Cyber Security: Challenges and proposed solutions

Name: KomalSaxena
Phd scholar in computer science
Singhania university

Dr. Anurag Awathi
GUIDE
SINGHANIA UNIVERSITY

Abstract: Cyber crime is of much concern these days and why not! It is the serious subject for discussion especially for small to large businesses and organisations. Cyber civilization is an important source for professional activities and information sharing such as banking transactions, business communication, advertisement and services. The World Wide Web is the source of storing a large amount of data online and sharing. With the change in time the web applications are becoming more complex and highly unsafe giving chance to cyber criminals to attack the system and steal or modify vital information.

At present online connectivity, individual privacy, mobile devices connected to internet and above all social networks are the major target for attacks. In this research paper you will find a detailed analysis of the existing system and their methodology, cyber security challenges and their solutions.

Key words: Cyber security ,CyberInsurance,cyber-frauds, Internet Attacks

1. INTRODUCTION

History speaks that the losses from the cyber crime activities on businesses, organisations and individuals have increased over time. In US, it is being revealed that "Pentagon's systems are tested by cyber criminals or unauthorized users for about 6 million times every other day." [1].The wrongdoing environment in the internet is entirely different when compared to the real world that is the reason there are numerous obstacles to uphold the cybercrime law as genuine space law in any general public.

For Example, age in genuine space is a self-verifying element as contrast with the internet in which age is not comparatively self-authenticating. A kid under age 18 can undoubtedly shroud his age in the internet and can get to the resources where as in real space it would be troublesome for him to do as such.

Cyber security includes securing the data by counteracting, detecting, preventing and resolving cyber attacks.Cyber security protects computers and networks from cyber criminals also from the crimes that are conducted on internet.The illicit exercises such as internet fraud, telemarketing, credit and debit identity theft, are cybercrimes when these exercises are conferred through the utilization of a PC and Internet [2

1.1 Intro of Cyber crimes:- ""Offences which are committed in opposition to persons or

categories of those that have some sort of legal motive to help deliberately damage your standing of your unwilling recipient or result in actual or mind damage, or decline, towards unwilling recipient precisely or ultimately, using modern telecommunication network including such as Internet and mobile phones(sms/MMS ,Email, chat etc)[10]

1.2Categories of Cyber crimes-

People who Involved in cyber crime

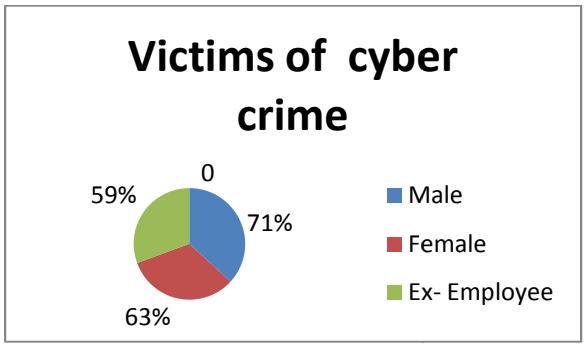

Fig1[9]

1.2[1]. Cybercrime against individuals such as spreading child pornography, provocation through mail, dispersal of disgusting material or infringement of security of residents. Such Cyber crimes have negative consequences upon the new era and society as entire, if not legitimately controlled.

1.2[2]. Cybercrimes against all manifestations of property incorporates PC vandalism (decimation of others' property), transmission of destructive programs, and utilization of different spyware to steal corporate information. Such unlawful acts brought about loss of millions of dollars around the world, by harming computer networks and systems.

1.2[3].Cybercrimes against Government incorporate the terrorist activities that often break the security system of military and government website. Computer based infringement may be in the manifestation of computer trespassing unapproved access, hacking, or a computer fraud.

