CYBER-SECURITY AND CRIME

Dr. G. Anitha[1], Mohamed Haris M.Y[2], Muthamil.T[2], EsakkiRaja. E[2]

ABSTRACT

Cyber-Security is suggested for technologies, practices and processes to shield networks, program, devices and data from attacks, damage or illegal access. Another name for Cyber-Security is information technology security. Cyber-Security is more important to keep our information safe, because an unauthorized access can do any redundant activities. It can be government, medial organization or military establishment and the data can be very sensitive. All sources broadcast sensitive data across networks in the itinerary of doing business, and cyber-security is needed to protect the information. Cyber-security includes hardware and software and consists of cyber-security and physical security, both of which are utilized to prevent unauthorized access. The function of cyber-security is to prevent cyber-attacks. It can defend information and it can safeguard against loss or larceny, an attempt to scan computers for spiteful code.

I INTRODUCTION

Cyber-crime is involves computers and networks. Directly or indirectly, it is an offence that is launched against individuals or groups with an illicit motive. By using modem telecommunication, a crime can cause physical or mental harm or loss. It can intimidate an individual or government security and financial health. These crimes include patent infraction, hacking, unwarranted mass investigation and child mentoring. A Cyber-crime falls into two major areas. An outline of attacks against hardware and software from viruses, malware, botnets and network intrusion. Another is financial, fraud and phishing. Cyber-security is predominantly concerned with information security. It focuses on protecting computer systems from malware and unauthorized access. Before being damaged it looks to guard all the systems by means of hard

II Keywords

Antimalware

It protects software and eliminates malicious programs on computing devices.

Botnets

On behalf of owners unauthorized access is configured to forward transmissions such as spam to devices.

Antivirus

Antivirus also referred as antimalware protects devices and detects virus from unknown access.

Phishing

In digital environment an attempt is made to get others' information like usernames, passwords and financial details proposed by masquerading as genuine or incognito.

[1] *Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education Coimbatore*

[2] *Students of MCA , Karpagam Academy of Higher Education, Coimbatore*

III Impact of cyber-crime

Crime against people provides frequent fake promotions and gives them a false delusion of protection to make them to manage their private information. It includes child pornography, a primary offence. The illegal access permits the illegal user to access or steal the private information of other users' computer systems. Usually, the system or machine of any organization is hacked by them. And also, sensitive, confidential and private data of system or server are stolen. Cyber-crime against governments is considered terrorism, and stealing of protected and secret records of the government and those of individual jeopardizes the trust of citizens.

IV Types of Hackers

There are several types of hackers around the internet world, and White, Black, Grey refer to the relationship between the hackers.

A. Black hat Hackers

The unauthorized entry of individual and group for malicious reasons like stealing others' information and access passwords without users' knowledge. They try to exact spoil by compromising sanctuary systems.

B. White hat Hackers

They are functioning organization to strengthen the defense system. They follow rules and regulation to engage the targets to secure organizational information; they individually specialize in right hack tools technique and method.

C. Grey hat Hackers

They are what black hats do. They identify system vulnerabilities of individuals or organizations and exploit them for personal gain.

D. Red hat Hackers

They are the vigilantes of hacker world. They damage the targeted computer systems by uploading viruses destroy them from inside out.

E. Blue hat Hackers

It is a script depicting kids taking revenge to get a blue hat. Blue hat hackers will seek vengeance on those who are angry against individuals or a group of computing systems. They have no desire to learn.

V Common Hacking tools

They implement a wide variety of technologies such as Root kits, Key loggers, vulnerability scanner, SQL injection attack and distributed denial of services.

VI Why cyber-security is needed

The digital technological advancements have opened up new ways of cyber-security. But antagonist also advancements as well the subset of cyber-security requires. Important data are protected by cyber-security. The main function of cyber-security is to secure computer systems against attacks. Cyber-security professionals have to deal with challenges such as kill shackles, nil day attack, and ransom ware, alert weakness and budgetary constraints. To control the threat governments and businesses must collaborate globally to fight against fast-spreading cyber-crime. The internet is fundamentally used for advancement of lifestyle, to make people aware of world-wide activities, to make users technically expert and strong. When a greater number of people use the internet, the crime is also increasing frequently. Most of the criminals are technical experts and have remarkable knowledge about hacking. There are some rules and regulation to control these crimes, generally known as cyber law.

VII CONCLUSION

The victims of Cyber-crime are perennially in danger in the computer world, and they need not sit all times at the computer to watch what is happening. The hackers have everything they need on their lap. They attack with mouse, cursors and passwords. Cyber-crime is an illegal act or a hazard that needs to be tackled constantly. It is a strong advice to take some defense while using the internet. Security has become a major problem. Computer is nothing without computer security.

REFERENCES

1. Anderson, R., Barton, C., Böhme, R., et al. (2012) Measuring the cost of cybercrime. Workshop on the Economics of Information Security, Berlin, June 2012
2. Brenner, S. (2007) “At light speed”: Attribution and response to cybercrime/terrorism/warfare. The Journal of Criminal Law & Criminology 97(2), 379– 475.
3. Commission of the European Communities (2007) Towards a General Policy on the Fight Against Cyber-crime. COM(2007) 267 final. Brussels: Commission of the European Communities. accessed January 21, 2013.
4. Congressional Research Service (2012) Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.
5. Hinnen, T. (2004) The cyber-front in the war on terrorism: Curbing terrorist use of the Internet. The Columbia Science and Technology Law Review 5(5), 1– 42.
6. Hutchings, A., & Lindley, J. (2012) Australasian Consumer Fraud Taskforce: Results of the 2010 and 2011 Online Consumer Fraud Surveys. Canberra: Australian Institute of Criminology. January 22,2013.
7. Kellerman, T. (2010) Building a foundation for global cybercrime law enforcement. Computer Fraud & Security 2010 (5), 5– 8.
8. Kerr, O. (2003) Cybercrime's scope: Interpreting “access” and “authorization” in computer misuse statutes. New York University Law Review 78(5), 1596– 1668.
9. Kshetri, N. (2009) Positive externality, increasing returns, and the rise in cybercrime. Communications of the ACM 52(12), 141– 144.
10. Peretti, K. (2008) Data breaches: What the underground world of “carding” reveals. Santa Clara Computer and High Technology Journal 25(2), 375– 414.
11. Symantec Corporation (2012) 2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually. September 5, 2012. Symantec. January 21, 2013.
12. Treasury Inspector General for Tax Administration (TIGTA) (2012) There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft. Washington, January 21, 2013.
13. World Bank (2012) Internet users. http://data.worldbank.org/indicator/IT.NET.USER/countries, accessed January 21, 2013.
14. G. Anitha (2014), Intrusion prevention and Message Authentication Protocol (IMAP) using Region Based Certificate Revocation List Method in Vehicular Ad hoc Networks, International Journal of Engineering and Technology,6(2)