Volume 5, Issue 3, July 2018 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

An Enhanced Cyber Security Methodologies to Avoid Cyber Crimes

Jatoth Santhosh Kumar
M.Tech Research Scholar
Department of Computer Science & Engineering
Dhruva Institute of Engineering & Technology,
Hyderabad (T.S) [INDIA]
Email: nayaksanthosh40@gmail.com

K.V. Naganjaneyulu
Professor & Principal,
Department of Computer Science & Engineering
Dhruva Institute of Engineering & Technology,
Hyderabad (T.S) [INDIA]
Email: kvnaganjaneyulu75@gmail.com

ABSTRACT

Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks. In a computing context, security comprises cyber security and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Today, given the increasing dependence on information and communication technologies (ICT), particularly the web, for delivery of services and operations, one among the largest challenges the globe faces is that of cyber security. Cyber security could be a advanced issue, touching several application domains and straddling several disciplines and fields. Securing the important infrastructures needs protective not solely the physical systems however, even as necessary, the cyber parts of the systems on that they swear. The foremost important cyber threats square measure basically totally different from those posed by the "script kiddies" or virus writers who historically have infested users of the web.

Given the sort of activities being allotted within the Net, Net merges seamlessly with the physical world. However thus do cybercrimes. Backbone of cyber criminals the underground black market supported by exploit kits, packaged malware and hacks is anticipated to continue and evolve citing tried-and-true crime ware like part, ransom ware, APTs that are improved and refined in ways in which shows the extent of expertness and methodology for developing malwares. Cyber attackers will disrupt important infrastructures like money and traffic management systems, manufacturing effects that square measure almost like terrorist attacks within the physical area. They will additionally do fraud and money fraud; steal company info like intellectual property; conduct spying to steal state and military secrets; and recruit criminal's et al to hold out physical terrorist activities. What makes network even a lot of engaging to criminals as well as non-state actors is that attribution in Net is tough, particularly only if Net is borderless and cuts across jurisdictions. It permits criminals to launch attacks remotely from anyplace within the world. With this growing threat landscape, cyber-readiness of the safety systems has been perpetually place to test. In this paper we also had undergone a research on cybercrimes.

Keywords:— *Cyber Security, Cybercrime, Cyber security research, Security, Computer, Privacy.*

I. INTRODUCTION

Cyber Security analysis is one context wherever the answer to modify cyber criminals is germinating. Investment of

your time and resources needs fostering ways for analysis and developing transformative answer to fulfill important cyber security challenges involving an explicit technology (e.g. cloud computing), or a specific application domain (e.g. finance), or a mixture of two. To begin with the main target of cyber security analysis is today to modify new rising threats and detective work the threats before they impact or cause smart quantity of damages. With growing variety of phishing, APTs and botnet attacks, there's heap to be worked in terms of technological advancements and detection technology to fulfill the cyber threats of the long run. The advent of computers and therefore the growth of the net made doubtless the accomplishment of enormous improvement in research, surgery, expertise, and communication. Unfortunately, computers and therefore the web have what is more supplied a replacement natural surroundings for crime. As Janet Reno, U.S. advocate general throughout the Clinton management, put it, "While the net and alternative information technologies area unit conveyance tremendous benefits to humanity, they what is more provide new prospects for lawless individual behavior" (Dasey, Pp. 5-19).

Cybercrime is roughly characterized as committing a misdeed through the utilization of a laptop or the net. The Internet has been characterized as "collectively the myriad of laptop and telecommunications amenities, encompassing gear and functioning programs, which comprise the interconnected worldwide mesh of systems that provide work the Transmission management Protocol/Internet Protocol, or any forerunner or successor protocols to such protocol, to broadcast information of every kind by cable or radio". In other phrases, the net could be a massive laptop mesh, or a string of connections of computers that area unit hooked up along. This property permits persons to connect to numberless alternative computers to accumulate and convey information, notes, and data. Unfortunately, this property what is more permits lawless individuals to broadcast with alternative lawless people and with their victims.

II. Application of Network Security

- It is used to avoid unauthorized users from accessing our network without interrupting our service.
- Sensitive information to be transferred in the public network.
- Which is used to determine and fix security issues?
- It is used to provide an enhanced system of warning alarms attempt to access public network.

Over the past few years, Asian country has witnessed large adoption of cyber technologies altogether the sides of life.. These challenges become a lot of severe once moving the national security and economic prospects of the country. Moreover, Asian country being a most well -liked outsourcing destination for IT and pace services needs a targeted and continued attention on security and privacy. This attention is important to keep up confidence of the world purchasers, as security and privacy issues square measure key parameters within the outsourcing choices. Therefore, a requirement for adequate efforts and investment in cyber security capability building and R&D activities has conjointly been emerged within the cyber system.

