Aspects of Cyber Security on Latest Technologies

Darshana Wajekar[1] ,
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science and
and Commerce, Rasayani

Ashwini Khillari[2] ,
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science
and Commerce, Rasayani

Priyanka Sonawane[3]
Asst. Professor, Department Of IT/ CS
Pillai HOC College of Arts, Science
and Commerce, Rasayani

Abstract— cyber security is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, it 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. This paper focuses on the role of cyber security for resolving cyber crimes.

Index Terms— Cyber Security, electronic data, cyber crimes,.

1 INTRODUCTION

Today Internet is the fastest growing technology in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unparalleled amounts of data on computers and other devices. The range of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. The major areas which are included in cyber securities are as follows:

a. Application Security:

Application security encloses measures taken to improve the security of an application often by identifying, fixing and preventing security weaknesses. Different techniques are used to aspect such security vulnerabilities at different stages of an applications lifecycle such as design, Coding, deployment, upgrade and maintenance. Security measures are applied on normal applications and a sound application security routine minimize the probability that unauthorized code will be able to manipulate applications to access, steal, modify, or delete private and sensitive data.

b. Data Security:

Data security has consistently been a major threat in information technology. In the cloud computing environment, it becomes particularly significant because the data is located in different places even in all the world. Data security and privacy are the two main factors of user's concerns about the cloud technology. Data security refers to the process of protecting and securing a data from uncertified access and data corruption throughout its lifecycle. Data security includes data encryption, tokenization, and key management practices that protect the data across all applications and platforms.

c. Network Security:

Network security is an activity designed to protect the usability and honesty of your network and data.

- It includes both hardware and software technologies
- It targets a variety of injuries
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

d. Disaster recovery:

Disaster recovery planning 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.

e. Web Security:

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

1.1 Cyber security framework

Any cybersecurity framework will provide detailed direction on how to implement a five-step cybersecurity process:

- **Identifying** vulnerable assets within the organization
- **Protecting** assets and data, and taking care of necessary maintenance
- **Detecting** breaches or intrusions
- **Responding** to any such breaches
- **Recovering** from any damage to systems, data, and corporate finance and reputation that result from the attack.

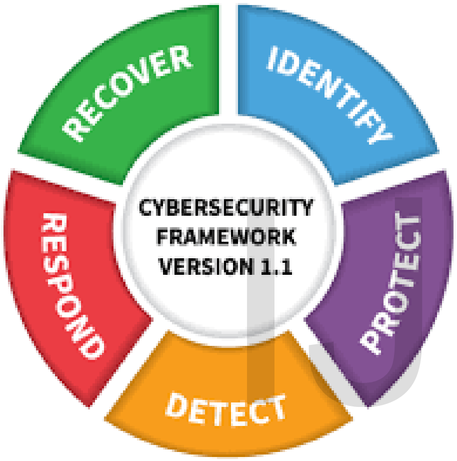

Fig: 1.1 Cyber security framework

2 LITERATURE REVIEW

1. “Cyber Security Survey Results “APARA presented and observed frequency of significant cyber security occurance, the range of threats and the generality of high risk cyber security findings. They suggested that all balanced have an ongoing strategy to address the evolving forms of cyber risk. [1]

2. "Eight trends changing network security" by James Lyne, mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest information about the cyber security techniques, ethics and the trends changing the profile of cyber security.[2]

3. In 2017 Farhad Alam1 et al. said “Usage of data Mining Techniques for combating cyber security”. Different data mining techniques are used for digital security. They showed that data mining based interference location instruments are amazingly valuable in finding security breaks. [6]

4. "A Study on Data Mining Frameworks in Cyber Security" focused on various types of cyber attacks and how data mining concept can help in detection and prevention of these attacks. Information security breach such as access control violations as well as a discussion of various attacks are presented. Finally we present a comparative analysis between a set of selected frameworks.[5]

3 Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.
1. Web based attacks
2. System based attacks

Web based attacks occurs on a website or web applications.
a. Injection attacks
It is the attack in which some data will be injected into a web application to operate the application and pick up the required information.
Example- SQL Injection, code Injection, log Injection, XML Injection etc.

b. Denial of Service
It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by drown the target with traffic or sending it information that activate a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Voume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
Protocol attacks- It consumes actual server resources, and is measured in a packet.
Application layer attacks- Its goal is to crash the web server and is measured in request per second.

c. Brute force
It is a type of security attack which uses a case and error method. This attack generates a large number of guesses and rectify them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

System Based attacks are intended to compromise a computer or a computer network.
a.Virus
It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
b. Worm
It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.
c. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chat room bots, and malicious bots.

4. Techniques Used in Cyber Security

Man creates technology, and it is the man who can get the better of this technology. Thus, no cyber security mechanism is foolproof and can ever be.

Here's a list of the top advanced cyber security technologies.

a. Artificial Intelligence & Deep Learning

Two-factor authentication works by confirming a user's identity based on 2-3 different parameters. The parameters being, something they know, are and have. Add to that additional layers of information and authentication, and that is where AI comes into the picture. Deep learning is being used to analyze data such as logs, transaction and real-time communications to detect threats or unwarranted activities.

b. Behavioural Analytics

Behavioral analytics helps determine patterns on a system and network activities to detect potential and real-time cyber threats. For instance, an abnormal increase in data transmission from a certain user device could indicate a possible cyber security issue.

c. Embedded Hardware Authentication

A PIN and password are no longer adequate to offer foolproof protection to hardware. Embedded authenticators are emerging technologies to verify a user's identity.

d. Blockchain Cyber security

Blockchain cyber security is one of the latest cyber security technologies in this era. Every member in a blockchain is incharge for verifying the originality of the data added. Moreover, blockchains create a near-impenetrable network for hackers and are our best bet at present to safeguard data from a compromise.

e. Firewalls

A firewall is a software program or tranquility of hardware that helps to find out hackers, viruses, worms, trojans that try to reach your computer over the Internet. All messages sent from or received by 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.

V. Conclusion

The proposition that both the "cyber" and the "security" components of the concept "cybersecurity" will be in rapid motion in recent years, because the world is becoming highly interconnected, with networks being used to carry out critical transactions. It is clear that cyberwar or at least cyber dispute will (continue to) happen, because wars will happen and the internet is a contested field, just like land, sea, air, and space. 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. This proposed study focuses on various technologies and tools used to minimize the cyber attacks on this digital world.

REFERENCES

[1]. APRA "Cyber Security Survey Results" in Australian Prudential Regulation Authority (APRA) 2016.

[2]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

[3]. G.NIKHITA REDDY1 , G.J.UGANDER REDDY2, "A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES". 2015

[4] A Recent Study over Cyber Security and its Elements **Article** *in* Journal of Advanced Research in Law and Economics · April 2017

[5] HANAA. M. SAID "A Study on Data Mining Frameworks in Cyber Security" in Faculty of Computing & Information Science in Shams University Abbassia, Cairo, EGYPTE.

[6]. Farhad Alam1, Sanjay Pachauri2 "Usage of data Mining Techniques for combating cyber security" in International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 6 Issue 1 Jan. 2017, Page No. 20011-20016 Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs