International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 4 Issue 8, August 2015

A Survey on Cybercrime - A Threat to Individual, Government

Manikeshwar.S.B, A.V. Krishna Mohan

Abstract— **In the present day world, India has come across innumerable Cybercrimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking. Even though the organizations and individuals have taken technological measures and being adopted, we have witnessed that the frequency of cybercrimes has increased over the last decade.**

The users of computer system and internet are increasing worldwide in large number day by day, where it is very easy to access any information easily within a few seconds by using internet which is the medium for huge information around the world. Hence precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime. In this paper, I have discussed various categories of cybercrime and cybercrime as a threat to Individual, and Government and Different types of Cybercrimes. In this paper, I have suggested few preventive measures to be taken to minimize the cybercrime.

Index Terms—**Cybercrime, Cyber stalking, Prevention of cybercrime.**

I. INTRODUCTION

Cybercrimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

Cybercrime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime could also include non-monetary offenses, such as creating and distributing small or large programs written by programmers called viruses.

Viruses are that they are self-replicating computer programs which install themselves without user consent. Viruses often perform some type of harmful activity on infected hosts, such as stealing hard-disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless.

II. HISTORY

The first recorded cybercrime took place in the year 1820. In 1820, Joseph-Marie Jacquard; a textile manufacturer in France produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened.

1. The crimes in which the computer is the target. Examples of such crimes are hacking, virus attacks,
DOS attack.
2. The crimes in which the computer is used as a weapon. These types of crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc. Cybercrimes are broadly categorized into three categories, namely crime against

- Individual
- Property
- Government

But here am considering only two issues here, i.e.

- Individual
- Government

Individual: This type of cybercrime can be in the form of cyber stalking, distributing pornography, trafficking and grooming.

Cybercrime done against person includes harassment by sending emails, cyber stalking, cyber bullying, child soliciting and abuse, and sharing, trafficking, posting of obscene material. Such cybercrime influence younger generation psychology in an awful manner and threaten them with weakening their growth. Cybercrime breaks user

privacy and leave irreparable scars on users if not controlled.

Cyber stalking: It is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel.

Cyber bullying: It is the use of social networks to repeatedly harm or harass other people in a deliberate manner. Cyber bullying includes, Posting mean things about someone on a website, making fun of someone in an online chat, Doing mean things to someone's character in an online world.

Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda.

The perpetrators can be terrorist outfits or unfriendly governments of other nations. Cybercrime against the government is just as much a threat as in the private sector. So much so, that there are a wide range of federal agencies that deals with the issue, including the FBI, Treasury Department, Department of Homeland Security and State Department. The government is susceptible to computer hackers trying to access sensitive government records, financial fraud, and cyber terrorism, to name only a few. All levels of government are at risk.

One type of cybercrime that targets the government in particular is cyber terrorism. It's a powerful platform for terrorist activity since it can be done in relative anonymity across the entire planet. Cyber terrorism shares similar traits to other cybercrimes. However, it tends to focus on disrupting computer systems and/or intimidating or coercing individuals in order to further a political or religious ideology. More than ever in history, our society is significantly dependent upon computers. Our financial system, aviation system, and all of our sensitive national security information contained on government computers are potential targets of cyber terrorism.

One of the more frightening parts of the potential of cyber terrorism is the mere suggestion of it, which creates anxiety and fear. In 1998, there were reports of a mere 12-year-old computer hacker who gained access to the computers that controlled the Theodore Roosevelt Dam in Arizona. An article in the Washington Post reported that if the child was successful in opening the gates, it could have flooded the cities of Tempe and Mesa, with populations that total about one million people.

III. DIFFERENT KINDS OF CYBER CRIMES

The different kinds of cybercrimes are:

1. Unauthorized Access and Hacking

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network.

Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking.

2. Web Hijacking:

Web hijacking is method, it means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Denial of service Attack:

This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic.

Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

Salami Attacks:

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer.

No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

5. Internet time theft:

Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

6. Data diddling:

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

7. Cyber Terrorism:

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control,

telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems.
Cyber terrorism is an attractive option for modern terrorists for several reasons.

a. It is cheaper than traditional terrorist methods.
b. Cyber terrorism is more anonymous than traditional terrorist methods.
c. The variety and number of targets are enormous.
d. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
e. Cyber terrorism has the potential to affect directly a larger number of people.

