International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-6, Issue-3, May 2019
DOI: 10.21276/ijirem.2019.6.3.2

Latest Trends on Cyber Security

Ananya Shukla
Student, Department of Computer Application, International Institute for Special Education, Lucknow, India
ananyadotshukla@gmail.com

Prof. Naveen Upreti
Senior Assistant Professor, Head, Department of Computer Application, International Institute for Special Education, Lucknow, India
naveenupreti@gmail.com

Prof. Manoj Kumar
Senior Assistant Professor, Department of Computer Application, International Institute for Special Education, Lucknow, India
iisemanoj@gmail.com

ABSTRACT

In the development of information technology as well as Internet services Cyber Security plays an important role. When we hear about the word "cybercrime" the first thing that comes in our mind on cyber security and the thing is that how good the infrastructure of our "National Cyber Security". This term cyber security is sometimes used interchangeably with the term information security. This paper throws light on the latest technology such as mobile, cloud; e-commerce etc. It also explains the challenges which are coming due to lack of coordination between Security agencies and the Critical IT Infrastructure. In the cybercrime the human is the target for cyber-attack, people participate in this unknowingly. Hacking can be good as well as bad based on the mind of the hacker. Hacking is done for the security of the organizations but it can also be used to harm anyone.

Keywords

Social Networking, Cloud Computing, Cyber Security, Information Security, Mobile Computing, Cyber Crime, E-commerce, Survey, Trends, Biometric , Phishing

1. INTRODUCTION

As we all know that the Internet is one of the fastest-growing areas of technical infrastructure and development [2].

Is is growing so rapidly that now a days everyone is able to access it as it is also cost efficient. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online [3].

In Today's life around 80 percent of total commercial transactions are done online through various websites and applications, therefore this field required a high quality of security for the best transactions and for the transparency in the transaction. The Cyber Security's scope extends to the security of IT systems within the enterprises, and also to the wider digital networks upon which they rely including cyber space itself and critical infrastructures [4].

Cyber security plays an important role in the ongoing development of information technology, as well as Internet services [5].

Expanding and updating cyber security and protecting critical information infrastructures are essential to nation's security as well as economic wellbeing. For the new services and government policy it is become essential to make internet safer [6].

Cybercrime is being an integral component of a national cyber security and it is also used for protection strategy of critical information. Cyber security requires a comprehensive approach for the formulation and implementation of a national framework. Strategies made by Cyber security such as development of technical protection systems or education for the users to prevent from becoming victims of cybercrime, these can help to reduce the risk of cybercrime. In the fight against the cybercrime the development of cyber security strategies are a vital element. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach [7].

Cyber security strategies for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime can help to reduce the risk of cybercrime [8].

The development and support of cyber security is an essential strategies against the in the fight with cybercrime [9]

2. RELATED WORK

G. Nikhita Reddy et al. proposed a scheme that mainly focuses on the challenges faced by the user in the field of cyber security on the latest technology. This paper also focuses on the trends, ethics and techniques of cyber Security.[10]

Iuon-Chang Lin et al. proposed a new scheme for Block chain technology which may bring more reliability and convenient services. This technology is not a single technique but it contains cryptography, mathematics, Algorithm etc. To solve traditional distributed database synchronize problem. This paper also focus on the security issues and challenges behind the this innovative technique.[11]

Anwaar Al Dairi et al. throw some light on security issues in Smart cities. In their paper they are providing detail literature of the major security issues and their solution. This paper also present some of the influence factor which affect data and security of information in smart cities.[12]

3. LATEST TRENDS IN CYBER SECURITY

Following are the recent trends which can be seen in 2019

3.1 Biometric Hacking

There are several cases came where data is theft from biometric. Biometric systems are used for the authentication and identification of the user which is being implemented by several financial institutions in META (Middle East, Turkey and Africa), 2019 will see criminals exposing vulnerabilities in passcodes, touch ID sensors and facial recognition," says Fabio Assolini, senior security researcher at Kaspersky Lab.

3.2 Use of AI technology for Cyber Attack

Hackers are using AI technology to make their attack more difficult to detect. Whereas AI also helps to deal with threats in advance way.

3.3 Phishing Attack

As Email attack is increasing very rapidly for any organization as well as individual user.

3.4 Viral of Fake Video

UK-based innovation foundation Nesta forecasts that 2019 will see a new level of malicious posts on social media as fake videos set the next stage in fake news. Attackers are misleading public by making fake videos with the help computer graphics and show the public that event which never happened.

3.5 Malware Attack in Mobile

While malware that runs on the Windows operating system vastly outnumbers malware for any other platform, users of mobile devices are increasingly subject to malicious activity that forces malware apps to the phones, tablets, or other devices running Android and iOS, according to computer network security company Sophos' 2019 Threat Report.