III. Cyber Security Research

Cyber security capability building may be a rising phenomena globally and Asian country isn't any exception during this and within the recent past country has witnessed vital improvement during this domain. R&D activities in cyber domain square measure gaining traction in camera sector and academe in Asian country, with the support of and encouragement by the govt. In recent past country has witnessed varied productive analysis outcomes and plenty of them are translated into businesses, through the emergence of autochthonous cyber security corporations. Academe is enjoying an important role in Asian country to make a healthy system for the cyber security analysis that is clear from rising of autochthonous cyber security corporations rising out from the incubation centers of those tutorial establishments. The world acceptance for the big selection of autochthonous merchandise & services offered by these corporations has conjointly been seen in recent past. Ancient IT services suppliers also are giving Due prominence to cyber security domain and a few of the players have swollen their analysis activities in cyber security. During this paper, a number of the continuing analysis activities within the country are mentioned and this paper mustn't be thought-about as a reputable supply for all the continuing analysis activities within the country. a number of the analysis square measure as are highlighted below.

IV. Results and Analysis

Computer geniuses, typically in their twenties, are thrown challenges to interrupt one or another security program, capture the passwords to remote computers and use their accounts to travel the computer network, enter information networks, airline reservation systems, banking, or the other "cave" additional or less dangerous. Managers of all systems have tools to manage that "all is well", if the processes ar traditional or if there's suspicious activity, a user is mistreatment to access roads that is not approved. All movements ar recorded in system files, which operators review daily (Farmer & Charles, Pp. 46). Furthermore, the network is turning into the best place for criminals and terrorists to hold out their actions and activities. Hence, law-breaking and cyber terrorist act have become 2 of the foremost serious threats appear to haunt Western societies. Moreover, the impact of the crimes on the victims and their measures to cope up with such crimes within the future also will be a vicinity of the paper.

V. Conclusion

For strengthening the cyber system, a targeted attention and adequate investment of efforts & resources would be needed for cyber security. Investment within the R&D activities in cyber security domain might lead to high returns like opportunities for entrepreneurs resulting in growth of companies that successively might lead to additional jobs within the market, multiplied trust and self-direction of the state. Although R&D activities touching on cyber security being undertaken in Asian nation have up late, a great deal additional must be done, especially to match the amount of technological advancements happening globally. By virtue of its dynamic nature, cyber security needs continuous pursuit of evolving technologies globally and its alignment with a country's R&D objectives and agenda. Increasing role of computer network puts in situ a high demand of intensive R&D activities to be applied within the nation, with a collection agenda. This demand is re-enforced within the lightweight of giant opportunities that exists within the international and domestic

market. Contribution would be needed from all the stakeholders - government, trade and academe - requiring that they are available along and outline a cyber security R&D roadmap for the country. Public personal Partnership (PPP) is that the means forward, because it would facilitate in combining better of each worlds and complement capabilities to develop a procurer cyber system. Arrangements conjointly ought to be place in situ for retentive the talent within the country and providing acceptable protection to the IPRs developed by the autochthonous cyber security analysis organizations. The govt ought to fund analysis in academe and conjointly within the trade, and supply incentives to the companies for investment in R&D activities.

The analysis ought to be market driven, and deliver solutions for the $64000 world. In conclusion, it is same that attacks on machines connected to the net have multiplied by 260% since 1994, with an calculable loss of one, 290 million bucks annually in the U.S. within the era of knowledge, ideas, knowledge and files on your network area unit most likely additional valuable than your entire company. Consider your client lists and records of shareholders, commercialism and promoting materials, marketing strategies and merchandise style, the loss of that might mean the significant loss for your firm. With advances in technology, nobody is safe from an attack by "hackers. Currently it's comparatively straightforward to realize management of a machine on the Internet that has not been adequately protected. Companies invest a big portion of their cash in protecting their info, since the loss of irreplaceable data could be a real threat to their business. The technology boom in the development of networks, digital communications and advances in software system technology allowed the birth of a virtual world whose final expression is that the web. Today, for the implementation of effective measures for protecting info needs not solely protection of information networks and mechanisms for a model of network security and implementation of a scientific approach or a collection of information protection - a posh of interrelated measures, delineate by the definition of "protected information".

REFERENCES:

[1] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011: Pp. 5-19.

[2] Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.

[3] Harrison, A. Privacy group critical of release of carnivore data. Computerworld; Vol. 34, No. 41, 2006: Pp. 24

[4] Internet Tax Freedom Act of 1998: 112 Stat. 2681–2719. Retrieved from: (http://www.cbo.gov/doc.cfm?index=608&type=0). Accessed on : 29th January, 2012.

[5] Katz, Mira L. & Shapiro, Carl. Technology Adoption in the Presence of Network Externalities. Journal of Political Economy; Vol. 94, No.4, 1986: Pp. 822-841.

[6] Ogut, Hulisi. Menon, Nirup. & Ragunathan, Srinivasia. Cyber Insurance and IT Security Investment: Impact of Independent Risk. Proceedings of the Workshop on the Economics of Information Security (WEIS), Cambridge, MA:

Harvard University, 2005: Pp. 14-28.

[7] Richards, James. Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.

[8] Roland, Sarah E. The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?. Suffolk University Law Review; Vol. 35, 2001: Pp. 638-45.

[9] Tipton, Harold F. & Krause, Micki. Information security management handbook (5th ed.). London: Taylor & Francis e-Library, 2005: Pp. 320-386.

[10] Whitman, Michael E. & Mattord, Herbert J. Principles of information security (2nd ed.). Boston: Thomson Course Technology, 2005: Pp. 205-249.

* * * * *