Some of the other cyber crimes that are affecting the world today are as follows-

- Cyber theft
- Cyber Vandalism
- Web Jacking
- Stealing Credit Card information
- Software Piracy
- Industrial Espionage
- Cyber Terrorism
- Child Pornography
- Cyber Contraband
- Spam
- Wi-Fi High Jacking
- Cyber Trespass
- Logic bombs
- Salami attacks
- Script Kiddies
- Denial of service

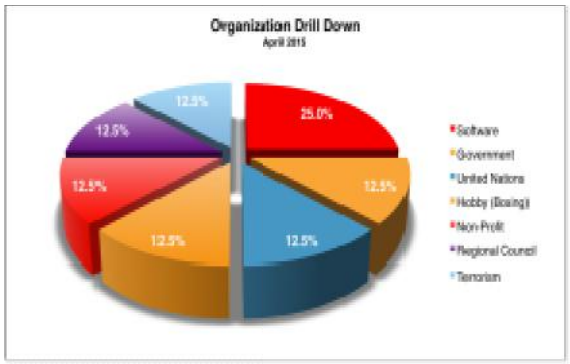

Figure2.[15] shown the crimes statistics of April 2015 in organization fragmentation

Statistics &prediction on growth ofcyber crimes:By 2017 the worldwide cyber security market is expected to skyrocket to dollar 120. 1 Billion from $63. 7 billion inside 2011 [9]. The actual setting regarding cyber crime remains surprising, also it is maintaining growth. In 2012, for example, america overall economy dropped $525. 5 million in order to cyber crime(Federal Bureau regarding Study, 2013), upwards above 45 million from 2011 with more widespread grievances inside 2012 currently being impersonate crimes, with email cons, intimidation and cons of which attempted to extort money from personal computer people. In 2012, cyber crime expense British businesses €21 thousand (Morris, 2012), and above one million personal computer people inside europe had been impacted every single day by cyber crime(EruActive, 2012). cyber crime inside these locations persists largely because of not enough consumer Education[13].

There are various cyber security solutions are available today, with the evolution of various new technologies and programming codes a number of solution exists like various types of vulnerability scanners, Interruption Detection System (IDS), Intrusion Prevention System (IPS), Network as well as Application Firewall.

As the greater part of the cyber crime acts attack the application layer utilizing port 80 or 443(SSL) for communication. Such security solutions are not the answer for application level attacks. System firewalls are just securing the inner system of the associations and are helpless against different application assaults by the cyber criminals. Various cyber security solutions in brief-

A. Interruption Prevention System (IPS)

Interruption Prevention system or frameworks are the product intended to not just to distinguish the unauthorized access to the resources yet likewise to keep these data(resources) from the cyber criminals.

B. Vulnerability Scanners

The Application web scanners are the mechanized tools which first creeps a web application and after that weigh its pages in request to discover the vulnerabilities in the application by utilizingpassive technique. In this method the Scanners creates a test inputs and after that check reaction against these data for the security vulnerabilities [3, 4].

C. Intrusion Detection System

Intrusion detection systems (IDS) are the product intended to recognize the illicit access to the computer system and resources. Intrusion Detection Systems based on signatures identify the attackers signature apply there on with the help of pattern matching algorithm [5] in order to detect the attack[6, 7, 8].

Inconsistency based framework dissects the information stream against builds profile and arranges all anomalous conduct aspernicious. Data Mining Methods for Anomaly detection give the structure to web application assaults taking into account the measurable procedures.

4. CHALLENGES

• Current Web application systems are responsive; cyber attacks are identified by regularly examining the framework logs and information; threats are just forestalled if the signature of the particular attack is perceived by the framework (generally the

attack is distinguished and may trade off the security of the framework). It is important to plan methods that are proactive and give essential measures to keep the misuse of vulnerabilities that may harm the application.

• Today, each existing systems are signature based, which keep up the syntactic representation of the threat. It is simple for an assailant to dispatch an attack by slight adjustment of this syntactic representation of the signature. One noteworthy challenge today is to design a system in such a waythat it detects and prevent from various pattern or variations of a specific attack.