IV. PREVENTIVE MEASURES TO MINIMIZE THE CYBER CRIME

- Avoid online banking, shopping, entering credit card details, etc if the network is not properly secured.
- Check your online account frequently and make sure all listed transactions are valid.
- Be extremely wary of e-mails asking for confidential information.
- Never ever click on a link given in a spam e-mail.
- Always delete spam e-mails immediately and empty the trash box to prevent clicking on the same link accidentally.
- Beware of lotteries that charge a fee prior to delivery of your prize.
- While using a credit card for making payments online, check if the website is secure as the CVV will also be required for the payment.
- Notify your bank/credit card issuer if you do not receive the monthly credit card statement on time. If a credit card is misplaced or lost, get it cancelled immediately.
- Do not respond to lottery messages or call on the numbers provided in the text messages.
- Do not provide photocopies of both sides of the credit card to anyone. The card verification value (CVV), which is required for online transactions, is printed on the reverse. Anyone can use the card for online purchases if they get that information.
- Do not click on links in e-mails seeking details of your account, they could be phishing e-mails from fraudsters.
- Do not give any information to people seeking credit card details over the phone.

V. CONCLUSION

Every data is important, so the data should be secured for the longer time without losing it or hacked by someone. Necessary care and precautions need to be taken by incorporating the encryption and decryptions methods and techniques until the data is on the network or internet. Provide security to every data and using up of Firewalls plays vital role in securing the data. With the advent of hand held computing, cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers (PCs). Cyber attackers have now taken advantage of the increasing popularity of mobile phone applications and games by embedding malware into them. Despite the increasing cyber threat risks, many boards fail to ask these questions or attain satisfactory answers.

Often, this happens because the first question can be the most difficult to answer. Cyber threats can be hard to quantify in terms of likelihood and business impact. As a result, many boards do not fully understand the nature of the threat and tend to inaccurately assume that cyber security is a technical issue. As the old adage goes 'prevention is better than cure' most organizations could gain improved value and security by adopting a preventive approach to tackling cybercrime related risks.

Adopting a preventive approach towards cybercrime risk management, however, typically requires a cultural shift that starts with board level executives who can incorporate cybercrime related risks into the enterprise risk strategy. By doing so, leaders can quickly start to identify gaps in the current cybercrime risk management strategy and encourage an organization-wide approach to countering cyber threats. Further, many organizations adopt a piecemeal approach towards cybercrime risk management.

ACKNOWLEDGMENT

I would like to thank Prof.A.V. Krishna Mohan, Asst. Professor, Dept. of CSE, Siddaganga Institute of Technology, Tumakuru for guiding and providing valuable suggestions to complete this paper.

REFERENCES

1. *Cyber Crime – A Growing Challenge for Governments, July 2011. Available: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf*

2. *Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.*

3. *Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available: http://www.microsoft.com/security/sir/.*

4. *https://en.wikipedia.org/cybercrime.*

5. *The Growing Threats of Cyber crime, Available: http://www.the41st.com/sites/default/files/41st-Parameter-Cyber-Crime-Whitepaper.pdf*

Manikeshwar.S.B

M.Tech student Department of Computer Science from Siddaganga Institute of Technology, Tumakuru

B.E from East Point College of Engineering and Technology, Bengaluru

A.V.Krishna Mohan

M.E. from BMSCE, Bangalore, Bangalore University.

B.E. from SJMIT, Chitradurga, Kuvempu University.

Digambar ,"An Approach to time synchronization using flooding method in Wireless Sensor Network", International Conference on Electrical, Electronics and Computer Science (ICEECS) held at Bangalore on 4th May 2014

A.V.Krishna Mohan, Prabhu Prasad B M "Reducing the Alarm Broadcasting Delay in Wireless Sensor Network" International Conference on Computer Science and Information Technology(CSIT_2013) held at
Goa, May 2013

Presented a Paper in the 10 th ISTE State Level Annual Convention and two day National Seminar on " Role of technical education in making India an Economic super power by 2020" during 23rd and 24th - November -2007 at Acharya Institute Of Technology , Bangalore

Presented a Paper in the 10th ISTE State Level Annual Convention and two day National Seminar on " Role of technical education in making India an Economic super power by 2020" during 23rd and 24th -November -2007 at Acharya Institute Of Technology , Bangalore

Life Member for Indian Society for Technical Education (LMISTE), LM -26414 dated 03-04-1998 Life Member for Computer Society of India (LMCSI), LM-00169714 dated 01-02-2008

