A Study on Cyber Security And Their Applications

Mrs. R.Jothi[1], Mrs. S.Vidhiya [2]
[1]Assistant Professor,Dept of Computer Science
[2]Assistant Professor, Dept of BCA,
[1, 2] Mahalashmi Women's College of Arts & Science, Paruthipattu, Avadi, Chennai – 71.

Abstract- *Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Securing the information have become one of the great challenges in day today life. Whenever we think about cyber security that comes to our mind is cyber crime which are increasing immensely .Government and various companies are taking many measures in order to prevent to the cyber crimes. This paper mainly focus on challenges on cyber security and the latest technology.*

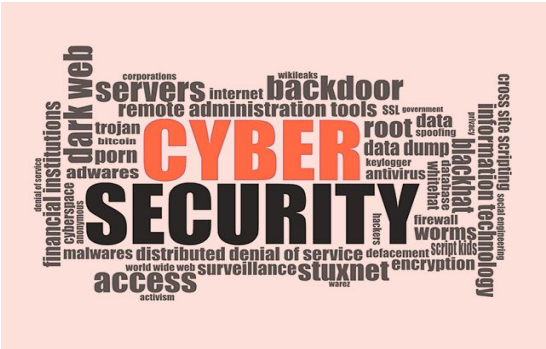
Keywords- Cyber Security, Cyber crime, Cyber ethics, Social media, Cloud computing.

I. INTRODUCTION

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.to steadily include these various types of components into a sophisticated and unified network.

CYBER CRIME:

Cyber crime is illegal activity that uses a computer as primary source for commission and theft. The growing list of cyber crimes includes crimes by computers, network intrusions, dissemination of computer viruses, identity theft, stalking, bullying and terrorism.



Cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity.

RISK IN CYBER SECURITY

Cyber Security refers to the technologies, processes and from unauthorized access by cyber criminals. The frequency and severity of cybercrime is on the rise and there is a significant need for improved as part of every organization's enterprise risk profile.

BENEFITS

Protects the system against viruses, worms, spyware, and other unwanted programs.

1. Protection against data from theft.
2. Protects the computer from being hacked.
3. Minimizes computer freezing and crashes.
4. Gives privacy to users.
5. Improved security of cyberspace.
6. Increase in cyber defense.

II. CYBER SECURITY TECHNIQUES

1. ACCESS CONTROL AND PASSWORD SECURITY

The concept of user name and password must be confidential and it is the first measures regarding cyber security.

2. AUTHENTICATION OF DATA

The documents that we receive must always be authenticated 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.

3. **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.

4. **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

5. **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. It 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

III. IMPACT OF CYBER SECURITY

We have a huge impact on cyber security that are as follows.

Web Servers:

The threat of attacks on web applications to extract data or to distribute malicious code. Cyber criminals distribute their malicious code via legitimate web servers.

Data-stealing attacks, get the attention of media is also a big threat nowadays, so we need a greater emphasis for protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data.

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. We have number of applications available in the cloud grows, policy controls for web applications and cloud services in order to prevent the loss of e information.

Apt's And Targeted Attacks Apt (Advanced Persistent Threat)

It 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. 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 in order to prevent more threats coming in the future.

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.

IPV6: New Internet Protocol IPV6

It is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities.

While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

Encryption Of The Code

Encryption is the process of encoding messages in such a way that 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.

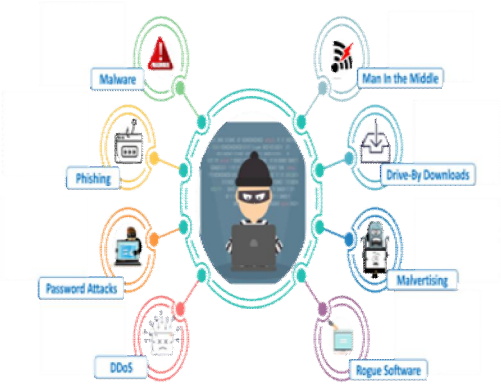
But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can 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. The top network threats are mentioned in below Fig -1. Fig -1 The above pie chart shows about the major threats for networks and cyber security.

TYPES OF CYBER SECURITY

The various types of security in Cyber model as follows:

1. Application Security
2. Information Security
3. Disaster recovery
4. Network Security



Applications Of Security

It encompass measures or counter-measures that are taken during the development life-cycle to protect applications from threats and flaws in the application design, development, upgrade or maintenance. The basic Techniques used in application security are as follows

i) Input parameter validation,
ii)User/Role Authentication & Authorization,
iii) Session management, parameter manipulation & exception management
iv) Auditing and logging.

