyone can easily access data and programs from a site. If dived further, the concept is similar to the function of the internet today.

If you mention the word internet, often ordinary people think that the Internet is a web (WWW / World Wide), when in fact the web is part of the internet facility. Here are some facilities provided by the Internet [6], namely:

1. World Wide Web or WWW, the web is the most frequently used services and has developed very fast because with this service user / user can receive information in various formats (multimedia) including text, images, sounds, movies and so on other. To access the WWW service on a computer (called WWW server or web server) used web client program called a web browser. The types of commonly used browsers nowadays are chrome, moziila firefox, opera and safari
2. Electronic Mail, abbreviated e-mail is the transfer or receipt of electronic mail over the internet.
3. Telnet, Facility to connect with other computers and search and retrieve information from the computer proficiency level.
4. File Transfer Protocol, Through FTP software, data or files can be sent from one computer to another. The process of sending a file from another computer to the user's computer is called downloading, while sending the files from the user's computer to another computer is called upload.
5. Social Media
   Social media are computer-mediated technologies that allow the creating and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks.

Internet use cannot be separated from information security (cyber defense) and also of course cyber-attacks, many forms of cyber-attacks that could be analyzed and summarized from many of the attack several such attacks [2]:

1. Advanced persistent threats (APT), denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks are usually done by overloading a system capacity and preventing legitimate users to access and use the targeted system or resources. These attacks are dangerous threats to organizations that rely almost entirely on the Internet's ability to run their activities;
2. Defacement attacks are carried out by replacing a victim's web page with a forged one, where the type of the contents depends on the criminal’s motives (can be either pornography or politics);
3. Malware attacks are malicious programs or codes that can be used to disrupt the normal operation of a computer system. Usually, a malware program is designed to get financial profits or other benefits;
4. Cyber infiltrations can attack a system through the identification of legitimate users and connection parameters such as passwords. These attacks are done by exploiting vulnerabilities that exist in the system. The main methods used to get access to the system are:

   a. Guessing very obvious passwords, such as one’s user name, the name of one’s spouse or child, a date of birth or things which are important and related to someone or his family, so it is easy to guess and find out;
   b. Exploiting unprotected accounts. Users can also make mistakes, by not entering a password or giving their password to others;
   c. Fraud and social engineering. For example, the offender may claim and act as an administrator and ask for the password for some technical reasons;
   d. Listening to data communication traffic. A tapper will listen to unencrypted data transmitted over the network via a communication protocol;

e. Trojan Horse, a specific spy program and a highly dangerous spyware. It can secretly record parameters used to connect to a remote system.
f. Exploiting the authentication system. All users' passwords should be stored on a server. A hacker will access the file that stores all users' encrypted passwords and then open it with tools available on the network;
g. Testing all the possible permutations that can be the key to cracking passwords, if a cracker knows cipher algorithm;
h. Spying. This is done by recording their connection parameters using software, spyware or multimedia devices, such as video cameras and microphones, to capture confidential information, such as passwords to access a protected system;
i.

5. Spamming and Phishing. Spamming is the sending of undesired mass emails to:

   a. Get publicity or for commercial purposes;
   b. Introduce malicious software, such as malware and firmware into a system;
   c. In the worst case scenario, spam may resemble a bomb attack, with the results of overloaded mail servers, full users' mailboxes and it could create a great discomfort in the email management. In the past, spam was only considered as a nuisance, but today, spam is a real threat. It has become a special vector for the spread of viruses, worms, Trojan Horses, spyware, and phishing attempts;

6. Abuse of Communication Protocol. A spoofing attack of Transmission Control Protocol (TCP) relies on the fact that the TCP establishes a logical connection between systems to support the exchange of data. This allows it to get through a firewall and establish a secure connection between two entities, a hacker, and a target. In addition to the above cyber threats, there are other types of cyber attacks. These cyber attacks can be categorized into [2]:

   1. Hardware threats. These threats are caused by the installation of certain equipment that serves to perform certain activities in a system. Therefore, the equipment is a disruption to the network system and other hardware. For example, jamming and network intrusion;
   2. Software threats. These threats are caused by the software of which functions are to steal information, to destruct information/system, to manipulate information (Information Corruption) in a system, and others.
   3. Data/information threats. These threats are caused by the spread of certain data/information for a certain motive. What is done in information warfare is considered propaganda.

Cyber-attacks almost certainly been felt by Internet users in Indonesia, in the country of Indonesia the development of information technology is still far behind compared to neighboring countries such as Singapore and Malaysia, which already apply information technology in everyday life even almost all parts touched by information technology.

