International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174, Volume 7, Number 5 (2014), pp. 517-522

http://www.irphouse.com

Cyber Security: Safeguarding the Networks

Gunjan[1] and Saguna Khajuria[2]

*[1,2]DPC Institute of Management, Plot no.-2, Institutional area,
Sector-9, Dwarka, New Delhi -110077*

Abstract

Cyber security associates with technologies, processes and practices designed to protect organization's networks. Today internet and cyber space is the life line of every business and to protect the data present in these networks is a big concern for every organization. Cyber security is basically protecting computer, computer networks, data and information from an unauthorized access, vulnerabilities and attacks by cyber criminals. It also protects the IT infrastructure from Cyber Terrorism, Cyber Espionage and Cyber Warfare. Cyber security has emerged as a strong player to deal with various security breaches and hacking issues in the cyber space, which impacts the economic growth of the organizations. With high profile security breaches and advanced threats, cyber security concerns have influenced the regulatory authorities to bring out necessary regulations. The paper investigates what is cyber security, various threats affecting organizations networks, steps taken by organizations and regulatory bodies in securing their networks. The study will be conducted through extensive literature review, obtaining information across various sources to evaluate what steps are taken to secure the valuable data in cyberspace.

Keywords: Vulnerability, Confidentiality, Integrity, Availability, Cyber Terrorism, Cyber Espionage, Cyber Warfare.

1. Introduction

The information technology infrastructures of almost every country today is very vulnerable, though various regulations and measures are taken to protect it still there are lots of illegal penetrations. Be it defense or commercial, cyber space of both the areas are frequently attacked by anonymous agents. The computer networks play a key role in processing data, storage of important information, monitoring and control of critical infrastructures and disruption in any of these can cause serious implications that can affect the progress of any organization which ultimately affects the progress of any nation.

Recently there were security breaches in the IT infrastructure of Google in China and it was so severe that Google had to terminate its operations there. Similar attempts have also occurred at many companies, to name a few- Exxon-Mobile, Conco-Philips and Marathon Oil, where the purpose of the attacks was to steal proprietary information. Not only organizations are affected due to cyber attacks but such attacks can also affect an individual, like theft of important personal information such as credit card details, Pin no, account details etc.

The present day cyber security systems cannot protect from all attacks since most of them are host based intrusion detection systems and as a result are not sufficient to protect the networks due to sheer volume, distributed nature of data, and real-time response, moreover these systems can only deal with known attacks. The main strategy to tackle cyber attacks is to build and maintain a trustworthy computing system which closely inspects and monitors the activities in cyber space and also is capable of detecting new attacks. A regular collection and analysis of the network traffic and the trails of system usage can help in inhibiting the attacks.

2. Objective

The paper investigates what is cyber security, various threats affecting organizations networks, steps taken by organizations and regulatory bodies in handling cyber crimes.

3. Methodology

The study will be conducted through extensive literature review, obtaining information across various organizations to evaluate what steps are taken to secure the valuable data in cyberspace. Furthermore we would also be considering the various security issues and cyber crimes that occur globally.

4. Major Cyber Threats [1]:

- **Cyber Terrorism:** Cyber terrorism is the disruption of computer networks and public internet which threatens the unity, integrity or sovereignty of India. There is much concern from government and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies. In the past, there have been many incidents where terrorists have caused cyber attacks on national security of many countries.
- **Cyber Warfare:** Cyber warfare is malicious cyber activity directly threatening the security, defense capabilities, important infrastructure or societies of a nation. Cyber warfare refers to politically motivated hacking on information and information systems to conduct espionage (acquisition of sensitive

information), destruction of critical infrastructure, manipulation of defense or other vital systems. Cyber warfare often can include personal information theft by various means in order to use it to gain access to bank accounts. Cyber warfare attacks can disable official websites and networks, disrupt required services, steal or alter classified data etc.

- **Cyber Espionage:** Cyber espionage involves the access to secrets of sensitive, personal or critical information stored on computers or networks without the permission of the holder of the information for strategic, economic, political or military advantage. Now days, cyber espionage involves analysis of public activity on social networking sites like Facebook and Twitter.

5. Goals of Cyber Security:

The main aim of cyber security is to protect valuable data and networks from external and internal threats present in an organization. However there are few more objectives of cyber security such as [2]:

- To help organizations in developing a secure organization culture.
- Reduction in misuse of data and information.
- To help people reduce the vulnerability of their ICT (Information and Communication Technology) Systems.
- Working in collaboration with public, private and international entities to provide a secure cyberspace.
- To be continuously updated about the threats present in networks and to develop effective measures to curb it.
- To manage Confidentiality, Integrity and Availability (CIA) of data.