4. RECENT SURVEY ISSUES ON CYBER SECURITY

4.1 Mobile Devices and Apps

The rapid growth of mobile devices comes with rapid growth in security risks. Every new smart phone, tablet or other mobile device, opens another route for a cyber-attack, as each creates another vulnerable access point to networks. Now it is not difficult for the thieves to attack mobile phones.

4.2 Social Media Networking

It is growing use of social media which is to personal cyber threats. Social media is very popular among the business therefore it is also threat of attack. Account on social media is increasing with days and also increase in attacks. Social media companies need to improve the policies and prevent the users from data leakage, cyber bulling etc.

4.3 Cloud Computing

In today's time there are many firms which are working on cloud computing technology. Due to its cheap and effective services people or companies are migrating towards cloud. Cloud having a well-managed architecture and well developed security planning reduce the risks of cyber attach

4.4 Protect systems rather Information

The main concern is to protect the information rather than system. As all the businesses are moving to online, therefore the requirement for the security is now beyond simply managing system to protecting the system.

4.5 New Platforms and Devices

Any new platform or devices creates new opportunity for cybercriminals. Security threats with personal computer running on Windows are being associated from long time. But the new platforms and devices create new threats. There are so many malicious apps available on app stores.

5. SPECIFIC CYBER SECURITY TECHNOLOGIES

5.1 Firewalls

Almost every system have inbuilt firewall but they never understand its importance. It is used to monitor traffic from the both side of computer that is in and out and give alert to the user for any unauthorized access.

5.2 Cryptography

This technology is used to keep the data safe when data is send from one user to another. It is well known for confidentiality as it encrypts the data then transmits it to the user.

5.3 Access Control and Identity Management

There should be Username and password for accessing any system which is the fundamental of computer access control

5.4 Authentication Documents

It need to be authenticated which should have been originated from a trusted source and that must not been subsequently altered.

5.5 Malware scanners

Using of Software, which scan files and messages for malicious code on regular basis.

6. KEY CHALLENGES TO SOCIETY

Complex infrastructures of our Nation are composed of public and private institutions or organization in the sectors of, emergency services, government, public health, defence industrial base, information and telecommunications, energy, transportation, banking and finance. India is also shifting gears by entering into the world of internet and making almost everything on e-governance. India has also brought sectors like income tax, passports visa, police, judiciary etc. Banks of India is also getting full-scale computerized.. This has also brought in concepts of e-commerce and e-banking. The stock markets have also not remained immune [1]

7. CONCLUSION

Cybercrime is now became a very serious as it affects the public, private as well as government sectors. It is spreading very rapidly. It is a very big risk for every people, institute or organization.. It affects the national and economic security. Now it is very importing to implement required measures against the cybercrime. There should be also strict rules for cybercrime. Although not everyone are victims to this, but still they are at risk. Crimes through internet are varying day by day. The hackers are the age from 12 years young to 60 year old. Because of the technology the hacker can hack your data from anywhere in the world. Hackers of this era do not need guns all they need is system and hacking techniques.

ACKNOWLEDGMENT

I thankfully acknowledges to Prof. Naveen Upreti and Prof. Manoj Kumar, Department of Computer Application, International Institute for Special Education, Lucknow.

REFERENCES

[1] Integrated Defense Staff, "National Informatics Center", Ministry of Defense, India

ISSN: 2350-0557, Volume-6, Issue-3, May 2019
DOI: 10.21276/ijirem.2019.6.3.2

[2] Yang, Miao, "ACM International Conference Proceeding Series", vol. 113

[3] Unisys Corporation, "Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security" USA, 2011

[4] Cyber Security Strategy of United Kingdom, 2009

[5] ITU Cyber Security Work Program to Assist Development Countries, 2009

[6] Rev. Jonames Burg, TTU WTSA Resolution 50, 2008

[7] ITU Cyber Security Work Program to Assist Development Countries, 2008

[8] Kellermann, "Technology Risk Checklist, Cybercrime and Security", IIB-2

[9] Schjolberg/Hubbard, "Harmonizing National Legal Approaches on Cybercrime", 2005

[10] G. Nikhita Reddy, G.J. Ugander Reddy A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies, *8 Feb 2014)*

[11] Iuon-Chang Lin1,2 and Tzu-Chun Liao2 "A Survey of Blockchain Security Issues and Challenges"Jan. 12, 2017)

[12] AnwaarAlDairiLo'aiTawalbehCyber"Security Attacks on Smart Cities and Associated Mobile Technologies"12 June 2017