Information Security

It protects information from unauthorized access to avoid identity theft and to protect privacy. The Techniques used in Information security i) Identification and authentication ii) Authorization of user and iii) Cryptography.

Disaster Recovery:

It is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster.

Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

Network Security

It includes activities to protect the usability, reliability, integrity and safety of the network. It has various network security targets a variety of threats and stops them from entering or spreading on the network. This includes

1. Anti-virus and anti-pyware, Firewall, to block unauthorized access to your network
2. Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
3. Virtual Private Networks (VPNs), to provide secure remote access

IV. LIMITATIONS OF CYBER SECURITY

Cyber security has never been a bigger problem in the modern era of business. Banks are more likely to receive phishing , unlimited access to information, to deal with the underground hackers and cyber attackers.

People are usually the ‘weakest links’ in these attacks, since most threats are allowed access into companies’ networks through scams

Lack Of Consistency

Cyber security awareness training, is a first step for the employee . While the employee forget the training to remember steps and procedures which are more crucial to their day-to-day work lives, hackers will be inventing new ways to get into your cyber security systems and steal you and your customers’ data, Training needs to happen constantly, and get updated constantly regarding cyber security

Lack Of Rigorous Testing

A lazy employee could easily sit through a cyber security awareness lesson every month then go back to work and forget everything as soon as they get through the door, but if they have an exam on what they have learnt – or 'real life' tests, such as invented cyber security threats – then they will have to actually pay attention and concentrate.

Introducing actual stakes to these tests, and treating cyber security like any other vital skills needed in your workplace, will make your employees take cyber security much more seriously, and make them more likely to learn – this will make any resources, time or money that you spend on these lessons worthwhile.

V. ADVANTAGES AND DISADVANTAGES OF CYBER SECURITY

Here some of the advantages and disadvantages of cyber security are as follows.

ADVANTAGES:

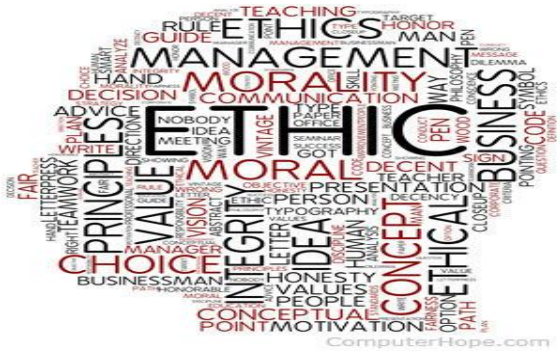
1) Protects the system against unwanted programs.
2) Protection against data from theft.
3) Protects the computer from being hacked.
4) Minimizes computer freezing and crashes.
6) Improved security of cyberspace.
7) Increase in cyber defense.
8) Increase in cyber speed.
9) Protecting company data and information.
10) Protects individual private information.
11) Protects resources.
12) Fight against computer theft.

DISADVANTAGES:

1) It can be difficult to configure correctly.
2) Firewalls may block users from performing certain actions.
3) Makes the system slower than before.
4) Need to keep updating the new software in order to keep security up to date.
5) Could be costly for the average user.
6) It will be costly for average users.

VI. CYBER ETHICS

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 important ways are used in Cyber on internet communications are as follows.



1. Internet is used to communicate and interact with other people.
2. Email and instant messaging makes it easy to stay in touch with friends and family members, colleagues, to share ideas and information with people
3. Do not operate others accounts using their passwords.
4. Never try to send any kind of malware to other's systems and make them corrupt.
5. Never share your personal information
6. Always adhere to copyrighted information and download games or videos only if they are permissible.

VII. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each 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 crime but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

[1] James Lyne, 2012, A Sophos eight trends changing network security, Article 04.12v1.dNA,
[2] Sunit Belapure and Nina Godbole, 2012, Cyber Security: Understanding Cyber Crimes, International Journal of Networking and Computer applications, Vol.5, No.3, pp.135-142.

[3] Audrie Krause and Luis corrons, 2012, Computer Security Practices in Non Profit Organisations – A Net Action Report by Look back on Cyber Security 2012 by– Panda Labs.
[4] Nikhita Reddy and G.J.Ugander Reddy, 2013, Study of Cloud Computing in HealthCare Industry, International Journal of Scientific & Engineering Research, Volume 4, Issue 9, pp.68 – 71.
[5] Nagesh et al., 2013, Safety Critical Systems – Next Generation IEEE Security and Privacy Magazine – IEEECS.
[6] Avanthi Kumar, 2013, Cyber security in malaysia, CIO Asia, September 3rd.