Cyber security Approach:

To have a successful Cyber security approach organizations should maintain a balance between accessibility and security. To implement an effective Cyber security program, organizations require few essential parameters, which are [3]:

- **Risk Awareness:** The foremost and most important parameter is to generate awareness throughout the organization regarding the probable risks, in other words to create a risk-aware culture. It is important for organizations to know about their vulnerable areas, from where attacks can come, what are the security goals and let everyone know about it.
- **Powerful Security System:** To deal with various attacks and threats, organizations need a robust security rich system, which can track and update all the systems, networks, as well as install the essential software regularly.
- **Incident Management:** It is important for Organizations to intelligently manage incidents. Application of automated response capabilities and intelligent analytics is the need of the hour for better monitoring and for better incident management.

- **Skillful Workforce:** The organization should have a team of experts which is able to handle the security systems. The workforce should have desired skills, knowledge and should be continuously updated about the risks and threats in the current scenario.

6. Effective Measures taken by organizations and regulatory bodies for Cyber Security:

There are several effective Measures taken by Government and Organizations to protect their networks [4, 5, 6, 7], some of them are:

- Effective security policy structured right at the strategic planning stage to ensure robust cyber security.
- Using up to date antivirus software
- Use of firewalls to protect against unauthorized access.
- Implementation of security control systems in organizations which help to secure the data and reports against any attack.
- Efficacious recovery and back up techniques should be implemented.
- A proper research and development department in the area of network crime and security should be there to study about emerging threats, work on finding solutions and raise awareness about it.
- Government of India has established NIC (National Informatics centre) to provide security and network support as well as various ICT services to central and state governments which protects them against any type of vulnerabilities.
- To enhance the security communications and information infrastructure, Cert-In (Indian Computer Emergency Response Team) was formed. It is the most important part of India's Cyber community and aims at providing security assurance. It also creates a panel of auditors for handling IT security and all the organizations operating in India are subject to this third party audit from Cert-In.
- NISAP(National Information Security Assurance Program), a government initiative for Cyber Security provides certain regulations and policies that all organizations in India should implement.
- An initiative by CII (Confederation of Indian Industry) to set up India Anti Bot Alliance for raising awareness about emerging threats.
- Indian government has formed a Crisis Management Plan for countering cyber attacks and threats which has to be followed by all the ministries and departments.
- Organizations have been informed to implement Information security management practices based on International standard ISO 27001.

7. Findings & Conclusion

Key findings from our research are that if organizations don't follow or implement Cyber security it can lead to financial loss and can also affect the image of the organization; the productivity is also affected. The management of the organization should make security policy a part of its strategic planning and every employee of the organization should be aware about the security policies and the probable risks that can affect their performance.

The government of India has taken many measures to overcome cyber crime and network security issues but still lots need to be done in this area.

Since more and more people are using online services, it becomes essential to educate them regarding cyber crime and how they can deal with it. An awareness needs to be generated amongst the common man so that he doesn't fall prey to any kind of cyber threat while using computer networks.

References

[1] Batsell, Stephen G., Nageswara S. Rao, and Mallikarjun Shankar. *"Distributed intrusion detection and attack containment for organizational cyber security."* 2006]. http://www. ioc. ornl. gov/projects/documents/containment. pdf (2006).

[2] Rob Mahoney, Jenny Holzer, Lance Joneckis, *Cyber Security Technology Initiatives*, IDA Document D-4584, Log: H 12-000352.

[3] IBM Security Services Cyber Security Intelligence Index- *Analysis of cyber security attack and incident data from IBM's worldwide security operations* July 2013.

[4] Proceedings of the First IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop 2011, Gaborone, Botswana 12 May 2011.

[5] Maria Paek, *Question of Cyber Security*, MUNiSC 2014 SC, http://munisc.qmischina.com/wp-content/uploads/2011/05/Question-of-Cyber-Security.pdf.

[6] Jonathan Diamond, *India's National Cyber Security Policy in Review*, The Centre for Internet and Society, July 2013.

[7] Department of Information Technology- National Cyber Security Policy of India.

[8] http://www.infosecurity-magazine.com/view/34549/indias-cybersecurity-challenge/