ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Recent Study over Cyber Security and its Elements

Jitendra Jain
Research Scholar, Faculty of Computer Science
Pacific Academy of Higher Education & Research
University, Udaipur, Rajasthan, India

Dr. Parashu Ram Pal
Professor, MCA
Lakshmi Narain College of Technology,
Bhopal, M.P., India

Abstract: Computer security or Cyber Security is combination of processes, technologies and practices. The objective of cyber Security is to protect programs, application, networks, computers and data from attack. In a computing context, security includes both cyber security and physical security. The attacker damage or theft software or information well as from disruption or misdirection of the services they misguide. Cyber security includes controlling physical access of the hardware, application, networks and protecting against harm that may come via networks. In this paper we proposed study of Cyber Security and its elements. We also give various security aspects related with cyber security.

Keywords: Cyber Security, Parameters of Cyber Security and Security Attacks.

I. INTRODUCTION

Cyber security is the combination of policies and practices to prevent and monitor computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation[1] The major areas which are included in cyber securities are as follows:

a. Application Security

Any software the user can use to run their business needs to be protected, whether the IT staff builds it or whether the user can buy it. Any application may contain holes, or vulnerabilities, those attackers can use to infiltrate user’s application. Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Application security encompasses measures or counter-measures that 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 measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

b. Information Security

Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security programs are built around the core objectives like maintaining the confidentiality, integrity and availability of IT systems and business data. These objectives ensure that sensitive information is only disclosed to authorized parties (confidentiality), prevent unauthorized modification of data (integrity) and guarantee the data can be accessed by authorized parties when requested (availability).

c. Email Security

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

d. Mobile Device security

Cyber criminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, the users need to control which devices can access their network. The user will also need to configure their connections to keep network traffic private.

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.

f. Wireless Security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, user need products specifically designed to protect a wireless network.

II. 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

Figure 1 shows the parameters of Cyber Security.

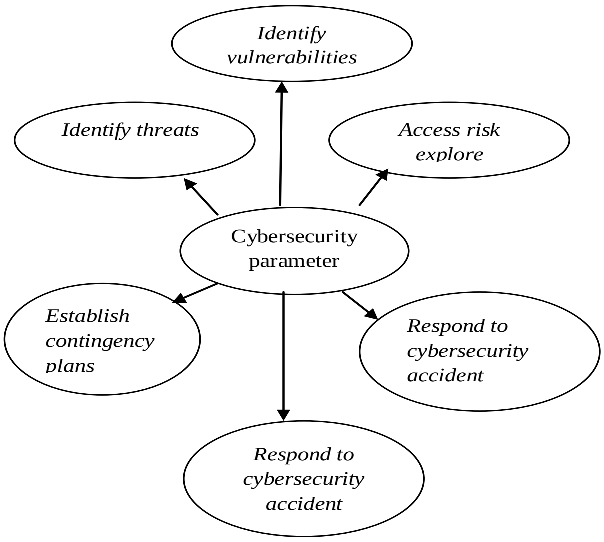
Identify vulnerabilities
Identify threats
Access risk explore
Cybersecurity parameter
Establish contingency plans
Respond to cybersecurity accident
Respond to cybersecurity accident

Figure 1 Parameters of Cyber Security

III. LITERATURE REVIEW

In 2013 Preeti Aggarwal proposed “Application of Data Mining Techniques for Information Security in a Cloud: A Survey”. She has discussed that how data mining techniques contribute extremely to do task of assuring security of information. She has reviewed the various data mining techniques and presented how these techniques are help to achieve security of information on cloud. [1]

In 2014 Kartikey Agarwal proposed “Network Security: Attacks and Defense”. They discussed various methods of attacks which are used as well as various defense mechanisms against them. They have also shown that some of the attacks are easily prevented by using simple. They also discussed some new attacks are found by researchers across the world and how to prevent from them. [2]

In 2015 Shikha Agrawal & Jitendra Agrawal et al. proposed “Survey on Anomaly Detection uses Data Mining Techniques”. This paper presented the various techniques or applications are available to protect data. They observed in their work that anomaly detection uses data mining techniques to detect chances of attacked. They also discussed that various hybrid approaches have also been made in order to detect known and unknown attacks. [3]

