IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

A Review Paper on Study of Cybersecurity on Cybercrime

Divyashree Mahesh[1], Divyashree S K[2], Dr. Madhusudhan S[3]
Students, Department of Computer Science and Engineering[1,2]
Assistant Professor, Department of Computer Science and Engineering[3]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on the study of cyber security on cyber crimes. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.*

Keywords: Cyber Security, Cyber Crime, Cyber Ethics.

I. INTRODUCTION

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies. it plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.

Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cybersecurity has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net- banking etc also needs high level of security. Since these technologies hold some important regarding a person their security has become a must thing. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must al be trained on this cyber security and save themselves from these increasing cyber crime.

II. CYBER CRIME

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone's security and financial health.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare. Warren Buffet describes Cybercrime as the "number one problem with mankind" and "poses real risks to humanity."

A report (sponsored by McAfee) published in 2014 estimated that the annual damage to the global economy was $445 billion. A 2016 report by Cybersecurity ventures predicted that global damages incurred as a result of cybercrime would cost up to $6 trillion annually by 2021 and $10.5 trillion annually by 2025.

Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that nearly one percent of global GDP, close to $600 billion, is lost to cybercrime each year. The World Economic Forum 2020 Global Risk report confirmed that organized Cybercrimes bodies are joining forces to perpetrate criminal activities online while estimating the likelihood of their detection and prosecution to be less than 1 percent iOne common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.88 There are several difficulties with this broad definition. It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim. Another broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the “Stanford Draft”),89 which points out that cybercrime refers to acts in respect to cybersystems.

III. Development of Cyber Crimes over 5 decades

3.1 The 1960s

In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology. At this early stage, offences focused on physical damage to computer systems and stored data. Such Understanding cybercrime: Phenomena, challenges and legal response incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university. In the mid 1960s, the United States started a debate on the creation of a central data-storage authority for all ministries. Within this context, possible criminal abuse of databases and the related riskss to privacy were discussed.

3.2 The 1970s

In the 1970s, the use of computer systems and computer data increased further. At the end of the decade, an estimated number of 100000 mainframe computers were operating in the United States.

With falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems that had dominated the 1960s, to new forms of crime. While physical damage continued to be a relevant form of criminal abuse against computer systems, new forms of computer crime were recognized. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud. Already at this time, multimillion dollar losses were caused by computer-related fraud. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cybercrime.

3.3 The 1980s

In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first formsof software piracy and crimes related to patents. The interconnection of computer systems brought about new types of offence. Networks enabled offenders to enter a computer system without being present at the crime scene. In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the process. OECD and the Council of Europe set up study groups to analyse the phenomena and evaluate possibilities for legal response.

3.4 The 1990s

The introduction of the graphical interface ("WWW") in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized.

Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990 and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples.

3.5 The 21st Century

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing", and "botnet attacks", and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP.

Understanding cybercrime: Phenomena, challenges and legal response (VoIP) communication" and "cloud computing". It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

IV. The Cybercrimes That Affect On Technology:

4.1 Web Servers

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud Computing and its Services

These days all small, medium and large companies are slowly adopting cloud services. In other words 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. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

V. APT's and Targeted Attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

5.1 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

5.2 Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.Hence the above are some of the trends changing the face of cyber security in the world.

VI. Protection Techniques To Cyber Security: Control And Password Security:

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.1 Authentication of Data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

6.2 Malware Scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

6.3 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

6.4 Anti-virus Software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

6.5 Cyber Ethics that has to follow to Control cyber crime

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of the 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

- Don't be a bully on the Internet. 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.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

VII. CONCLUSION

Computer security is becoming more important now a days because the world is becoming highly interconnected, with networks being used to carry out critical transactions, sharing messages and even it has becoming the ditialized transcation of amount too. due to that Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. 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. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space for our software.

REFERENCES

[1]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[2]. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
[3]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[4]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[5]. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN
[6]. 2229-5518, "Study of Cloud Computing in Health Care Industry " by G. Nikhita Reddy, G. J. Ugander Reddy
[7]. IEEE Security and Privacy Magazine IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[8]. CIO Asia, September 3rd H1 2013:Cyber security in malaysia by Avanthi.