• Similarly conduct based IDSs that usually runs at the application layer are not based on signature and may distinguish new, beforehand obscure, attacks. Then again, in these frameworks, a little variation from the information makes high false positives results. This is now a challenge to outline a framework or design a system that minimizes these false positives without obliging the information and to successfully distinguish zero day attacks.

• Statistical procedures utilized as a part of IDSs essentially give the solution at the network layer. This solution is not compelling at the application layer in light of the fact that these methods concentrate on the character conveyance of the data and don't take into record its logical nature.

• Security systems that are learning based create an abnormal state of false positives and learning methodology must be rehashed after every adjustment in the application rationale, which is a period devouring errand.

• Most of the current arrangements are utilizing primitive (yet genuinely successful) signature based threatrecognitionmechanism. No functional framework has been actualized which utilizes semantic examination to information/conventions to moderate this issue yet. This conceives a test to apply procedures from the field of semantic web application.

5.Researchesby the organization on cyber security

*IT universities doing more research on cyber security & Risk

*TelestraAustrallian co more into research on cyber security

*Hosted Mail Securityidentity theftLaw & orderMalwareMcAfeeMcAfee Avert LabsMcAfee Security InsightsMicrosoftMobilePandaPandaLabsPhishingRandy AbramsscamSecuritySecurity Responsesocial networkssophosSophosLabsSpamSunbelt SoftwareSymantecSymantec Security ResponseTenable Network SecurityTrendMicroUncategorizedvulnerabilitiesvulnerabilityWeb Application Security,Websense,Zscaler Research.McAfee Calls for EU Solution on Cyber Preparedness. Legislators, representatives from NATO, the European Defense Agency (EDA), the Military Staff of the EU (EUMS), and the European Network and Information Security Agency (ENISA) .Dupont, sans Institute. IIT invest (approx.)1 crore on cyber security research, SANS INSTITUTE,HP,DELL SECURE WORK-Sec Lab: Predictions and Trends for Information, Computer and Network Security, Trend Micro on advance persistent Threat.

A. Cyber security service Providers some of them are listed below:-

1. IBM,
2. FireEye INc,
3. Trend Micro,
4. SANS security lab,
5. HP security
6. Dell security works
7. Cisco security
8. Web sense Lab
9. Semantec
10. Homeland security
11. ISASC

B.Prevention & Detection offered in cyber security:-Several methods of Prevention and detection offered by various organizations few of them discussed Here:-

B 1.Trend Micro: They uses a generic techniques to detect the Malicious activity.[15]

-Protocol aware Detection
-HTTP Headers
-compressed Archives

B [2].DELL SECURE WORK They work on policies standards, more research on information security to protect customer to resolve threat intelligence also cover vulnerability of software's. In this the analyst more research on protection & solution on security[16]

B[3]Cisco : They are also provide some solution on cyber security & Risk . How to cover the security by using different methods to control Malware & threats also proposed threat centric approach to security that reduces complexity while providing superior visibility, endless control,and advanced threat protection across the entire attack range. With this threat-centric securitymodel, organizations can act fast before, during, and when an attack.[17]

B. Insurance companies covered a Cyber Security&Risk.:- A full Jacket on threats, Malware etc. Cybersecurity insurance is designed to mitigate losses from a variety of cyber cases, including data breaches, business interruption, and network damage. A strong cybersecurity insurance market could assistance reduce the number of successful cyber attacks by: (1) supporting the adoption of preventative processes in return for more coverage; and (2) encouraging the implementation of best practices by establishing premiums on an insured's level of self-protection. Many companies relinquish available policies, however, citing as rationales the observed high cost of those policies, confusion about what they insurance, and insecurity that their organizations will undergo a cyber attack.

