International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

Security Threats & Their Solution to Prevent Against Cyber Attacks

Manish Bhardwaj[1], Ajay Fageria[2], Naveen Sain[3], Bhavesh Kumar[4]
Department of CSE, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India

Abstract: ***Cyber Security is of major concern in today's era of computing to secure data, network resources, and other critical information of an organization. In this Review Paper i will discuss about various cyber security threats and their solution as well. This paper also describes the various challenges of cyber security in India and Internet crime evolving around the world. Cyber Security is not only restricted to Either PC or LAPTOP but it also include mobile, tablets & similar gadgets as well because they became very important communication medium because of technological advancements grown up very rapidly in past few years. To resolve issues related to cyber security the community of security researchers should work together with govt. & private sector as well to secure against cyber threats.***

Keywords: Cyber Security, Cyber Crime, IC3 (Internet Crime Complaint Centre), CERT-In (Computer Emergency Response Team India), ISTF (Inter Departmental Information Security Task Force).

I. INTRODUCTION

Due to lack of information security various cyber crimes arises, — Cyber security means set of activities, technical and non-technical aspects of protecting information, devices, computer resources, network resources and other critical information stored there in from unauthorized access, modification and disruption, disclosure. According to emerging cyber threat report 2014 of college -- Georgia Institute of Technology android mobiles bring a new set of threats, including allowing malicious software an unparalleled look into victim's lives. While mobile device platforms are largely been safe for everyone i.e. consumers and businesses, researchers and attackers are finding ways around the ecosystems security. Cyber threats are asymmetric because as we know attacks may be perpetrated from the few upon the many, with little cost and resources. So cyber security in Information technology is of major concern in today's world of computing.

Fig. Top 5 Countries by Count: Victim Complainants (Numbered by Rank)

According to IC3 report 2012 (Internet Crime Complaint Centre) an alliance between the National White Collar Crime Centre (NW3C) and Federal Bureau of Investigation (FBI) the top five countries by count in victim complaints as numbered by Rank) as follows.

II. THE INDIAN CYBER SPACE

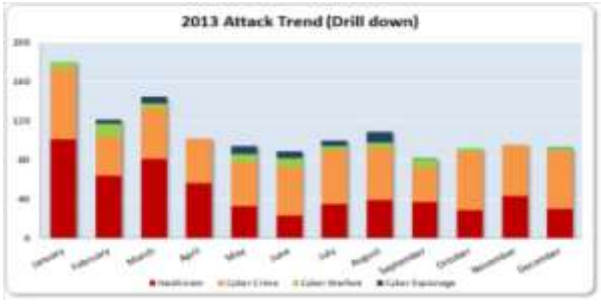
The quick development of the Internet over the past few years appeared to have facilitated to increase in the incidents of Online cyber attacks. In India National Informatics Centre's were setup in year 1975 to provide various IT related solutions to the government. There were three major networks were setup at that time.

(a) *INDONET:* It connects IBM mainframes that are made up India's complete computer infrastructure

(b) *NIC NET:* It a NIC Network for public sector organizations that connects the Central government to state & district administrations.

(c) *ERNET:* It stands for Education Research Network which is used to serve the academic and research communities.

Critical sectors such as Defense, Energy, Finance, Space, Telecommunication, Transport and other public services heavily depends on the network to relay data, for communication purpose and for commercial transactions. So these sectors have a huge impact of using the Internet as an communication source, & information according to National broadband plan the target for broadband is 160 million households by the end of 2016 and the estimate idea on Networking index that India's Internet traffic will grow nine-fold in between 2017 and 2015. Although ambitious of the government has plan to raise cyber connectivity, ecommerce services and communication channel but at the same time the government should make strong policies to stop the cyber attacks and to increase our cyber security. The government should make policies to protection against critical information infrastructure through the public private partnership (PPP).



Concluded from the data drawn from global stats. That the major cyber attack types are Hacktivism, cyber crime, cyber warfare and cyber espionage are displayed in a graph showing Attack Trends.

III. NATIONAL SECURITY POLICY 2013

Before 2013 India did not have own cyber security policy. In 2013, According The Hindu News Paper, citing documents leaked by NSA (National Security Agency) whistleblower Edward Snowden, has been aligned that much of the NSA(National Security Agency) surveillance was focused on India's domestic politics and the strategic & commercial interests. This leads to spark furor among people. Under pressure, Government unveiled a National Cyber Security Policy 2013 on 2 July 2013.

This policy is a proposed law by Department of Electronics and Information Technology, Government \of India. Which is, aimed towards protecting the public and private infrastructure from cyber-attacks. This policy also intends to safeguard "information, like personal information (of web users), financial and banking information and sovereign data .Ministry of Communications and Information Technology of India defines Cyber-attack is a complex environment consisting of interactions between everyone like, software services supported by worldwide distribution of information and communication technology.

1. Enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
2. To provide fiscal benefit to businesses for adoption of standard security practices and processes.
3. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of low enforcement capabilities through appropriate legislative intervention.

Some days before United Nation is led Internet Governance Forum in Indonesia, India, held its own – and first of its kind – conference on cyber governance and cyber security. The support of the NSCS(National Security Council Secretariat) of the Government of India, the two-day conference was organized by private think-tank Observer Research Foundation and industry body, Federation of Indian Chambers of Commerce and Industry, (FICCI) speakers were from a host of countries including Estonia, Germany, Belgium, Australia, Russia, Israel, and of course, India. There are two broad outcomes of this conference. The first is that India has indicated its willingness to start shouldering discussions to do with the global cyberspace. The other is, as India's National Security Advisor put it, ――India has a national cyber security policy not a national cyber security strategy.‖ This is certainly a start to building a consensus for that strategy.

