"TO IMPROVE THE CYBER SECURITY BY USING SOFTWARE AND HARDWARE DEVICES"

Ravi Shankar Gupta[1]
rsgpta1100@gmail.com

Dr. Praveen Kumar[2]
praveencs10@yahoo.com
(Head, Research & Development Cell)
Mr. Nitin Kumar Kansal[3]
nitinkk65@gmail.com

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, DELHI INSTITUTE OF ENGINEERING & TECHNOLOGY, MEERUT, UTTAR PRADESH, INDIA

ABSTRACT

Cyber security is one of the biggest problem of all over the world. As you know that all the a countries are improving day by day due to their digital things but inspite of this it is seem that often a cyber crime is going on this is only possible due to hackers as well as some masquerdor. In this whole presentation we focus where is the vulnerability then after we will try to resolve it due to this many family as well as many futures are destroying so we must have to be aware about it and do not leave any vulnerability of our system as well as any where.

1. INTRODUCTION

Cyber security is the protection of internet connected system, including hardware, software and data from cyber attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Security related to the protection which includes system security and information security.

2. MAJOR AREAS INCLUDED IN CYBER SECURITY

2.1 APPLICATION SECURITY

Application security is the use of software. Hardware and procedural methods to protect applications from external threats. Application security encompasses the are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design development deployment upgrade or maintenance.

Security measure built into application and a sound applicant security routine minimize the likelihood that unauthorized code will be able to manipulate application to access, steal. modify or delete sensitive data.

2.2 INFORMATION SECURITY

Information security is a set of strategies for managing the process tools and policies necessary to prevent threats to digital and non-digital information .Information security programs are built the core objectives like maintaining the confidentiality ,integrity and availability of IT systems and business data .This objective ensure that sensitive information is only disclosed to authorized parties (confidentiality),prevent unauthorized and guarantee authorized parties when requested (availability).

2.3 EMAIL - SECURITY

Email gateways are the number one threat vector for a security breach. Attackers uses personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to email security application blocks incoming attacks and controls outbound messages to present the loss of sensitive data .

2.4 WEB – SECURITY

A web security solution will control your staff's web use block web-based threats, and deny access to malicious websites "web security" also refers to the steps you take to porters to your own website.

2.5 MOBILE DEVICE SECURITY

Cyber criminals are increasingly targeting mobile devices and apps. Of course, devices can need to control which devices can access their network. The user will also need to configure their connections to keep network traffic private

2.6 WIRELESS SECURITY

Wireless security are not as secured as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere including the parking lot

3. SECURITY ATTACKS AND TYPES

Security attack is any action that comprises the security of information owned by an organization using any process that design to detect there are several type of attacks but most common security attacks are described below.

3.1 DENIEL OF SERVICE ATTACKS

These attacks are mainly used to unavailable some resource like a web server to users. These attacks are very common today . They used overload to resource with illegal time request for service .The resource cannot process the flood requests and either slows or crashes.

3.2 BROWSER ATTACK

These attacks target end user who are browsing the internet. The attacks may encourage them to unwittingly download malware . These attacks used fake software update or application .Websites are also force to download malwares . The best way to avoid browser –based network attack is to regularly update web browsers.

3.3 SHELLSOCK ATTACKS

These attacks are refers to vulnerabilities found in bash, a common command ,line shell for Linux and Unix systems. Since, many systems are never updated , the vulnerabilities are stile present across the web. The problem is so widespread that shell sock is the target of all network.

3.4 SSL ATTACKS

These attacks are interrupted data that is sent over on encrypted connection . These attacks successfully access to the unencrypted information . These attacks are also very common today.

3.5 BACKDOOR ATTACKS

These attacks are used to bypasses normal authentication to allow remote access .these attacks are added in software by design .They are added in the programs .Backdoor is less common types.

3.6 BOTNET ATTACKS

These attacks are hijacking .They are computers that are controlled remotely by one or more malicious actors .

Attackers use botnet for malicious activity ,or rent the bonnet for malicious activity ,or rent the bonnet to perform malicious activity for others. Malicious of computers can be caught in a bonnet’s snare

4. CYBER SECURITY PARAMETERS

THE PARAMETERS FOR CYBER SECURITY AS FOLLOWS

Identify threats

Identify vulnerabilities

Access risk explore

Establish contingency plan

Respond to cyber security accident

Establish contingency plan

In 2015 McAfee reported that there attacks are detected and percentages of their attack are shown with the help of table

Name of attack	percentage of attack
Senile of service attacks	37%
Brute force attacks	25%
Browser force attacks	9%
Shellshock attacks	7%
SSL attacks	6%
Backdoor attacks	2%

5.COMMERCE SECURITY TOOLS

Firewalls- software and Hardware

Encryption software

Digital certificates

Digital signature

Biometrics – retinal scan fingerprints, voice, etc

Passwords

Malicious code

VIRUSES they have ability to replicate and spread to other files most also deliver a payload of some sort, include macro viruses, file –infecting viruses and script viruses.

Trojan Horse they are design to benign but then does something other than expected.

