Importance of Cyber Security

[1st] Ms Shivani Ghundare
Computer Science department
MITACSC, Alandi (D)
Pune, India

[2nd] Ms. Akshada Patil
Computer Science department
MITACSC, Alandi (D)
Pune, India

[3rd] Prof. Rashmi Lad
Computer Science department
MITACSC, Alandi (D)
Pune, India

***Abstract*-Cybercrime is one of the major crimes done by computer expert. In this paper, need of cyber security is mentioned and some of the impacts of the cybercrime Cyber security is combination of processes, technologies and practices. The objective of cyber security is to protect program, applications, network, computer and data from attack. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude of activities whose loss would all but cripple these organizations. As a consequence, cyber security issues have become national security issues. Protecting the Internet is a difficult task.**
Cyber security can be obtained only through systematic development; it cannot be achieved through hazard seat-of-the-pants methods. Applying software engineering techniques to the problem is a step in the right direction. In this paper author introduces security and privacy in online networking, cryptographic application in cloud computing and internet of things and privacy- preserving computing. Approaches to prevent, detect, and respond to cyber-attacks are also discussed.

Keywords: Cyber security, cryptographic, cyber-attack, insecure network, systematic development, network-based software, cloud computing.

I. INTRODUCTION

Cyber security is also body of technologies, processes and practices designed to protect and secure networks, computer systems, various programs and data from cyber-attack, damage all these things or unauthorized access these. In a computing context, security includes both cyber security and physical security.

A major contributor to internet is that many computer systems and software applications were not designed with enough attention to security. For instance, the Domain Name System (DNS) was not designed to be completely secure.

Implementing cyber security has software, hardware and human components. Humans must implement policies such as using strong passwords and not reveling them, software must be kept up to date with patches that fix its vulnerabilities. Antivirus software and firewalls can help prevent unauthorized access to private data.

II CYBER SECURITY AND PRIVACY IN ONLINE SOCIAL NETWORK

Now a days, the idea of communication has used mainly Smartphone and computers the internet is used. Due to facing the problem of security, various cyber-crimes events happened in the past decade. Cyber security plays an important role in the current development of information technology and services. Cyber security is tried to secure the users to keep their personal and professional information undamaged from the attacks on the internet.

The significance role of cyber security is to protect networks, computers, programs from unauthorized access and loss. Most of the users are not aware of the risks and share their information unknowingly and their lack of knowledge makes them vulnerable to cyber-attacks. So cyber security is the main concern in today's world of computing.

Social media has become very important in the life for many people. But, as with anything else online, it's important to be aware of the risks. We use social media to keep in touch with others, plan events, share our photos and comment on current events. But, as with anything else online, it's important to be aware of the risks. This are some advice on how you can keep your social media accounts safe and secure.

A. Look after your logins

One of the very achievable things of social media is that person is connected from anywhere and always. However, it's very important that where and how you can log in to your accounts our system or device. Avoid your mobile phone safe and secure

B. Use strong passwords on your accounts

We can secure yourself by using strong and unique passwords to maintain for social media accounts is one of the easiest ways to keep them secure.

III CYBER SECURITY AND CRYPTOGRAPHY

Cryptography is also very important models of cyber security. Cryptography applies on algorithms to encrypt and decrypt the bits that represent data in such a way that only authorized users can use it, them to get the original data. Cryptographic algorithms use mathematics or some logic to achieve effective encryption and decryption.

Most common cryptographic standards are available to all and this algorithm are and published, but the clever mathematics makes it impractical to decode the shuffled bits.

Definition

Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange.

In this section we investigate the current cryptographic solutions which provide access to All of these serious crimes are committed online and can be stopped or at the least limited to some level by using Cyber Security Tools. Some of the best Cyber Security Tools made available today are:

A. ***BMQ _Radar Advisor and Watson***

This is by far the best security tool in use by any of the organizations. Watson, *using artificial intelligence (AI)*, is a self-learning and self-evolving system. The working goes as such: IBM Q-Radar tracks the section and gathers information and links online, offline and within the system with that code. It formulates a strategy to encompass it and then when an incident is raised, it kills the threat. This is one of the best online incidents – kill security tools being used.

