International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 835-840

http://www. irphouse.com

Inside of Cyber Crimes and Information Security: Threats and Solutions

[1]Sunakshi Maghu*, [2]Siddharth Sehra and [3]Avdesh Bhardawaj

[1, 2]Department of EECE, ITM University, Sector 23 (A), Gurgaon, Haryana, India
[3]Department of Applied Sciences, ITM University, Sector 23 (A),
Gurgaon, Haryana, India,

ABSTRACT

With the rapid technological developments, our life is becoming more digitalized. Be it business, education, shopping or banking transactions everything is on the cyber space. There are some threats posed by this incredible rise in digitization which is creating a new set of global concern called as cyber crime. It is easy to fall prey to such unethical way of hacking and penetrating into personal life which is feasible at a click of a button. Cyber crimes thereby take place in many forms like illegal access and theft of data, intrusion into devices and fraud which is a big concern amongst all the users. This paper identifies the importance of being acquainted with the effects of cyber crime keeping in mind the recent activities that have taken place and offering solutions to protect oneself from it. Moreover, highlighting the need of being cyber safe and how such illegal activities can be a problem for us. The present paper reviews the current solutions to deal with the alarming rise in these criminal activities. Hi-tech technologies that need to be adopted to prevent oneself from getting webbed have been recommended in the paper. A few case studies have been discussed and innovative suggestions for future cyber security proposed.

Keywords: Cyber Crime, Information Security, Cyber threats, Hacking, Phishing, Cyber Safety, Digital Data

1 INTRODUCTION

Cyber Crimes relates to the word cyber which encompasses the computer network, using which one can perform any activity in the real time world. Cyber Crimes such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy use digital data from Computer systems and other electronic devices. [1]These devices are used as a target by attacking the computer through viruses, as a weapon to commit crimes or as an accessory to store illegal information. Cyber Crimes also affect business every year, losing billions of money and damaging the company's reputations leading to loss of future business as well. In today's world, cyber systems provide flexibility leading to its illicit use. With the Government framed Internet policy, Internet along with making the life easy with economic activities like buying, selling, online transactions and social networking brings along many threats. Hacking tools are available on the internet which does not require people to be highly skilled and also encourage them to do inappropriate acts online. Thus, cyber space has made users vulnerable making it important to take necessary steps and avoid exposure from to acts. Highly populated countries like Asia, China are dependant on web resources which creates opportunity to commit such crimes and also makes it difficult to detect and prevent Internet Crimes in the wide networking environment. [2]

2. DISCUSSIONS

2.1) There are a lot of cases of Computer Assisted crime where computer is the instrument for committing crime. Some of them are discussed below:

2.1.1) Data Piracy: This involves reproduction of digital data and easy distribution of print, graphics, sound and multimedia combinations even the use of copyrighted material either for personal use.

2.1.2) Pornography/Child pornography: It is the unethical and illegal distribution of sexually implicit material especially involving children.

2.1.3) Illegal Interception of Material: Data transfer over the net has resulted in greater speed and capacity but also greater vulnerability. It is now easier for unauthorized people to gain access to sensitive information. It has many forms like:

2.1.3.1) Internet time thefts: Phishing, spoofing or spam (unsolicited mail) wherein a perpetrator sends fictitious mails which appears official causing the victim to release personal information. [3]

2.1.3.2) Online Credit card fraud, E- Bank theft: Illegal acquisition of credit card number for online purchases or bank account details where the perpetrator diverts funds to account accessible to criminal.

2.2) There are other situations of Computer Oriented Cyber Crime where Computer is the target of crime like:

***2.2.1) Hacking*:** Information theft from computer storage device or hard disk and stealing username, password and altering information is called hacking.

2.2.2) Forgery: It includes reproduction of documents, certificates, identity thefts and fake currency.

2.2.3) Altering Websites: Here the hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

2.2.4) Cyber terrorism: It involves E-murder or homicide or suicide or Spyware. [4]

3 CAUSES OF CYBER CRIMES

3.1) ***Ease of access:*** The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of violating the technology by stealing access codes, recorders, pins, retina imagers etc. that can be used to fool biometric systems and bypass firewalls to get past many a security system.

3.2) Cyber Hoaxes: Cyber Crimes can be committed just to cause threats or damage one's reputation. This is the most dangerous of all causes. The involved believe in fighting their cause and want their goal to be achieved. They are called cyber-terrorists. [5]

3.3) ***Negligence*****:** There are possibilities of not paying attention in protecting the system. This negligence gives the criminals control to damage the computer.

3.4) Revenge or Motivation: The greed to master the complex system with a desire to inflict loss to the victim. This includes youngsters or those who are driven by lust to make quick money and they tamper with data like e-commerce, e-banking or fraud in transactions.

3.5) ***Poor law Enforcing Bodies*****:** Due to lack in cyber laws of many countries, many criminals get away without being punished.

