Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.586 – 590

RESEARCH ARTICLE

CYBER SECURITY -Trends and Challenges

Vidhya P.M
Sree Narayana Gurukulam College of Engineering
Kadayiruppu P.O, Kolenchery
Ernakulam dist., Kerala. Pin 682311
vidhya.mohanan@gmail.com

Abstract: Cybersecurity is a necessary consideration for information technology as well as Internet services. We need to recognize the importance of different types of risks that exist in the online world Enhancing cyber security and protecting critical information are essential to nation's security and economic being. Whenever we think about the cyber security we think of 'cyber-crime' which is increasing day by day. Various Governments and companies are taking many measures to prevent the cyber-crime. This paper mainly focuses on trends, challenges and cyber ethics in the field of cyber security. Cyber incidents emphasize the importance of staying up-to-date on global cybercrime trends, especially concerning the use of mobile and personal computing devices.

Keywords: cyber security, cyber-crime, cyber ethics, social media, cloud computing

I. INTRODUCTION

Technology evolved through different ages. Internet has enabled human beings to send and receive any form of data at a faster rate. But how securely the data is being transmitted to the other person without any leakage of information is a question. Today Internet is one of the fastest growing infra-structure. In today's technical environment many latest technologies are changing the face of the mankind. When looking ahead one thing is clear: technologies will not look like they look, today. But due to these emerging technologies we are unable to safeguard our private information in a very effective way. Despite technological measures adopted by organizations and individuals, cyber-crimes are increasing day by day. Most of the commercial transactions are done online now a days, so this field requires a high quality of security. Hence cyber security has become an important issue.

To ensure that the society continues to enjoy the benefits of information technology, the Vulnerabilities, threats and risks have to be managed through the cybersecurity. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer has become integral to the development of new services as well as governmental policy. A comprehensive and a safer approach have to be incorporated to fight against cyber-crime. The technical measures alone are not sufficient to prevent any crime, we need to have enforce law to investigate and prosecute cyber- crime. Today many nations and governments are imposing strict laws on cyber securities.

II. CYBER CRIME

Cyber-crime refers to the act of performing a criminal act using computer or the Internet network, as the communication vehicle. The U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence. All types of cyber-crimes involve both the computer and the person behind it as victims. Cyber-crime could include anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. As day by day technology is playing in major role in a person's life, the cyber-crimes is also increasing along with the technological advances.

III. CYBER SECURITY

We are living in a world where the information is maintained in as 0's and 1's. Privacy and security of data is a primary concern of most of the organizations. Social networking sites provide a space where users feel safe as they interact with friends and family. The capability to detect, investigate, analyze, and to respond to cyber threats and attacks is an indispensable component of cybersecurity

IV. TRENDS IN CYBER SECURITY

Information technologies have revolutionized the functioning of economies, societies, and governments around the globe. Some of the technological trends in cyber security are explained below.

A. Mobile Technology

Mobile technology penetrates the global market, with the number of mobile devices expected to exceed the number of people on earth by the end of 2016. Already there are nearly six billion mobile subscriptions. Mobile technology, by itself, poses a tremendous cybersecurity challenge. Smartphones equipped with internal cameras, and internet may be "the ultimate spy tool "enabling hackers to listen to calls made on the device, monitor messages to and from the mobile, and to track the location of the device. Hackers could use a hacked phone "as a hidden camera, secretly record video, to eavesdrop or make audio recordings, and track your movements via GPS location."

B. Web servers

Web servers are one of the best platforms for the cyber criminals to steal the data. The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their virus through the terminals that they have hacked. But data-stealing attacks, many of which get the attention of media, are also a big threat. We must use a safe browser in order not to fall as a victim of cyber crime

C. Cloud computing

Cloud computing means that your data is stored on somebody else's computer. The world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. The number of applications available in the cloud is growing, policy controls for cloud services also need to evolve in order to prevent the threat posed by cyber criminals. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns.

D. Advanced Persistent Threat

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. An APT attacker often uses spear fishing to access the network through legitimate means. Once access has been achieved, the attacker establishes a back door. As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. We must improve our security techniques to prevent these threats.

V. SOCIAL NETWROKING AND CYBER SECURITY

The rise of social networking also brings new cybersecurity challenges. Hackers have long relied on "social engineering", convincing people to disclose information that they should not to gain the trust of targets and compromise their networks. As we become more social through these social networks, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and contribute to cyber threats.

As corporate security improves, adversaries increasingly rely on "social engineering" to gain the trust of targets, to convince people to disclose information that they should not, and subsequently to compromise target networks. Nearly forty percent of records compromised through cyber data breaches were compromised as a result of incidents employing social tactics. Moreover, industry data suggest that spear-phishing is at the heart of most targeted attacks. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. Though social media can be used for cyber-crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

VI. SOME PROFESSIONS GIVING BIRTH TO CYBER CRIMES

IT Professionals

Since Cyber Crime is all about computers and Networks (Internet), many types of IT & Technology professionals are quite prominently active in the same, which include but are not restricted to:

- Network Engineers
- Cyber Security Software Professionals
- Cyber Forensic Experts
- IT Governance Professionals
- Certified Internet Security Auditors
- Ethical Hackers

Cyber Law Experts

Cyber Law has become a multidisciplinary approach and hence specialization in handling cyber-crimes is required. Cyber law experts handle:

- Patent and Patent Infringements or other Business Cyber crimes
- Cyber Security for Identity thefts and Credit Cards and other financial transactions
- General Cyber Law
- Online Payment Frauds
- Copyright Infringement of software, music and video.

Cyber Law Implementation Professionals

Many agencies play a role in cyber law implementation, which include the e-Governance agencies, law and enforcement agencies, cybercrime research cells and cyber forensic labs. Each of these would have a different category of professionals

VII. CATEGORIES OF CYBER CRIME

Cybercrimes can be divided into following categories:

A. Cyber-crimes against government.

Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

When the European Convention drafted the Cyber Crime Convention, no exact definition of cyber-crime was provided. Every country has its own way of defining cyber-crime, which is peculiar to its own socio cultural situations. For instance, in India defamation is a significant and rampant form of cyber-crime. The UN is strongly trying to put in place a global mechanism to improve awareness as well as to implement and install effective security measures for cyber-crime.

B. Cybercrimes Against Society

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

Child Pornography: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

Cyber Trafficking: It involves **trafficking** in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime.

Online Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Financial Crimes: This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet.

C. Cyber-crimes against property.

These crimes include computer vandalism and transmission of harmful viruses or programs. There are certain offences which affects person's properties which are as follows:

Intellectual Property Crimes Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered **the** name first on by right of using it before the other or using something similar to that previously

Cyber Vandalism: Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized **access**/control over the computer. Due to the hacking activity there will be loss of data as well as computer system

Transmitting Virus: Viruses are programs **w**ritten by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They mainly affect the data on a computer, either by altering or deleting it. A worm attack plays major role in affecting the computer system of the individuals.

VIII. CYBER ETHICS

Cyber ethics are nothing but the code of the internet. Prevention is always better than cure. It is always better to take certain precautions while working on
the network. Few cyber ethics one must follow while using the internet are given below.

- DO use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world
- Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

IX CONCLUSION

Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so .Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime

REFERENCES

1. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
2. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
3. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
4. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68-71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy
5. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
6. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