In 2016 APRA presented “Cyber Security Survey Results “. This paper presented and observed frequency of significant cyber security incidents, the range of threats and the prevalence of high risk cyber security findings. They suggested that all regulated have an ongoing strategy to address the evolving forms of cyber risk. [4]

In 2017 Farhad Alam1 et al. proposed “Usage of data Mining Techniques for combating cyber security”. They discussed about different data mining methods that are effectively connected for digital security. They showed that data mining based interruption location instruments are amazingly valuable in finding security breaks. [5]

IV. SECURITY ATTACKS AND TYPES

Security Attack is any action that compromises the security of information owned by an organization using any process that designed to detect. There are several types of attacks, but most common security attacks are described below:

a. Denial of Service Attacks

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

b. Brute Force Attacks

These attacks try to kick down the front door. It’s a trial-and-error attempt to guess a system’s password. One in four network attacks is a brute-force attempt. This attack used automated software to guess hundreds or thousands of password combinations.

c. Browser Attacks

These attacks target end users 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 ways to avoid browser-based network attacks is to regularly update web browsers.

d. Shellshock 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 still present across the Web. The problem is so widespread that Shellshock is the target of all networks.

e. SSL Attack

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

f. 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 or created by altering an existing program. Backdoors is less common types.

g. Botnet attacks

These attacks are hijackers. They are computers that are controlled remotely by one or more malicious actors. Attackers use botnets for malicious activity, or rent the botnet to perform malicious activity for others. Millions of computers can be caught in a botnet’s snare.

In 2015 McAfee reported that these attacks are detected and percentages of their attack are shown with the help of table in Table 1 and with graph in Figure 2.

Table 1 Percentage of Various Attacks

Name of Attack	Percentage of attack
Denial of service attacks	37%
Brute force attacks	25%
Browser attacks	9%
Shellshock attacks	7%
SSL attacks	6%
Backdoor attacks	2%
Botnet attacks	2%
Others	12%

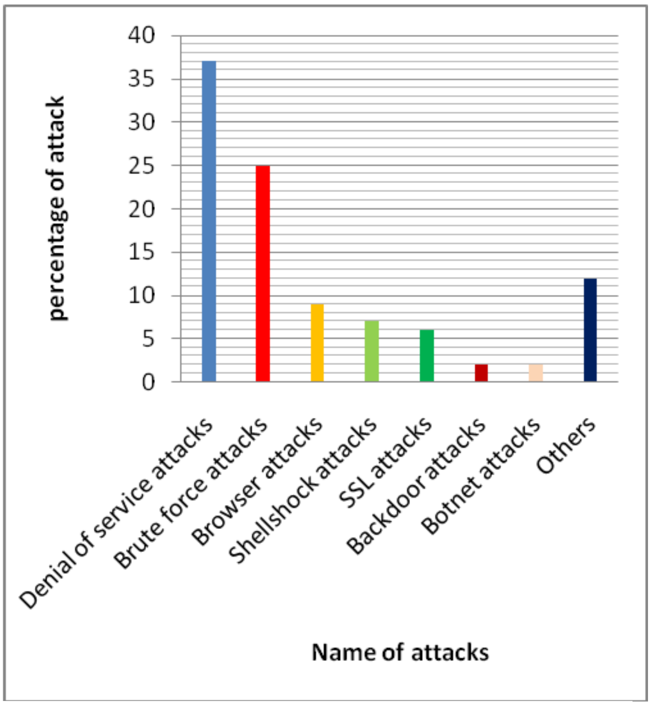

Figure 2 Percentages of Various Attacks

V. REFERENCES

[1] Data Warehousing and Data Mining Techniques for Cyber Security by Anoop Singhal.

[2] Preeti Aggarwal "Application of Data Mining Techniques for Information Security in a Cloud: A Survey" in International Journal of Computer Applications (0975 – 8887) Volume 80 No 13, October 2013.

[3] Kartikey Agarwal & Dr. Sanjay Kumar Dubey "Network Security: Attacks and Defense" in International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.

[4] Shikha Agrawal, Jitendra Agrawal "Survey on Anomaly Detection using Data Mining Techniques" in 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems Available online at www.sciencedirect.comProcedia Computer Science 60 (2015) 708 – 713 2015

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

[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

[7] Bhavani Thurai singham, Latifur Khan "Data Mining for Security Applications" in 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing

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