3.6) ***Cyber Crimes committed for publicity or recognition*****:** Generally committed by youngsters where they just want to be noticed without hurting someone's sentiments. [6]

4 CYBER CRIME INVESTIGATIONS

Research has shown that no law can be fully brought into function to eradicate cyber crimes. The year 2012 experienced 61 % increase in cyber crimes totalling to 2, 876 with Maharashtra recording the most number of cases. A total of 176, 276, 356, 422 and 601 cases were registered under cyber crime related sections of the Indian Penal Code (IPC) during 2008, 2009, 2010, 2011 and 2012. The past year illustrated how quickly the threat landscape continues to evolve, with risk to organisations continues to be amplified and it's now expanding across diverse mobile platforms. The Websense Security Lab reinforced that traditional security measures are no longer effective in eradicating cyber attacks. The security providers need to evolve towards more practical defences. Here some Case studies have been included to elaborate on the threats and methods of defending against cyber attacks:

Case 1: Phishing Case Study

One Doctor from Gujarat had registered a crime stating that some persons (“perpetrators”) have perpetrated certain acts through misleading emails ostensibly emanating from ICICI Bank’s email ID. Such acts have been perpetrated with intent to defraud the Customers. The investigation was carried out with the help of the mail received by the customer, bank account IP details & domain IP information, the place of offence at was searched for evidence.

Case 2: On line credit Cheating and Forgery Scam

In one of the noted cases of 2003, Amit Tiwari, a 21yr old engineering student had many names, bank accounts and clients with an ingenious plan to defraud a Mumbai based credit card processing company, CC Avenue of nearly Rs. 900, 000.

Case 3: Financial Crimes

Wipro Spectramind lost the telemarketing contract from Capital one due to an organized crime. The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario.

5 DEFENDING AGAINST CYBER CRIMES

5.1 As noted from the above three cases, predefined safety from cyber crimes to safeguard the network of agencies are important. The cyber criminals detect security holes which career criminals or even cyber-terrorist could use to attack them in future. Safeguarding and monitoring wireless access points, network access points, and network-attached devices by securing interfaces between agency-controlled and non-agency controlled or public networks, Standardizing authentication mechanisms in place for both users and equipment, Controlling users’ access to information resources.

5.2 To prevent insider attacks on agency networks access rights to files should be controlled and access should be granted only on as required for the performance of job duties. [7]

5.3 Networks that serve different agencies or departments should be segregated, and access to those segmented networks should be established as appropriate through the use of VLANs, routers, firewalls, etc.

5.4 Access badges should l be programmed to allow entry only into assigned places of duty like after the Wipro Spectramind case, thorough security check of employees takes place and Mobile phone use is prohibited and technology is used to monitor data records.

5.5 Users' activities on systems should be monitored.

5.6 To prevent unauthorized access of information all hosts that are potential targets of DoS(Denial of Service) should be secured.

5.7 Authentic programs should be installed with Trojan scan Programs.

5.8 To prevent against exploitation:

- Periodic scanning for spyware, adware and bots (software robots) shall be conducted with anti-spyware programs that detect these malicious programs.
- Denial of all inbound traffic by default through the perimeter defence.
- Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate agency approval

5.9 **Virus Protection:** To minimize virus hoax Virus detection programs and practices shall be implemented throughout agencies All agencies shall be responsible for ensuring that they have current software on their network to prevent the introduction or propagation of computer viruses by using of antivirus software, performing frequent backups on data files, using write-protected program media, such as diskettes or CDROMs, validating the source of software before installing it all CDs or other media brought from home or any other outside.

6 CONCLUSIONS

It has been deducted from this present study that with increasing rate of cyber crimes more detection techniques along with educating the users on being safe online needs to be established with complete guidance to know about the pros and cons of the web before entering it. There is no doubt that the Internet offers criminals several opportunities. Information is the best form of protection. Concrete measures must be found in order to track electronics evidence and preserve them so that systems are better protected from cyber intrusions. Besides, new cyber laws and policies must be developed by to tackle the various families of cyber crime. Even the companies need to take appropriate measures to investigate and prevent their data.

7 REFERENCES

[1] Dacey, Raymond & Gallant, Kenneth S. (1997) "Crime control and harassment of the innocent, " Journal of Criminal Justice, Elsevier, vol. 25(4), pages 325-334.

[2] H. Choi, H. Lee, H. Lee, and H. Kim (2007) "Botnet Detection by Monitoring Group Activities in DNS Traffic, " in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007) pp.715-720.

[3] Kshetri, Nir (2005) "Pattern of global cyber war and crime: A conceptual framework, " Journal of International Management, Elsevier, vol. 11(4), pages 541-562

[4] Kshetri, Nir (2005) "Information and communications technologies, strategic asymmetry and national security, " Journal of International Management, Elsevier, vol. 11(4), pages 563-580, December.

[5] Michael Massourakis & Farahmand Rezvani & Tadashi Yamada (1984) "Occupation, Race, Unemployment and Crime In a Dynamic System, " NBER Working Papers 1256, National Bureau of Economic Research, Inc.

[6] Panu Poutvaara & Mikael Priks (2005) "Violent Groups and Police Tactics: Should Tear Gas Make Crime Preventers Cry?, " CESifo Working Paper Series 1639, CESifo Group Munich.

[7] Ying-Chieh Chen, Patrick S. Chen, Jing-Jang Hwang, Larry Korba, Ronggong Song, George Yee, (2005) "An analysis of online gaming crime characteristics", Internet Research, Vol. 15 Iss: 3, pp.246 - 261