Worms They are design to spread from computer to computer

Bots it can be covertly installed on computer responds to external commands send by attackers.

Unwanted programs there are installed without the user's informed constant.

Phishing an email –borne attack that involves tricking the email recipient into disclosing confidential information or downloading malware by clicking on a hyperlink in the message.

Spear phishing amore sophisticated form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.

6. COMPUTER SECURITY

In computer security a countermeasure is an action device procedure or technique that reduces a threat a vulnerability, or an attack by eliminating or preventing it by minimizing the harm it can cause or by discovering and reporting it so that corrective action can be taken.

Security by Design security by design means that the software has been designed from the ground up to be secure, In this case security is considered as a main feature .

Security Architecture the open security Architecture organization defines IT security architecture at the design artifacts that describe how the security controls are positioned and now they relate to the overall information technology architecture.

Security Measures a state of computer "security "is the conceptual ideal attained by the use of the three process

Response These processes are based on various policies and system components which include the following User account access control and cryptography can protect system files and data respectively

Firewalls are by far the most common prevention system from a network security prospective as the can shield access to internal network services and block certain kinds of attacks through packet filtering.

Intrusion Detection system (I D S) products are design to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems

Response is necessarily defined by the assessed security requirements of an individual system requirements of an individual system requirements of an individual system and may cover the range form simple upgrade of protections to notification of legal authorities counter attacks and the like.In some special cases, a complete destruction of the compromised system the a compromised system is favored, as it may happen that not at all the compromised sources are detected. Today, computer security comprises mainly preventive “measures .

7. VULNERABILITY MANAGEMENT

Vulnerability Management is the cycle of identifying and remediating or mitigating vulnerabilities, especially in Software and firmware .Vulnerability Management is the integral to computer security and network security. Vulnerability can be discovered with a vulnerability scanner, which analyzes of known vulnerabilities such as open ports, insecure software configuration and susceptibility to malware. Many organization contract outside security auditors to run .

8. HOW TO MAINTAIN EFFECTIVE CYBER SECURITY

Organizations and governments have taken a reactive point product approach to fighting cyber threats,cobbling together individual security technologies to protect their network and data.

8.1 Machine Learning

Can help accurately identifying variation of know threats, recognize patterns , predict the next steps of an attack and inform automation tools to create and implement protection across the organizations all in near real time.

With shared threat intelligence, anything one user sees, identifies or prevents benefits all other members of the shared community more comprehensive prevention attainable more quickly reduces over all cyber security risk to something easier to manage .

8.2 SECURE THE ENTERPRISES

Build for simplicity our lightly integrated innovations are easy to operate , delivering consistent protection across network cloud and mobile users.

8.3 SECURE THE CLOUD

Prism is the industry’s most complete cloud security offering. Accelerate your cloud journey with a product suite desired to secure Today’s complex IT environment.

8.4 SECURE THE FUTURE

The industry's only open and integrated AI- based continuous security platform the constantly evolves to stop the most sophisticated threats.

9. WHAT IS A CYBER SECURITY SPECIALIST

Cyber security specialists help to ensure the safety of a company's computer network and systems they maintain the through testing as well as virus protection and regular updates.

Because they are in charge of the electronic security of the organizations they will need to able to communicate with members of other departments and explain the necessary precautions taken to prevent any attacks periodically these specialists recertify the security of applications and the server. They troubleshoot and implement creative solutions.

10. WHAT DO I NEED TO STUDY TO BECOME A CYBER SECURITY SPECIALIST?

For cyber security specialist you should obtain a four year bachelor's degree in computer programming computer science, information science or computer engineering. English , statistics and mathematics courses will be needed as well.In some instances according to U.S bureau of labor statistics (BLS) relevant work experiment with certification may be sufficient for employment.

11. CONCLUSION AND FUTURE SCOPE

For better and safe calculation anti-vireus software are installed and be helpful for global network freely. Information is the best form of protection ,frequently checks the viruses. Cyber security provide a safe and secure environment for performing all the task that needs security. Cyber security has a better scope for all the students who want to become a cyber security expert or who want to learn more about the security of the system.

12. REFERENCE

1. Dinesh.S, Dinesh.A, Kirubakaran.K, "UTILISATION OF WASTE PLASTIC IN MANUFACTURING OF BRICKS AND PAVER BLOCKS'' International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 1, 2016.
2. Maneeth.P.D, Pramod.K, Kishore Kumar, Shanmukha Shetty, "UTILISATION OF WASTE PLASTIC IN MANUFACTURING OF PLASTIC-SOIL BRICKS''International Journal of Engineering Research and Technology (IJERT), Volume 3, ISSN 2278-0181, Issued 8th edition 2014.
3. Hiremath, P.M., S. Shetty, P.G.N. Rai and T.B. Prathima, 2014. Utilization of Waste Plastic in Manufacturing of Plastic-Soil Bricks. International Journal of Technology
4. Alan Solomon, Dmitry O Gryaznov 1995. Dr. Solomon's virus encyclopaedia
5. Mark Ludwig 1998. The giant black book of computer viruses.

6. Szor Peter. The art of computer virus was published in 2005