ISSN No. 0976-5697

Volume 6, No. 8, Nov-Dec 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Development in stages of Cyber security & Risk

Ms. Komal saxena
Phd. Scholar
SinghaniaUniversity(Raj) India

Dr. Anuraag Awasthi
Singhania University(Raj) India

Abstract: Though the digital world has eased the way of doing work yet it possesses threats to mankind. Networks, computer viruses, Phishing, stealing of data by hackers, and other cyber crimes affect people's life from inconvenient to life-threatening ways. With the increase in the number of mobile users, data network, digital applications, there is also an increase in cyber crime activities leading to exploitation.

Keywords: Cyber security, Cyber-risk, Security-Standards, Risk –Assessment, Vulnerability

I. INTRODUCTION

Cyber security sometimes is referred to as computer or IT security, focusing on securing computers, programs and data, networks from unauthorized access, destruction or change. The field comprises all the mechanisms and processes by which digital devices like Computers, Laptops, Smartphone or Tablets information, data and services are protected from an unintended access. It is of foremost significance in line for to growing demand of computer's in offices, business, organisations, etc.

II cyber security

Yes, it is important today the reason is most of the Corporations, Businesses, Financial Institutions, Military, Hospitals and Governments, collect, store and process a large amount of data in the form of information on computer systems and transmit that data via networks to other systems.[5] There is a risk involved when transferring data from one system to another, this is cyber attack. An ongoing attention is required to protect vital business and personal information against cyber crime activities.[5][6]

III.Vulnerabilities

There are various types of vulnerabilities such as Spoofing, Repudiation Information disclosure, Denial-of-service attack, Social engineering, Direct-access attacks, Eavesdropping, Damaging, Secondary attacks, and Trojans, etc,[3] that may affect computer systems in areas like financial systems, Aviation, consumer devices, large corporations, automobiles and government.[8]

IV. Cyber security and risk are on developing stage

A. Systems design

Though there are various perspectives toward contemplate after planning a PC framework, security can end up being vital. In 2010 the Symantec, has done the surveyed they found 92% toward actualize security enhancements to their PC frameworks, with 42 % declaring cyber security by means of the maximum risk.[10] Now there are numerous organisations are enhancing security measures and numerous sorts of cyber crimes are discovering their ways.

B. Security measures standards

A condition of PC "security" is accomplished by the utilization of the three procedures: risk avoidance, then exposure and finally recovery. These techniques are taking into account by different approaches and framework parts, which include-

- Access controls, Client record,, and cryptography can secure documents plus information.
- Firewalls remains a long shot the greatest well-known anticipation frameworks from a system security fact of observation as they can protect access to Border Protection Device, and square assured categories of assaults through bundle sifting. They may be both equipment and programming constructed.
- Intrusion Detection Systems (IDSs) are intended to identify system assaults in development and help with post-assault criminology, whereas review lines and table/logs serve a comparable capacity for specific frameworks. [9]

C. New credit card improved the security

Looking at the cyber crime activities, credit card companies are coming up with various security solutions against cyber crime activities like Chip and PIN credit cards, which will become more common in 2015 [4]. It comprises a computer chip that gives a unique code for every transaction made, making them highly secure against the existing credit cards that generally store account information on a magnetic stripe.[4]

VII BSI Quality

A. Cyber Security guidelines-

The Federal Office for Information Security (BSI) has been putting forth data and help on all parts of IT security for a long time. The BSI's IT-Grundschutz has turn into the most extensive standard take a shot at IT security.[7] It is utilized by various organizations and open bodies as the premise on which to assemble their own particular inventories of measures. In accordance with improvements in data security, the IT-Grundschutz has turn out to be more perplexing and more extensive running. Henceforth, SMEs with constrained budgetary and human resources particularly require a prologue to the subject that is simple and quick to execute.[7]

These Guidelines or rules are expected to fulfill the need, giving an overview of the most essential Cyber security measures. It focuses on securing organizational work and illustrating cyber threats through practical cases. To put it

plain and simple, any individual who consequently executes the proposals made in these guidelines or who utilizes them to draw up administration contracts with IT service providers suppliers, is in the right path for a sound level of Cyber security [4].

V. Web application firewall (WAF)

It can be characterized as a method for splitting system info among a cloud or a system and another system, for illustration, the Internet, can be symbolized as program consecutively on the device, instructing & using the stack method to give continuous sifting and blocking. Another convention is an suspected physical firewall which encompasses of a unlike device examining system movement. They are regular amongst a device that remains forever linked by Internet.

A Web application firewall (WAF) monitors then filters and finally chunks the HTTP traffic flow .Through adaptable review, it has the capacity to anticipate assaults, for example, XSS, buffer overflows; SQL injection and session hijacking, which IDSs and network firewalls are unable to perform. They similarly ready to recognize also to avoid novel obscure occurrences by looking for same designs/pattern in the congestion or in data traffic.[1][2]

It can be network based or cloud-based .It is also is regularly conveyed over a proxy also set before a single or more Web applications. WAFs are a typical security mechanism used in various organisations to secure Web applications against impersonation, zero-day exploit also varied vulnerabilities.