Cyber-attack is not minimized in the country of Indonesia; the Indonesian state itself already has a special organisation that regulates the security of the information that is under the ministry of communications and information, namely the Information Security Coordination Team, Directorate of Information Security, and Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) [2].

Organization above is to supervise, control and maintain the security of the Internet in Indonesia, one of the forms of security that has been done in the country of Indonesia is blocking access porn sites with INTERNET SEHAT firewall, while also blocking some sites radicals associated with ISIS or propaganda tribe , race, culture and religion.

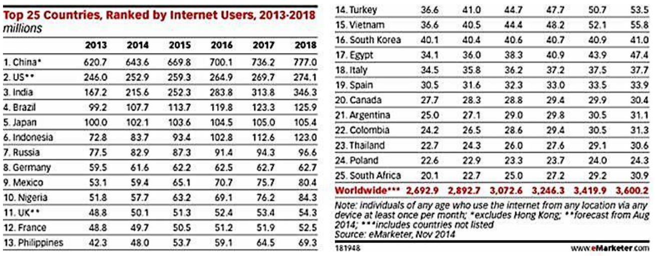
INTERNET SEHAT Firewall is one form of security which is owned by the government of Indonesia to address some of the cyber threats that exist primarily accessing pornographic sites, IP Tracer, Proxy System and others, although the use of firewalls Internet Sehat pretty good but not quite as well due to another attack even more powerful even some government sites are also subject to attack.

III. RESULTS AND DISCUSSION

Research Analysis

Indonesia is a country with a population that is very much even including the world's largest population of the 5 countries, with a population that is very large, the percentage of the number of internet users is also very high, according to market research agency e-Marketer, population netter country reached 83.7 million people in 2014.

The figures apply to anyone who accesses the Internet at least once a month it seated Indonesia ranked the sixth largest in the world in terms of Internet users.



Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide***	2,692.9	2,892.7	3,072.6	3,246.3	3,419.9	3,600.2

*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014

181948 www.eMarketer.com

Figure 1. Ranked Internet User

Source : https://kominfo.go.id

based on the above of course can be seen internet users is quite large, with the number of internet users is quite big, definitely not a few threats or attacks made possible among internet users are commonly called hackers or crackers, attacks that do get exposed to anyone whether personal, company or also the government, one large enough attack occurred there on Election Commission of 2004 where all the party logo was changed to pictures of fruit, this event became the beginning of the next attack better just to demonstrate the ability even as a business competition.

Issue threats and cyber-attacks is not insurmountable, there are some steps that can be done based on the analysis of the author:

1. Availability of a special unit under the ministry of defense cybersecurity Indonesia
2. Special forces working in the ICT field inspection and identification of the network, so that all data packets in and out can be analyzed
3. Data Center Indonesia has and stores all data regarding Indonesian public information, such as ID Card, Bank Account and so on and this information can be used by the authorities for inspection
4. Cyber Warrior formed consisting of hackers who work for state security from hacker attacks originating from inside or from abroad are also attacks that could steal data Indonesian government for the benefit of other countries

IV. CONCLUSION

Security of information in a country is very important especially in countries Indonesia with Internet users No. 6 in the world, monitoring internet usage can not only be done by government alone but also the awareness of users themselves, to cyber threats needs to be made clear regulation of the legal aspects and also the need to set up a special body consisting of cybercrime specialists or experts in the field of internet network.

V. REFERENCES

[1] H. Siburian, "Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia," International Journal of Science and Research (IJSR), vol. 5, no. 11, pp. 511-514, 2016.

[2] M. Rizal and Y. M. Yani, "Cybersecurity Policy and Its Implementation in Indonesia," Journal of ASEAN Studies, vol. 4, no. 1, p. 61078, 2016.

[3] R. Rahim and A. Ikhwan, "Study of Three Pass Protocol on Data Security," International Journal of Science and Research (IJSR), vol. 5, no. 11, pp. 102-104, 2016.

[4] T. Booth and K. Anderson, "Network Security of Internet Services: Eliminate DDoS Reflection Amplification Attacks," Journal of Internet Services and Information Security (JISIS), vol. 5, no. 3, pp. 58-79, 2015.

[5] B. M.Leiner, "Internet Society," Internet Society, Online]. Available: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet. Accessed 20 11 2016].

[6] O. olufunmilola , O. Faith, A. Akindele and A. Alasela, "Assessment of Utilization of Internet Facilities Among Pre-Service Teachers in University of Ilorin, Nigeria," Malaysian Online Journal of Educational Technology, vol. 3, no. 3, 2015.