Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 6; October-December, 2016, pp. 544-545
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

A Study on Cyber Awareness

Mayank Jain[1] and Aquil Ahmad Khan[2]

[1,2]ICERT, New Delhi
E-mail: [1]engineermayankjain@gmail.com, [2]akhan2786@gmail.com

Abstract—*Cyber security has reached its paramount level with the large volume of breaches, attacks, malware, ransom ware, DDoS, and vulnerability exploitations particularly in banking, finance, and critical sector. Recently, cyber-attacks have emerged as a major challenge for organizations across the globe with hackers targeting not only sensitive data, but also rendering public services dysfunctional through use of disruptive malware like ransom ware.*

Keywords*: Cyber security, Cyber-attack, Cybercrime.*

1. INTRODUCTION

India is one of the quickest developing internet markets that makes it more vulnerable to cyber-attacks. With increased connectivity and digitization of services, the attack surface in India is increasing at an exponential rate. It is vital to comprehend that digital security challenges do not stop at national or state outskirts. In recent years, the scourge of activists, cyber criminals and nation-state actors has taken a monstrous turn by straightforwardly focusing on governments for numerous reasons - fun, defame, revenge, financial and political gains. Attackers are profoundly prepared, organized, highly funded, and trained with generous scientific capabilities.

Because of the poor cyber hygiene, insufficient strategic intelligence and lack of cyber awareness, give a simple play area to attackers to execute their malicious targets. Secure organizations against such evolving threats can be done but also we have to focus on users who act as the first line of defence.

Digitization has changed security dynamics, and it will get worse if we do not make people aware now. There are various challenges, which need to be addressed in cyberspace such as legal issued related to cyber security & cloud computing, mobile law challenges, and social media a legal issue. Hackers, now deploy sophisticated social engineering techniques like Spear phishing, Business Email Compromise, etc. to bypass traditional defence mechanisms and attract user to download malicious software on their devices.

Fact Check: Recent Cyber Attacks in India

- India was the third most impacted country in the Wannacry attacks.
- A food delivery app was targeted as a cyber-attack in India recently where hackers stole the credential of customers.
- Dark Pulsar, Magniber, Kuik Adware, Emotet Trojan, Panda Banker / Zeus Panda are latest malware with advanced features like file exfiltration, remote command execution and anti-vm techniques.

2. LITERATURE SURVEY

Cyber security is major concern of government and private sector around the world. Cyber threat can be in the form of cyber-attack, but can also be in result of “mistakes” or even natural disasters. Therefore, there should be specific approach to the particular problem in the framework of cyber security [1]

Cybercrime is the one of the emerging trend of crime which has the prospective to destroy each and every aspect of the life as it is easy to commit but it’s really hard to detect and often hard to locate in jurisdiction terms, given the geographical indeterminacy of the net [2].

Cyber security threats are “outpacing the ability to overcome them unless all stakeholders begin to cooperate. Holistic awareness and proper scaling of streamlined cyber security processes can help bridge this gap in Digital India [3].

There is need for the Cyber Security to protect the evolving ICT. The expert group should find and recommend suitable mix of solutions in critical ICT systems supporting the governance structure of the nation [4].

3. PROPOSED IDEOLOGY

India to prevent a cyber hazard getting converted into a cyber disaster, it needs proper management of cyber risks via faster threat detection and automatic sharing of alerts with sector specific organizations and their users. With the increasing complexity of cyberspace, the real time awareness is finding its way into current age cyber security architecture and is being touted as indispensable for tackling modern cyber threats.

4. CONCLUSION

There is a need to track and alert each stakeholder against latest security threats like malware, vulnerabilities, phishing methods and latest Tactics, Techniques and Procedures (TTPs) through sharing of threat bulletins, advisories and real time reports.

There is a requirement of Automated Security, Alerting with Strategic Intelligence sharing to mitigate the cyber security threats.

REFERENCES

[1] David Satola and Henry L.July, “Towards a Dynamic Approach to Enhancing International cooperation and collaboration in Cyber Security Framework”, ‘The MW. Mitchell law journal’.

[2] Aashish Kumar Purohit , “ Role of Metadata in Cyber Forensic and Status of Indian Cyber Law” , International Journal of computer technology application, vol.2(5) sep-oct, 2011.

[3] World Economic Forum’s Cyber Resilience Playbook for Public-Private Collaboration. January 2018.

[4] M.M.Chaturvedi, M.P.Gupta and Jaijit Bhattacharya “Cyber Security Infrastructure in India : A Study”pp.1-15