It activated to pick up consideration once the “PCI Security Standards Council” framed and PCI DSS agreeability well-ordered by Credit card companies for dealers that started transaction through payment plastic card. “ PCI DSS” indulges that Web applications are strengthened done both a WAF and program security evaluation.[1][2]

Examples of WAF

- NetScaler AppFirewall, Citrix Systems Incorporation's [2]
- FortiWeb-400C, Fortinet Incorporation's [2]
- “BIG-IP Application Security Manager”, F5 Networks Incorporation's [2]

VI Risk-Assessment: Comprehensive approach

The one approach of making a security idea is the conventional risk assessment. This involves concocting an individual security shields for a current IT environment. The assets which need to be protected are computer systems, data and other vital information that are analyzed to see which threats they meet. The next stage is to break down the likelihood of a security occurrence; the probable degree of harm, what security protections can be taken and what risks stay after the security idea has been executed. [9]

Doing risk assessment gives important data, but is connected with a great deal of work due to the need to do them on an individual premise: specialists with proper expertise are required. The applicable data variables, for example, the likelihood or degree of harm, are extremely hard to determine and best case scenario must be ascertained generally. Hence, a risk assessment though is comprehensive and most suitable, but at the same time is expensive.

B. **BSI'sIT-Grundschutz methodology acts as an efficient alternative**

- IT-Grundschutz methodology is on the BSI standard 100-2 consisting [11]of various modules, threats and safeguard catalogues.Utilizing the IT-Grundschutz approach, it is conceivable to actualize Cyber security ideas basically and monetarily as far as the assets needed. The achievable level of security is sufficient and sensible for ordinary assurance prerequisites and can serve as the premise for Computer systems and applications which oblige a greater level of protection. Just if the protection necessity is altogether higher or the computer systems concerned are not secured in the IT-Grundschutz Catalogs is it important to do a security analysis.

IT-Grundschutz methodology gives the following advantages: [11]

- Standard security shields (safeguards) are depicted in detail. [11]
- The subsequent IT security ideas are adaptable, compact and can be fixed, as they allude to an existing source.[11]
- The security protections to be executed are field-demonstrated and have been chosen so that their execution will be as cheap as could reasonably be expected.
- Even in the event that somebody ought not to make a complete security idea, because of the measured structure, the IT-Grundschutz Catalogs can serve as specialized rules and a wellspring of counsel on an extensive variety of security issues, which clearly is beneficial[11].
- Now in the present scenario, yes, there is an improvement in cyber security methodologies and risk assessment procedures with the help of some of the innovative security measures like Web application firewall, BSI’s Guidelines and methodologies, etc.

VIII. Conclusion:

Looking at the present scenarios there is an increase in cyber criminal activities. Cybercrime through computer networks, phishing, hacking are the most common ones infecting computer systems and stealing personal information. It is now time to improve computer cyber security from such vulnerabilities so that the data is secured and protected. Today, there is a risk involved when transferring data from one system to another, this is cyber attack. An ongoing attention is required to protect vital business and personal information against cyber crime activities.

Various security measures can be taken like Firewalls are by a long shot the most well-known anticipation frameworks from a system security point of view as they can shield access to inward system administrations, and square certain sorts of assaults through bundle sifting. Firewalls can be both equipment and programming based. Intrusion Detection Systems (IDSs) are intended to identify system assaults in advancement and help with post-assault

criminology, while review trails and logs serve a comparable capacity for individual [8]frameworks.

A Web application firewall (WAF) is another security measure that first monitors then filters and finally blocks the HTTP traffic from a web application. Through adaptable review, it has the capacity to anticipate assaults, for example, XSS, buffer overflows; SQL injection and session hijacking, which IDSs and network firewalls are unable to perform. A WAF is likewise ready to recognize and avoid new obscure attacks by looking for patterns in the traffic data.

BSI's Guidelines and methodologies if properly followed then surely your system is protected. Utilizing the IT-Grundschutz approach, it is conceivable to actualize Cyber security ideas basically and monetarily as far as the assets needed. The achievable level of security is sufficient and sensible for ordinary assurance prerequisites and can serve as the premise for Computer systems and applications which oblige a greater level of protection.

References

[1]https://www.owasp.org/index.php/Web_Application_Firewall

[2]http://www.cyberoam.com/webapplicationfirewall.html

[3]www.webopedia.com/TERM/S/security_vulnerability.html

[4]http://www.usatoday.com/videos/tech/2015/01/06/21330105/

[5] http://trilateralresearch.com

[6]http://cs100w-anthonytsang.blogspot.com

[7]http://www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Standards-for-IT-and-cyber-security/

[8]http://www.kb.cert.org

[9]https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security

[10] www.symantec.com

[11]BSI Standard 100-2 IT-Grundschutz Methodology

Author's Profile

Ms. Komal saxena perusing Ph.D. in computer science from singhania University .My research is on Cyber security and risk Presently working in university. I have total 15 years of experience in teaching and more than 3 years in corporate. I Published more than 6 paper in reputed Journals.

Dr. Anurag Awasthi(Guide) Over 27+ years of rich overseas and indigenous experience (21 years in Corporate and 6+ years in Academics/Consulting)(Worked in India, Japan, France and Thailand. Visited SriLanka and Pakistan.). (Ex) Director and Professor (MCA) with Noida Institute of Engineering & Technology (NIET), Greater Noida. Ph.D. (Computer Science) - ('An Integrated Framework for Implementing Process Improvement in Software Development Organisation') fromKumaun University, Almora (Uttarakhand), 2005.