IV. EXISTING COUNTER CYBER SECURITY INITIATIVES

Before looking into the security initiatives to be taken, look at the graph showing various industries and government areas that interest the attackers for intrusion.

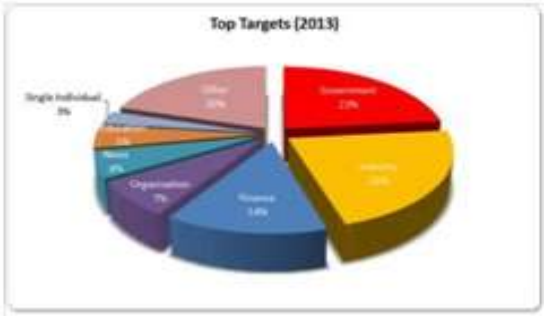


Fig. 3. (Governments and Industries have been the most preferred targets for Cyber Attackers with similar values (respectively 23% and 22%). Targets belonging to finance rank at number three (7%), immediately ahead of News (6%) and Education (5%).)

So on the recommendations of ISTF the following initiatives have been taken:

1) Indian Computer Emergency Response Team (CERT-In) has been established to respond to the cyber security incidents and take steps to prevent recurrence of the same.
2) Public Key Infrastructure (PKI) has been set up to support implementation of Information Technology Act and promotes use of Digital signatures.
3) Government has been supporting R&D activities through premier Academic and Public Sector Institutions in the country.

Some of the other initiatives that can be taken

A. NIC (National Informatics Centre):

Premier organization providing network backbone & e-governance support to the Central Government, State

Governments, Union Territories, Districts and other Governments bodies provides wide range of information and communication technology services including nationwide communication Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

B. Indian Computer Emergency Response Team (CERT-In):

Cert-In is the most important constituent of India's cyber community. It is mandate states, 'ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through

proactive action and effective collaboration aimed at security incident prevention and response and security assurance

C. National Information Security Assurance Program (NISAP):

This is for Government and critical infrastructures, Highlights are :

(a) Government & critical infrastructures should have a security policy and create a point of contact.

(b) Cert-In to create a panel of auditor for IT security.

(c) All organizations to be subject to a third party audit from this panel once a year.

V. RECOMMENDATIONS

A. Security Policy and Assurance:

1) The critical sector can be protected by improvising the software development techniques & system engineering practices. In order to secure critical sectors more strengthened security models should be adopted.

2) Better training must be provided in order to assist users in IT security.

B. Early Detection and Response:

1) To avoid malicious cyberspace activities rapid identification and information exchange methods should be adopted.

2) Identification of key areas within the critical infrastructure.

3) Establish a public – private architecture for responding to national- level cyber incidents.

C. Security Training and Programs:

1) National awareness programs such as National Information Security Assurance Program (NISAP) need to be promoted.

2) Providing training and education programs to support the Nation's cyber security needs

3) Increasing the efficiency of existing cyber security programs and improving domain specific training programs (such as: Law Enforcement, Judiciary, and E – Governance etc).

D. Promotions and Publicity:

1) In India we need to organize various workshop programs, conferences, and research programs in various IT institutes to enhance cyber security skills.

2) The promotion and publicity campaign could include seminars, exhibitions, contests, radio and TV programs, videos on specific topics, Web casts, Leaflets and posters, suggestion and award schemes.

E. Specific Recommendations [6]:-

1) Emphasis should be placed on developing and implementing standards and best practices in government function the private sector. Cyber security audits should be made compulsory for networked organizations. The standards should be enforced through a combination of regulation and incentives to industry.

2) The government should launch a National Mission in Cyber Forensics to facilitate prosecution of cyber criminals and cyber terrorists.

3) Impact of the emergence of new social networking media, and convergence of technologies on society including business, economy, national security should be studied with the help of relevant experts of including political scientists, sociologists, anthropologists, psychologists, and law enforcement experts. It should be ensured that the issues of privacy and human rights not lost sight of a proper balance between national security imperatives and human rights and privacy is maintained.

VI. CONCLUSION

The government has ambitious plans to raise cyber connectivity. There has a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily life activities, and become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility.

The cyber-attack holds the fifth place in common space and it is vital to have co ordinations and cooperation among all nations regarding cyberspace. The need of cyberspace and its exploitation is growing rapidly. The cyberspace is becoming important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cyber-attack and, thus urging a need to modify the existing laws through which these activities can be put on a check. There is a need of international cooperation of nations to crack down the efficiency on cyber-attack, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

VII. REFERENCES

[1] Emerging Cyber Threats Report 2014.

[2] Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain.

[3] Internet Crime Report 2012.

[4] B. B. Gupta, R. C. Joshi, Manoj Misra, ANN Based Scheme to Predict Number of Zombies Involved in a DDoS Attack, International Journal of Network Security (IJNS), Vol. 14, No. 1, pp. 36-45, 2012.

[5] Institute for Defense Studies and Analyses, India's cyber security Challenge, First Edition, March 2012.

[6] 2013 Cyber Attacks Statistics (Summary).

[7] Cyber Crimes.

[8] National Cyber Security Policy 2013.

[9] India Challenges Cyber Governance and Security.

[10] R. M. Johri Principal Director (information Systems) Office of CAG of India, Cyber Security - Indian Perspective"

[11] Cyber Security in India's Counter Terrorism Strategy, Col SS Raghav.