Few of the insurance co into cyber security are listed below :-

1.CHUBB Group of cyber security,

2. EY insurance co.
3.cyber edge also dealing in insurance of cyber security,
4.Marsh offering insurance on cyber security & risk as threats of data, security breaches, and other online intrusions proliferate, it takes a cyber riskprofessional to identify your vulnerabilities and help you develop an effective policy of hindrance, preparation, and security for your organization.
5.Home land security deals with insurance.

5. CONCLUSION

Looking at the present scenario every business and organization is gearing to be online. This will make them place large amount of data at the cloud. Cyber attackers have eye on such data and try to steal and modify the information. The present cyber security solutions are static based on signature i.e. it can only detect cyber crime activities when the signature is present. Hence there is a need of dynamic and semantic solution to detect and prevent cyber crime.

6. REFERENCES

[1] Dupont A. Time to attack cybercrime with a strong security policy. WWW page, October 2010.

[2] Justice, U. D., INVESTIGATION, F.B. Parent's Guide to Internet Safety. Compiler 19, 1 (1999),4.

[3] Fong, E. and Gaucher, R. "Building a Test Suite for Web Application Scanners". In hicss (2008), IEEE Computer Society, p. 479.

[4] Fong, E., and Okun, V. "Web Application Scanners: Definitions and Functions". In System Sciences, 2007.HICSS 2007.40th Annual Hawaii International Conference on (2007), IEEE, pp. 280b– 280b.

[5] Boyer, R., and Moore, J. A fast string searching algorithm. Communications of the ACM 20, 10 (1977), 762–772.

[6] Guha, B., and Mukherjee, B. Network security via reverse engineering of TCP code: vulnerability analysis and proposed solutions. Network, IEEE 11, 4 (1997), 40–48.

[7] Ryutov, T., Neuman, C., Kim, D., And Zhou, L. Integrated access control and intrusion detection for web servers. IEEE transactions on parallel and distributed systems (2003), 841–850.

[8] Roesch, M. et al. Snort lightweight intrusion detection for networks.

[9]http://www.go-gulf.com/blog/cyber-crime/

[10]http://en.wikipedia.org/wiki/Computer_crime[11]Halder, D., &Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

[12]Internet security system March 2005

[13]http://www.enotes.com/research-starters/social-impacts-cyber-crime

[14]E:\cyber security research\2012 Cyber Attacks Statistics _ Hackmageddon.com_files

[15]**www.trendmicro .com DETECTING APT ACTIVITY WITH NETWORK TRAFFIC ANALYSIS**

[16] Dell- secure-Work threat report updateIQ122015

[17]Cisco 2014 Annual Security Report: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[18]IBM SECURITY SOLUTION

[19]ISASC SECURITY SOLUTIONS

[20]Mc free Avert Lab

1.First Author: Ms. Komalsaxena perusingphd in computer science from singhania University .My research is on Cyber security and risk .Presently working in university. I have total 15 years of experience in teaching and more than 3 years in corporate.

2.Second Author: Dr. Anurag Awasthi(Guide)

- Over 27+ years of rich overseas and indigenous experience (21 years in Corporate and 6+ years in Academics/Consulting)(Worked in India, Japan, France and Thailand. Visited SriLanka and Pakistan.)
- (Ex) Director and Professor (MCA) with Noida Institute of Engineering & Technology (NIET), Greater Noida. Ph.D. (Computer Science) - ('An Integrated Framework for Implementing Process Improvement in Software Development Organisation') from Kumaun University, Almora (Uttarakhand), 2005.
- Ph.D. (Management) – ('A Study of Employee Engagement Practices in IT industry, with reference to the organizations in Delhi/NCR') from Singhania University, Rajasthan, 2013.
- M.C.A from BIT, Mesra, Ranchi, 1988.
- M.Sc. (TQM) from Kuvempu University in 2006. (University Gold Medallist).
- PGD-HRM from IMT Ghaziabad, 2008. (2 years)
- LLB from Delhi University, 1993.
- B.Sc. - Physics, Maths, Statistics from Meerut University, 1984.