B. ***Wire shark***

It is one of the most widely used network analyzer protocol. It assesses the vulnerable sections on the network upon which the user is working. Wireshark can gather or see the minutes of the detail and activities which are going on a network. The incoming and outgoing packets of data and the protocol which is being used in the transmission can be easily viewed. It captures the live data and creates an offline analysis sheet, which helps in tracking.

C. ***Crypto stopper***

It is one of the best tools available online right now to stoptheransomware or malwareattacks on a system. What crypto stopper does is that it finds the bots which are encrypting the files and deletes them. It creates a pattern and formula for the threat to latch it on by itself onto the formula, once it latches itself, crypto stopper detects and delete that code. Crypto stopper tends to make a promise of a 9-second threat detection and elimination challenge

D. ***N MAP***

It is one of the primary and open source utilities made available for network securities. NMAP is not only good with small but large networks as well. It recognizes the hosts and the receiver on a network. Along with it, it also runs on all the distributions of operating systems.

E. ***Burp Suite***

It is another web scanning algorithm security tool, which helps to scan web-based applications. The main purpose of this tool is to check and penetrate the compromised system. It checks all the surfaces which might be affected along with the sender and destination's requests and responses for the threat. If any threat is found, it can be eliminated.

F. ***Open VAS***

A utility of Nessus , but very different from Nessus and Metasploit though they work the same, yet different. It is considered as one of the most stable, less loophole and use of web security tools available online at the moment.

IV THERE ARE TWO MAJOR COMPONENTS OF OPEN VAS

1. ***Scanner***

It scans the vulnerable sections and sends a compiled report of all of it to its manager.

2. Manager

It compiles all the requests which are received from the scanner and then it makes a report of all such incidences.

V. CYBER SECURITY PARAMETERS

The parameters for Cyber security are as follows:

1. Identify threats.
2. Identify vulnerabilities.
3. Access risk explore
4. Establish contingency plan.
5. Respond to cyber security accident.
6. Establish contingency plan.

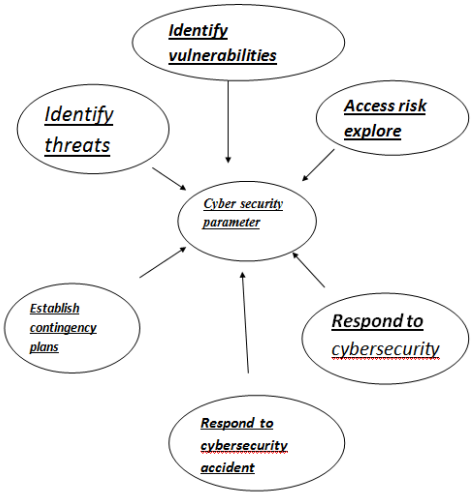

FIG. 1 PARAMETERS OF CYBERSECURITY

VI. WAYS TO PREVENT ,DETECT AND RESPOND TO CYBER ATTACKS

A. Training employees in cyber security principles.
B. Install, use and regularly update antivirus and antispyware software on every computer used in business.
C. Use a firewall for your internet connection.
D. Download and install software updates system and applications as they are available.
E. Make backup copies of important business data and information
F. Control physical access to your computers and network components.
G. Secure your Wi-Fi network. If you have a Wi-Fi network for your workplace make sure it is secure and hidden.
H. Require individual user accounts for each employee.
I. Limit employee access to data and information and limit authority to install software. Regularly change password.

CONCLUSION

Any intelligence device that can pass data to one or more other devices (either through a network or not) is encompassed within the scope of cyber security that include

pretty much the entire foundation of modern society. All need to be aware of cyber security as well as cybercrimes and its little seriousness about security regarding online, social and other activities through which probability of risk is higher. It causes loss of data, modifying data removing useful information as personal details, passwords of mail accounts or bank accounts. People may also know about laws against cybercrimes or cyber laws and action which will be taken and how to fight against crimes.

REFERENCES

[1] Martin , john rice . cyber crimes understanding and addressing the concern of stake holders computer and security.in computional and applies science 'MIT A